



Beschreibung zur Weitergabe an den DVO, Stand 15.12.2025

Gültig ab EVIDENT Version 6.05

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 herunter, abgelegt unter

<https://www.evident.de/service/technische-voraussetzungen-downloads/>

Schritt 1: An dem Arbeitsplatz, an dem KIM-Nachrichten versendet und empfangen werden sollen nehmen Sie die technische Einrichtung im Menü **Praxis, Arbeitsplatz**, Registerseite **KIM** vor.

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



Arbeitsplatz-Einstellungen

Bildschirm Einstellungen Geräte & Schnittstellen Praxis Sortierung Intern Verzeichnisse

Formulare SMS U-Pad Smart Edit **KIM** Verordnungs-Software (VoS) eRezept

KIM - Arbeitsplatz

POP3 - Server: 10.0.0.248

POP3 - Port: 995

SMTP - Server: 10.0.0.248

SMTP - Port: 465

POP3 / SMTP Anwendung: TLS

LDAP (ECS)

Server: 10.0.0.250

Port: 636

SSL: SSL

Ablaufdatum Stammzertifikat

Ablaufdatum : 07.08.2023 15:14:04

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/
importiert werden.

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 und dort validiert.
- EVIDENT Programmversion ab 6.05.
- 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.

Aktivierung EVIDENT Zertifikatsverwaltung (ECS)

Nach Anwahl der Zertifikats-Einstellungen öffnet sich ein Dialogfenster. Dort beginnen Sie im oberen Teil per Klick auf die Schaltfläche

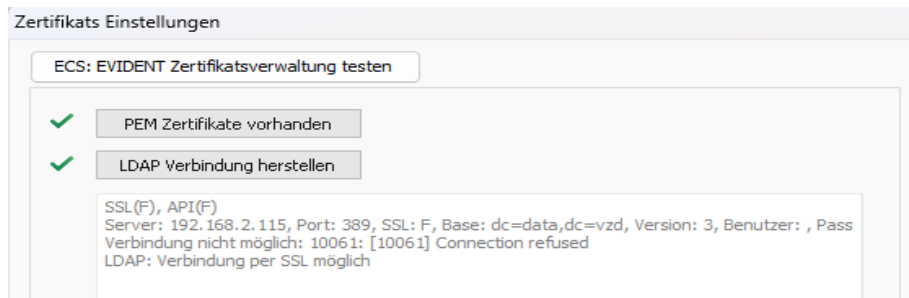
ECS: EVIDENT Zertifikatsverwaltung testen

Damit wird geprüft, ob der EVIDENT Cert Store (ECS) verwendet werden kann.

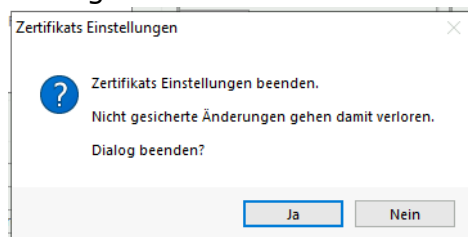
Im Erfolgsfall erkennen Sie das positive Ergebnis an den beiden grünen  Haken vor den Anzeigen PEM Zertifikate vorhanden und LDAP Verbindung



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 Firewallinstellungen 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



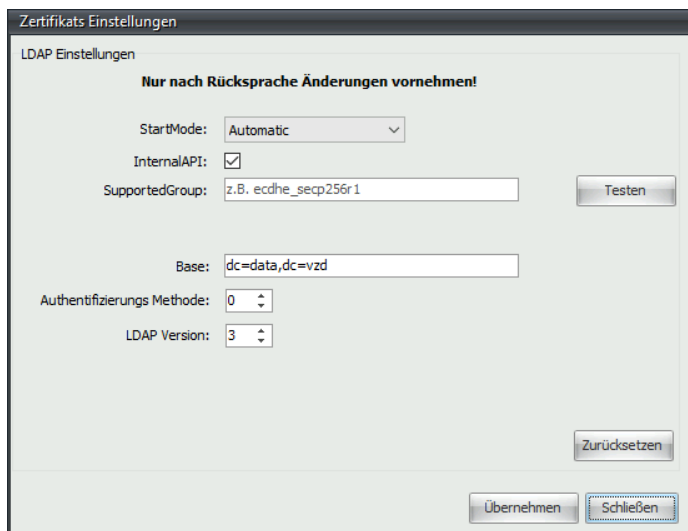
Konnte bereits beim Anklicken des Testen Buttons keine Verbindung hergestellt werden, erhalten Sie eine Fehlermeldung.



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



Nach Anklicken des Zahnrad-Symbols erscheint folgendes Fenster:



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

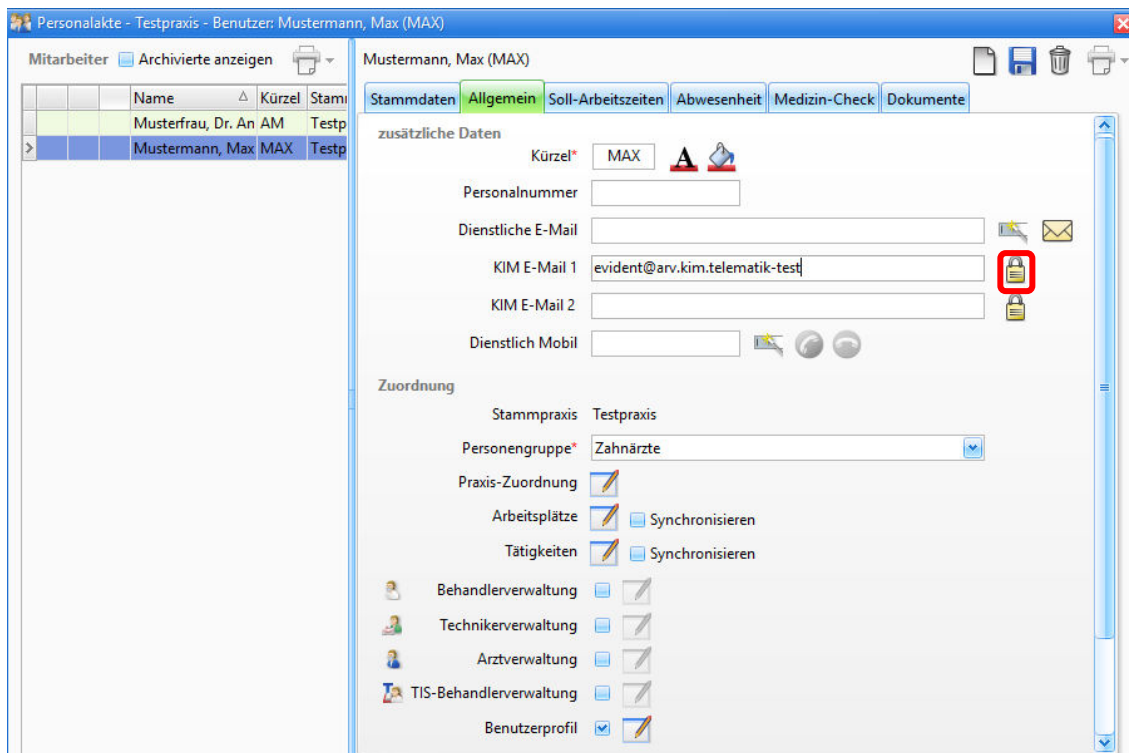




Ergänzen der Arztdaten liegt Ihnen vor oder Sie erhalten es von uns bei der Installation.

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: _____



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.

KIM Benutzereinstellungen für Mailaccount evident04@arv.kim.telematik-test

KIM E-Mail	<input type="text" value="evident04@arv.kim.telematik-test"/>	<input checked="" type="checkbox"/>			
Kennwort	<input type="password" value="*****"/>				
POP3 Anmeldename	<input type="text" value="evident04@arv.kim.telematik-test#mail.arv.kim.telematik-test:995"/>			Suffix	<input type="text"/>
SMTP Anmeldename	<input type="text" value="evident04@arv.kim.telematik-test#mail.arv.kim.telematik-test:465"/>			Suffix	<input type="text"/>
Identifikator	<input type="text" value="PRAXIS#EVIDENT#ANMELDUNG01"/>				

Ausfüllhinweise **KIM E-Mail Test für evident04@arv.kim.telematik-test**

Empfang erfolgreich durchgeführt.
Die Nachricht wurde in der KIM-Verwaltung im Ordner "Posteingang" gespeichert.

POP3: evident04@arv.kim.telematik-test#mail.arv.kim.telematik-test:995#PRAXIS#EVIDENT#ANMELDUNG01
SMTP: evident04@arv.kim.telematik-test#mail.arv.kim.telematik-test:465#PRAXIS#EVIDENT#ANMELDUNG01

Der Versand und Empfang wurde erfolgreich durchgeführt. Sie können jetzt die Einstellungen für eine erleichterte Einrichtung zwischenspeichern.

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-Fachdiensteanbieter: 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

Handling der Zertifikate

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.

1. Handling Serverzertifikate

Das Erstellen der Serverzertifikate ist abhängig vom jeweiligen Konnektormodell (KoCoBox, Rise, Secunet).

Konkret bedeutet dies, dass es Sache des jeweiligen **DVOs** ist sich mit dem Ablauf der Zertifikatserstellung vertraut zu machen, um diese erledigen zu können. Im Konnektor Manager (KM) von EVIDENT lässt sich das Server-Zertifikat dann direkt importieren. Näheres dazu lesen Sie unter Punkt 2.

Wichtiger Hinweis: Aufgrund einer Vorgabe des Bundesamtes für Sicherheit und der Bundesnetzagentur stellt die Telematik-Infrastruktur (TI) ihren Verschlüsselungsalgorithmus von RSA (Rivest-Shamir-Adleman) auf ECC (Elliptic Curve Cryptography) um. Mit dieser Migration soll das Sicherheitsniveau und die Effizienz der Systeme verbessert werden.

Damit, dass ECC-Zertifikate zum Standard im deutschen Gesundheitswesen werden, geht einher, dass dabei grundsätzlich **ECC NIST-Zertifikate** einzusetzen sind.

Die Gematik GmbH hat ihre Authenticator-Anwendung nämlich so konzipiert, dass sie ECC NIST-Zertifikate unterstützt, während die Unterstützung für sogenannte Brainpool-Kurven aus den Spezifikationen entfernt werden wird.



Aus diesem Grund ist bei Neueinrichtungen und Umrüstungen **grundsätzlich** bei allen Konnektoren das **ECC-Zertifikatsverfahren** einzurichten. **RSA-Konnektoren mit den bisherigen RSA-Clientzertifikaten sind ab 01.01.2026 nicht mehr einsetzbar.** Lediglich Arzt- und Praxisausweise mit RSA-Verschlüsselung können übergangsweise noch bis 30.06.2026 weiter verwendet werden.

Diese Fristverlängerung nur für die Ausweise wurde kurzfristig im November 2025 beschlossen.

Damit der Start zum Jahreswechsel 2025/2026 möglichst reibungslos erfolgt, kann ein letzter Check hilfreich sein: Ist der Konnektor ECC-fähig? Sind die Updates für das PVS und den KIM-Dienst installiert? Auch ein Blick auf den Arzt- und den Praxisausweis ist wichtig. Denn sollte das Gültigkeitsdatum demnächst ablaufen, ist ein rascher Tausch schon vor dem 1. Juli 2026 notwendig.

2. Zertifikate in den Konnektor Manager (KM) importieren und validieren

Nachdem die erforderlichen Zertifikate erzeugt wurden, 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:

Informationen | Log | Konnektor-Statusinfos | **Einstellungen** | Zertifikate

Einstellungen bearbeiten

Mode Online Check: Always	Startparameter & Zertifikat Informationen	vorhandene Zertifikate
Konnektor: On/Offline: Online		
Konnektor Verbindung: TLS mit Client-Zertifikat	<input checked="" type="checkbox"/> Autostart nach (Sek.): 5	Client / Konnektor
SIS: SIS im Konnektor deaktiviert	<input checked="" type="checkbox"/> EVIDENT automatisch starten	Client.Key / Konnektor Schlüssel
mandant-wide allgemein <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Automatische PIN Eingabe SMC-B Karten	Server / Aussteller
mandant-wide GCT <input type="checkbox"/>	Benutzername: EVIDENT	DIFFIE-HELLMAN
	Kennwort: *****	

Um den Dienst-Verzeichnisdienst (DVD) per **HTTPS** statt http vom Konnektor zu beziehen, ist es erforderlich den Konnektor zu bearbeiten. Hier nochmal die Stelle im KM.



Konnektor bearbeiten

Name:

HTTPS: IP: Port:

Benutzername:

Kennwort:

Zum Import bzw. zur Validierung der Zertifikate wechseln Sie auf die separate **Registerseite Zertifikate**.

Informationen | Log | Konnektor-Statusinfos | Einstellungen | **Zertifikate**

Server / Aussteller

SERVER.PEM Zertifikat ist validiert

Client / Konnektor - Client.Key / Konnektor Schlüssel

CLIENT.PEM Zertifikat ist validiert
CLIENTKEY.PEM Zertifikat ist validiert
ECC verschlüsselt

EVIDENT Zertifikat

EVIDENT.PEM validiert
ID: 19B9DC4F65F883134FA13C1689FCB265
Datum plausibel

3. Server Zertifikate importieren

Das Register Zertifikate ist von oben nach unten in drei Bereiche unterteilt. Los geht es mit dem Bereich Server / Aussteller.

Informationen | Log | Konnektor-Statusinfos | Einstellungen | **Zertifikate**

Server / Aussteller

SERVER.PEM nicht validiert
ID: 829ADBEA0B5668BDD176A33D8CC2C601
FP: SHA1 Fingerprint=F0:D5:56:B3:5E:74:12:58:54:43:2D:7A:85:20:C9:2



Per Klick auf die **Schaltfläche vom Konnektor importieren** verzweigen Sie in folgendes Fenster:

Zertifikat von Konnektor ermitteln

Konnektor TLS ...

Nach Eingabe der URL oder der IP-Adresse des Konnektors lässt sich das Zertifikat ermitteln und speichern.

4. Client Zertifikate importieren

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

Nach Öffnen der P12 Datei erscheint die Passwortabfrage:

.P12 Passwort

Passwort:

Es ist das gesicherte und gemerkte Passwort einzugeben, das beim Generieren des Zertifikats über die Konnektoroberfläche generiert wurde.

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

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

Startparameter & Zertifikat Informationen

Autostart nach (Sek.): 5

EVIDENT automatisch starten

Automatische PIN Eingabe SMC-B Karten

Benutzername :

vorhandene Zertifikate

- KONNEKTOR
- KONNEKTOR Schlüssel
- AUSSTELLER
- DIFFIE-HELLMAN

Importierte Zertifikate, egal ob Server- oder Klient-Zertifikat, werden automatisch validiert. Dies gilt unabhängig davon von welchem Konnektor diese stammen.

5. RISE Klient Zertifikat importieren

Grundsätzlich ist der Ablauf identisch wie zuvor für secunet beschrieben.

Das heißt, das Klient Zertifikat, das vom RISE exportiert wird, ist ebenfalls eine .P12 Datei, insofern ist die Vorgehensweise des Klient-Zertifikatimports die gleiche wie unter Punkt 4 ausgeführt.



6. KoCoBox Klient Zertifikat importieren

Auch für die KoCoBox ist das Klient Zertifikat auf dem gleichen Weg in den KM zu importieren. D. h. Sie können sich wiederum an Punkt 4 orientieren.

Im Falle der KoCoBox soll nochmals auf die Gegebenheit hingewiesen werden, dass **grundsätzlich ECC NIST-Zertifikate** zu verwenden sind, da ECC-Zertifikate auf Basis von **BrainPool-Kurven** seitens der gematik **nicht vorgesehen** sind. Um diese Anforderung zu erfüllen, müsste für die betroffene Praxis ein neues Konnektor-Client-Zertifikat auf Basis der NIST-Kurve erstellt werden.

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 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.