EPIKUR TIaaS Installation

Differenzanleitung

Kurzanleitung

Version 1
Stand: 05.09.2023

Inhaltsverzeichnis

Vorbereitung

1. EPIKUR Updaten – (Version: min. 23.3.0)
2. Admin-PIN vom Kartenterminal bereithalten
3. Kartenterminal Updaten (Version: **min. 3.8.2**)
4. Sudo/Admin-Passwort vom PC bereithalten
5. Für MacOS: Appstore-Passwort bereithalten
6. Mindestens macOS 12 erforderlich für Download von Wireguard aus AppStore
7. TIC herunterladen:

   Windows → https://client.rise-tiaas.de/installer/tiaas-client-installer_windows.exe

   macOS → https://client.rise-tiaas.de/installer/tiaas-client-installer_macos.dmg

Allgemeiner Hinweis zu mehreren Konfigurationspaketen

Ein Installationspaket kann mehrere Konfigurationspakete mit VPN-Zugängen und PVS-Zertifikaten enthalten. Es muss zu jedem Zeitpunkt sichergestellt werden, dass die Paktzuordnung von nur einem PC exklusiv genutzt wird. D.h. es sollte vor der Einrichtung festgelegt werden, welchem PC Paket 1, welchem PC Paket 2, etc. zugeordnet werden soll. Diese Zuordnung bitte dokumentieren!

In den nachfolgenden Schritten werden die Konfigurationspakete, VPN-Konfigurationen, etc. referenziert. Hierbei muss immer auf die oben beschriebene Zuordnung geachtet werden.

1 Abweichende Einstellungen bei TIC-Installation

1.1 Nur bei MacOS: Wireguard installieren und konfigurieren

Bitte den WireGuard vor der TIC-Installation einrichten!

1.1.1 Vorbereitung

1) Den Ordner "TIC-Installationspaket_Epikur-XXXX" entpacken.
   (Ausgewähltes) Konfigurationspaket entpacken (Bitte
2) **Allgemeiner Hinweis zu mehreren Konfigurationspaketen** beachten).

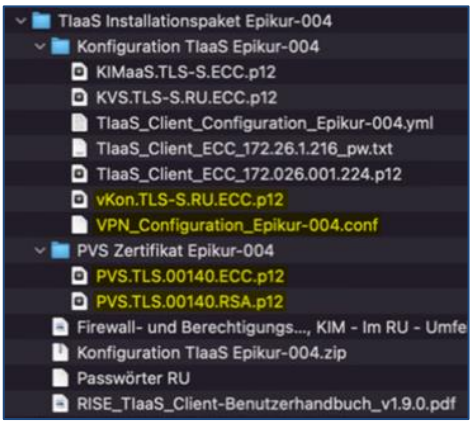


Abbildung 1- Aufbau Installationspaket

1.1.2 Installation von WireGuard

1) Laden Sie die App 'Wireguard' im Appstore herunter und installieren Sie diese.
2) Starten Sie die Wireguard-App.

1.1.3 Konfiguration von WireGuard

1) Klicken Sie auf: “Importiere Tunnel aus Datei”.

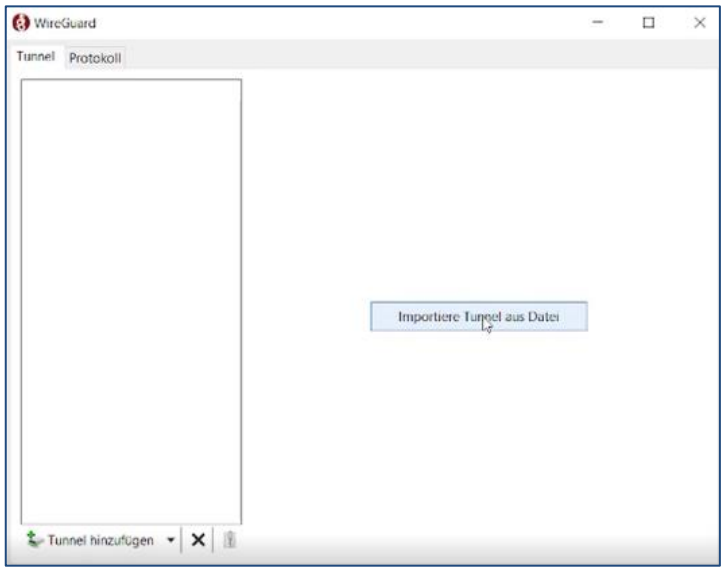


Abbildung 2- WireGuard - Konfiguration importieren

3) Datei VPN_Configuration_Epikur-xxx.conf öffnen (Aus dem in der Vorbereitung entpackten Verzeichnis).

4) Nach Import der Datei den Tunnel bearbeiten (siehe Abbildung 3).

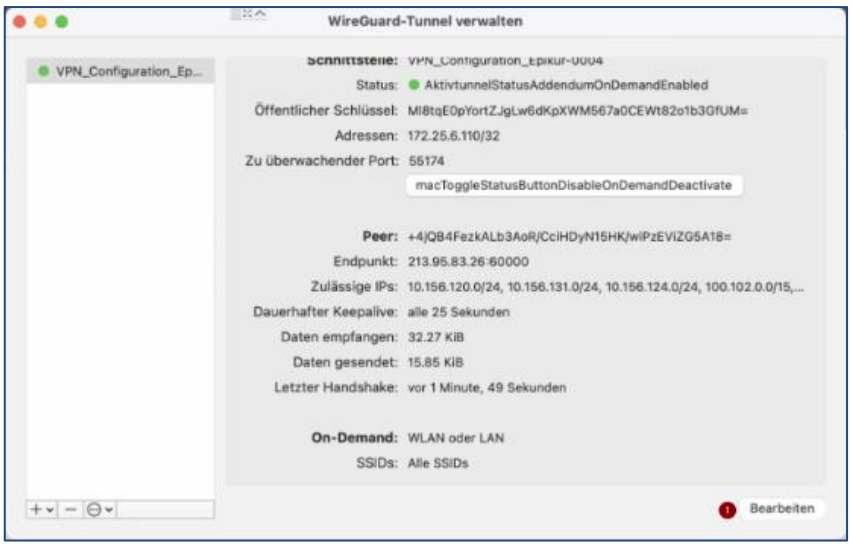


Abbildung 3- WireGuard mit aktiviertem On-Demand

5) Bitte das SUDO-Passwort eingeben.
6) Setzen Sie den Hacken bei “On-Demand” LAN sowie WLAN und speichern Sie hiernach (siehe Abbildung 4).

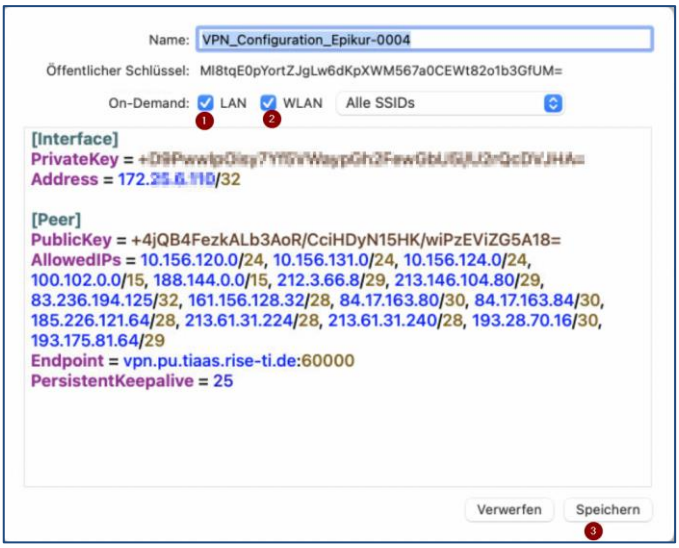


Abbildung 4- WireGuard-Konfiguration bearbeiten

Hinweis: Hiernach sieht der Zustand des Buttons “Aktivieren” so aus, wie in Abbildung 3 dargestellt. Der Wireguard startet jetzt automatisch, wenn eine LAN oder WLAN-Verbindung aktiv ist.

1.2 TIC - Installationsoptionen anpassen

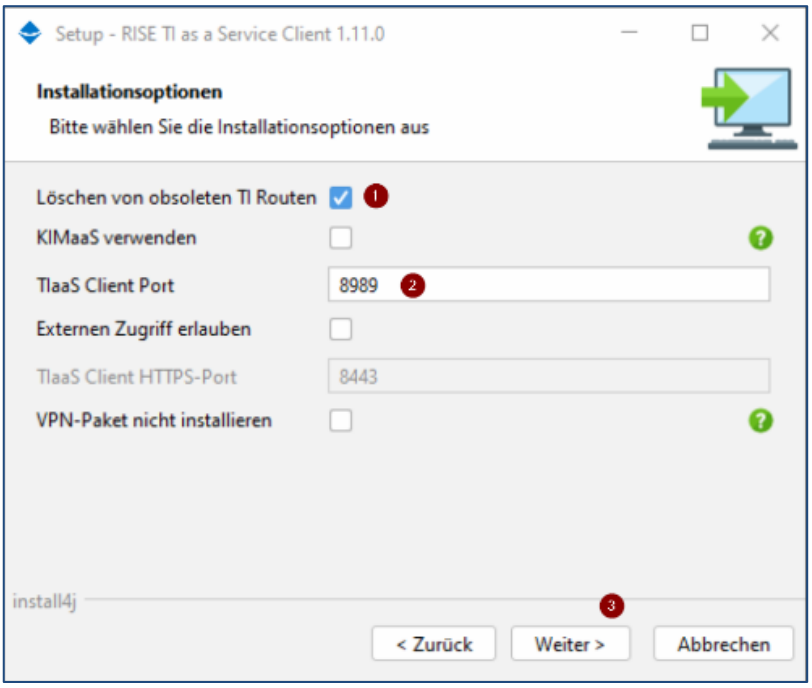


Abbildung 5- Einstellungen für Windows

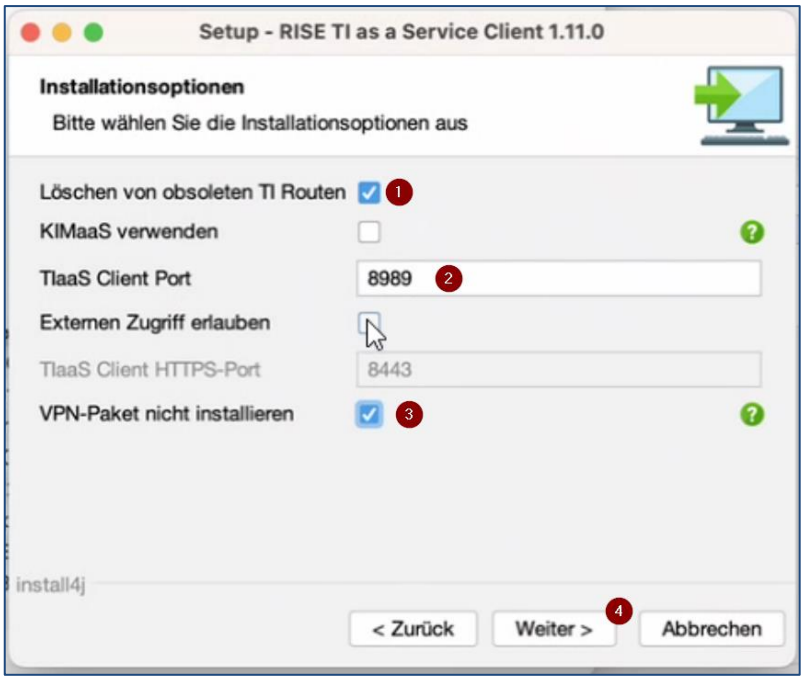


Abbildung 6- Einstellung für MacOS

7) Setzen Sie den Hacken bei „Löschen von obsoleten TI Routen“.
8) Passen Sie den TIaaS Client Port an zu: 8989.

9) Bei Windows: setzen Sie keinen Hacken bei „VPN-Pakete nicht installieren“ (siehe Abbildung 5).
10) Bei MacOS: setzen Sie den Hacken bei „VPN-Pakete nicht installieren“ (siehe Abbildung 6).

Hinweis: Bei MacOS: Wenn nach Zugriffsrechten auf "System Events" gefragt wird, diese bitte erlauben.

2 EPIKUR Einstellungen

2.1 Umstellung auf Rechenzentrum

1) Loggen Sie sich als Administrator ein und rufen Sie die Konnektor-Einstellungen auf.
2) Stellen Sie den Konnektor-Typ auf "EPIKUR-Rechenzentrum" um.
3) Setzen Sie die Konnektor-Adresse auf "konnektor.pu.tiaas.rise-ti.de" (Wird automatisch vorbefüllt).

2.2 Import des Installationspakets

2.2.1 Automatischer Import

Hinweis: Sollte ein automatischer Import nicht möglich sein, fahren Sie mit dem Abschnitt 2.2.2 fort.

1) Durch Klick auf “Import Rechenzentrum” kann der automatische Import gestartet werden.

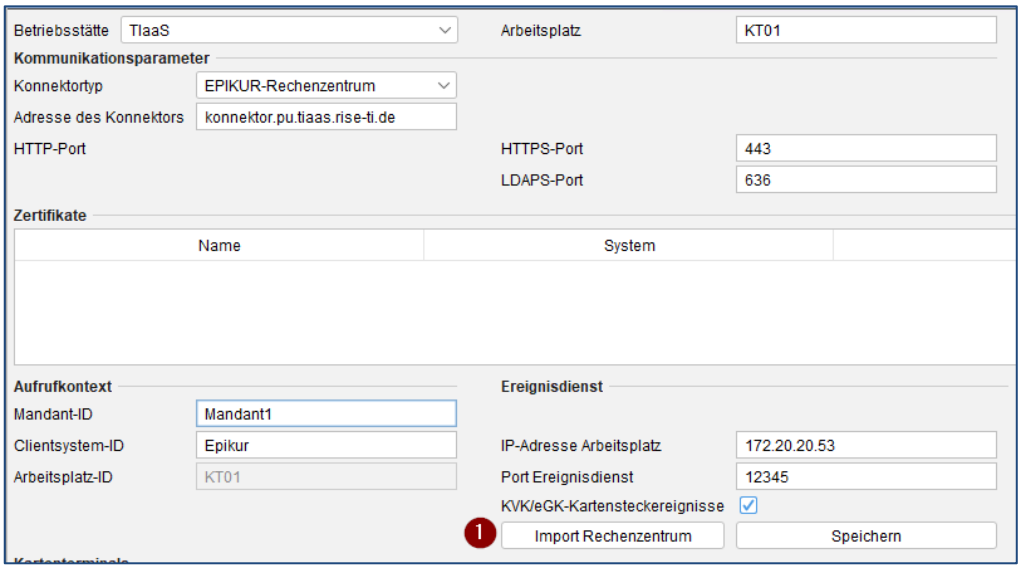
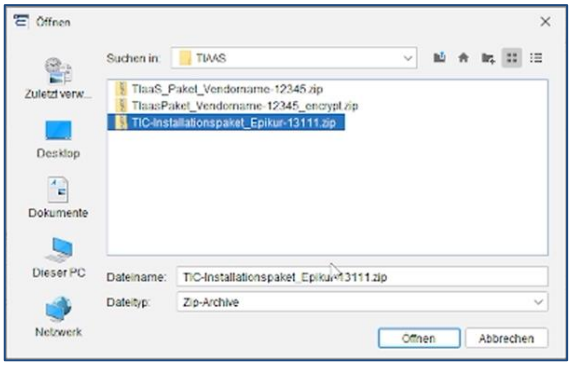
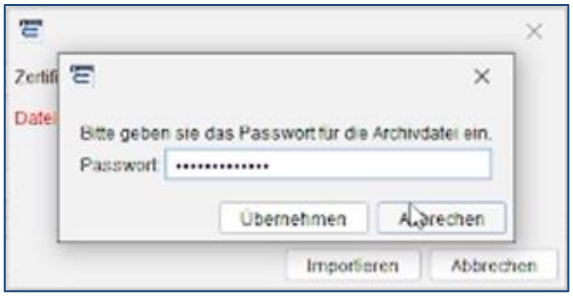


Abbildung 7 - EPIKUR Automatischer Import

2) Wählen Sie nun das verschlüsselte und nicht entpackte Installationspaket als ZIP-Datei - "TIC-Installationspaket_Epikur-XXXX.zip" aus.



3) Geben Sie nun das Passwort zur Entschlüsselung ein und bestätigen Sie dies mit „Übernehmen"



Bitte nur die gewünschten Daten auswählen (Bitte

4) **Allgemeiner Hinweis zu mehreren Konfigurationspaketen** beachten).
   a. Es wird je Installation der Ordner "PVS_Zertifikate…" und "TIC_Konfigurationspaket…" benötigt

b. Sollte nur ein Konfigurationspaket in der ZIP-Datei enthalten sein, werden die Ordner “PVS_Zertifikate…” und “TIC_Konfigurationspaket…” angezeigt.

Hinweis:

Sind mehrere Installationspakete enthalten, werden die Ordner mehrmals angezeigt und sind mehrmals wählbar - dann sind die Ordner mit voranstehender Zahl "XX" nummeriert → z.B. 01 für das erste Installationspaket (siehe Screenshot).

5) Anschließend klicken Sie auf “Importieren”.
   Die Zertifikate werden importiert. Die IP-Adresse des Arbeitsplatzes wird ebenfalls automatisch übertragen.
6) Setzen Sie den Haken bei „KVK/eGK-Kartensteckereignisse“.

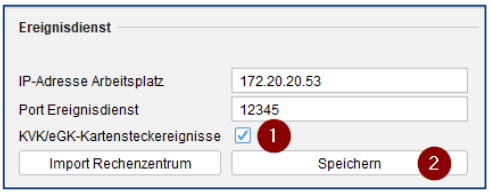


Abbildung 8- Ereignisdienst konfigurieren

2.2.2 Manueller Import

Sie müssen neue Zertifikate (RSA-Client-Zertifikat, ECC-Client-Zertifikat, ECC-Konnektor-Zertifikat) aus dem entpackten Installationspaket einspielen.

- Vor dem Import der neuen Zertifikate sind ggf. die alten Zertifikate zu löschen.
- Für jedes Zertifikat sollten Sie bei der Tabelle „Zertifikate“ auf Hinzufügen klicken.

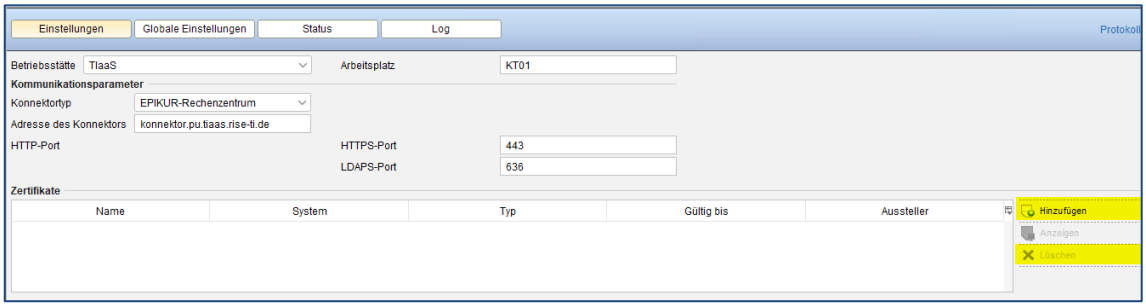


Abbildung 9- EPIKUR Zertifikate hinzufügen

Beim Zertifikatsimport ist eine Passwort-Eingabe notwendig. Die notwendigen Passwörter liegen jeweils neben den Zertifikatsdateien in einer .txt-Datei (siehe Abbildung 10).

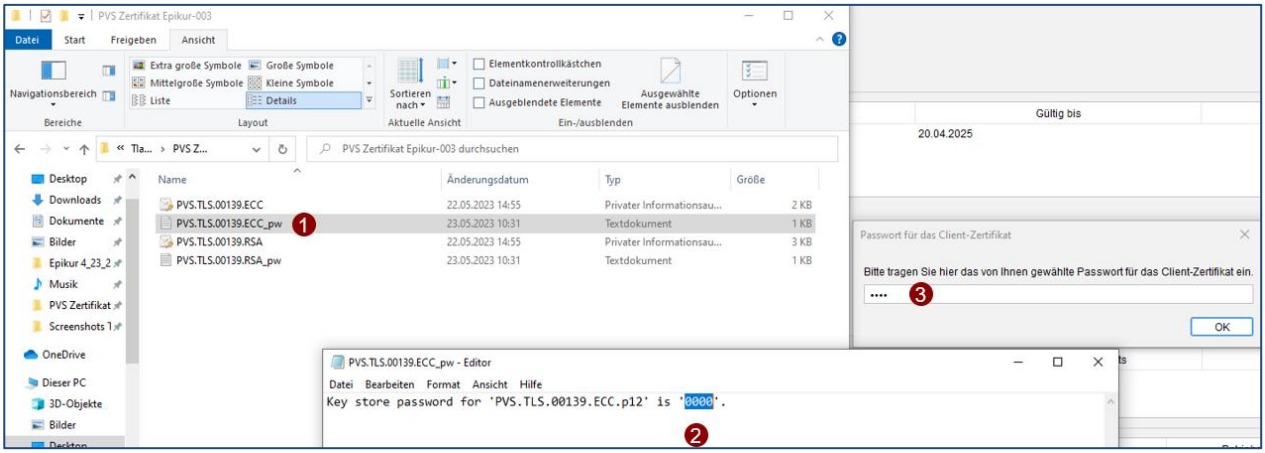
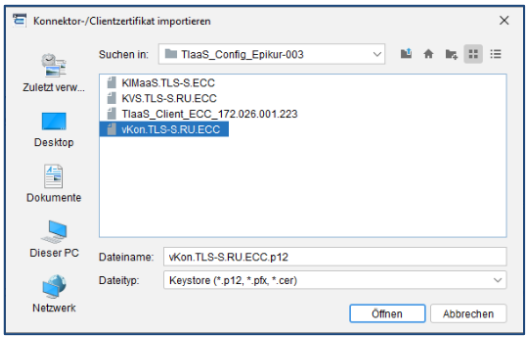


Abbildung 10- EPIKUR Import Zertifikat

Für das Konnektor-ECC-Zertifikat wählen Sie aus dem entpackten Ordner "TIaaS_Config_Epikur-XXXX" (welcher in dem entpackten Ordner "TIC-Installationspaket_Epikur-XXXX" liegt) das: vKon.TLS-S.PU.ECC.p12 Zertifikat aus (Bitte 1) **Allgemeiner Hinweis zu mehreren Konfigurationspaketen** beachten). Das Passwort lautet: „**000000**"



Wählen Sie das
- Client-ECC-Zertifikat (PVS_ECC_client-XXXXX.konlan.p12) und

- Client RSA-Zertifikat (PVS_RSA_client-XXXXX.konlan.p12)
aus dem Ordner "PVS Zertifikat Epikur-XXXX" (welcher in dem entpackten Ordner "TIC-Installationspaket_Epikur-XXXX" liegt) aus und importieren Sie dieses (Bitte
2) **Allgemeiner Hinweis zu mehreren Konfigurationspaketen** beachten).

Nachdem die Kommunikationsparameter eingestellt wurden und alle drei Zertifikate importiert sind, kann auf Speichern geklickt werden. Es sollte nun eine Verbindung zum Konnektor und dem/der Kartenterminal/-s aufgebaut werden können.

2.3 Ereignisdienst konfigurieren

Die VPN-Config-Datei "VPN_Configuration_Epikur-XXX.conf" aus dem entpackten Ordner "TIaaS_Config_Epikur-XXXX" (welcher in dem entpackten Ordner "TIC-Installationspaket_Epikur-XXXX" liegt) mit dem Texteditor oder TextEdit öffnen (Bitte

1) **Allgemeiner Hinweis zu mehreren Konfigurationspaketen** beachten).
2) Kopieren Sie die IP unter [Interface] -> Address (siehe Abbildung 11)
Hinweis: NUR IP und nicht Subnetzmaske!

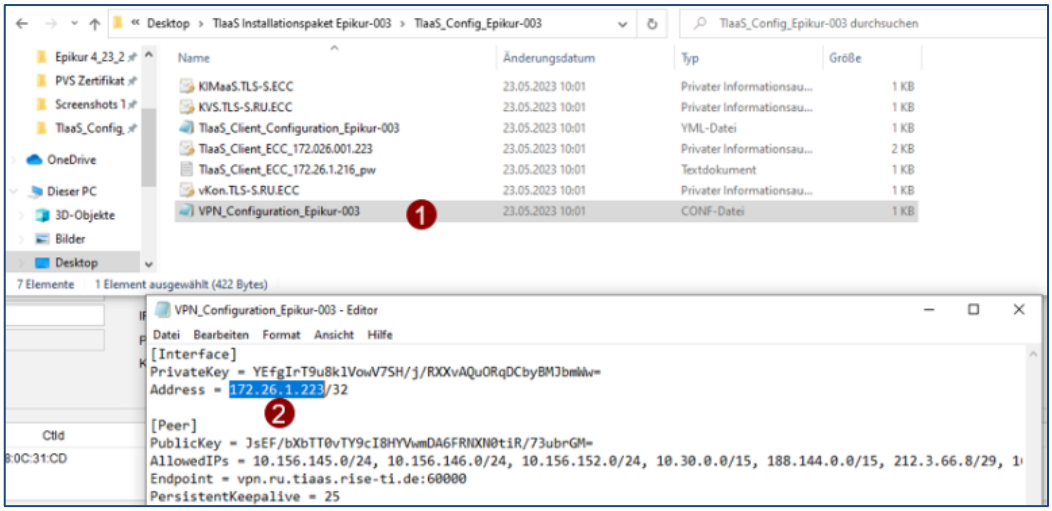


Abbildung 11 - VPN Konfigurationsdatei

3) Navigieren Sie in EPIKUR zum Ereignisdienst. Tragen Sie unter: „IP-Adresse Arbeitsplatz" die kopierte IP ein.
4) Setzen sie den Haken bei „KVK/eGK-Kartensteckereignisse".

2.4 Kartenleser hinzufügen

1) Loggen Sie sich in EPIKUR als Administrator aus und melden Sie sich nun als Nutzer an.
2) Klicken Sie auf Programmeinstellungen → Geräte → KLG und Drucker (Siehe Abbildung 12 – Schritt 2).

3) Ggf. das alte KT aus der Liste löschen (Bitte Bezeichnung und Kürzel notieren).
4) Klicken Sie auf Kartenleser suchen (In Toolbar) um KT neu hinzuzufügen (Schritt 3).
5) Ggf. Konfiguration des alten KTs (Bezeichnung und Kürzel) auf das neue KT übertragen anpassen.
6) Klicken Sie auf OK und starten Sie EPIKUR neu (Schritt 4).

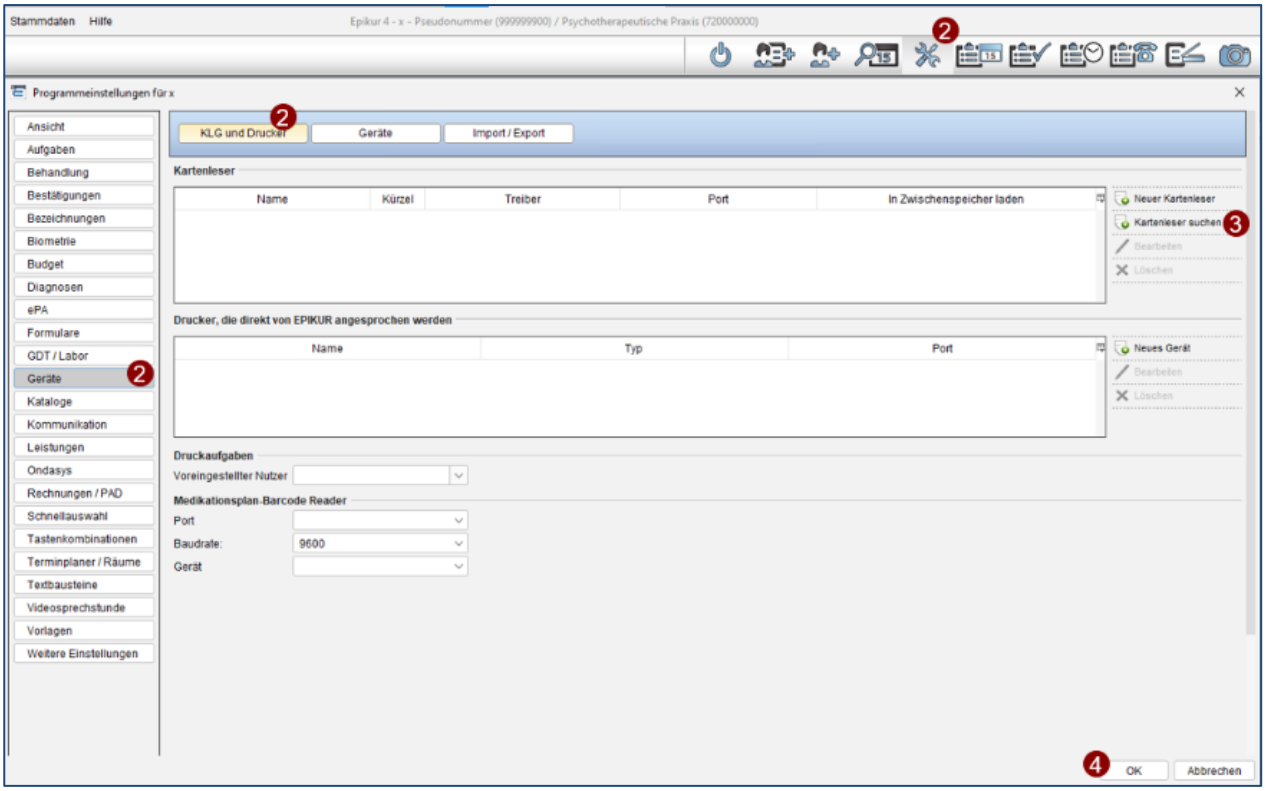


Abbildung 12- EPIKUR Kartenlesegerät hinzufügen

2.5 PIN-Eingabe und Verbindungstests

2.5.1 PIN-Eingabe

Hinweis: TI-Ampel ist beim RZK aktuell deaktiviert und zeigt keine Farben an, was aber nicht auf Fehler hindeutet. Nach einem Klick auf die TI-Ampel kann weiterhin der Status eingesehen werden.

Nach einem EPIKUR-Neustart und Nutzerlogin, sollten Sie aufgefordert werden, die SMC-B-PIN einzugeben um die Karte freischalten.

Hinweis: SMC-B-PIN muss nun nach jedem Start des PCs/Laptops eingegeben werden, da der TIC sich jedes Mal neu mit dem Rechenzentrumskonnektor verbindet, wodurch eine neue Freischaltung erforderlich wird.

2.5.2 Verbindungstest

1) Eingeloggt als Nutzer, über “Hilfe” → “Info” → "Verbindungen prüfen" überprüfen, ob alle benötigten Verbindungen zur Verfügung stehen.
2) Im KV-Bereich via Webbrowser anmelden
3) KIM-Nachricht an die Adresse des Kunden versenden (Nachricht an sich selbst - wenn Account vorhanden)
    a. Falls fehlerhaft und Arvato Postfach: Die Konfiguration erneut in das KIM-CM übertragen (Admin → KIM → Konfiguration übertragen)
    b. Falls fehlerhaft und externes Postfach: Konfiguration im entsprechenden KIM-CM anpassen lassen und den Kunden an den Anbieter verweisen.
4) VSDM testen (wenn Karte vorhanden): Karte stecken → prüfen, ob das Kartensteckereignis angezeigt und die Karte kann eingelesen werden kann