RISE TI-Client

Bedienungsanleitung

Autor: **RISE**

Version: **2.5.3**

Stand: **23.05.2025**

Referenzierung: **RISE-TIGW-CLIENT-BED**

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektentwicklung GmbH

www.rise-world.com • welcome@rise-world.com

Änderungshistorie

Version	Datum	Autor	Änderungen
2.5.3	23.05.2025	RISE	Kapitel Konfiguration für Remote PIN+ angepasst
2.5.1	05.05.2025	RISE	Kapitel Benutzerspezifische Änderungshistorie hinzugefügt, Kapitel PIN+ Ladeindikator bleibt dauerhaft aktiv hinzugefügt, Abschnitt Werksreset des vKonnektors hinzugefügt, Abschnitt Remote PIN+ angepasst, Abschnitt Installationsprozess Docker angepasst, Allgemeine Richtlinien für Portauswahl in Kapitel Vorbereitung hinzugefügt, Format für Internetadressen angepasst
2.5.0	24.04.2025	RISE	Webbrowser Versionen aktualisiert, Betriebssystem Versionen aktualisiert, Kapitel Einleitung angepasst, Kapitel Kartenterminal-Proxy angepasst, Kapitel Vorbereitung angepasst, Kapitel Installationsprozess angepasst, Kapitel Remote PIN+ Konfiguration angepasst, Kapitel RISE KIM-Clientmodul hinzugefügt, Kapitel Anpassen des WireGuard-ListenPorts hinzugefügt, Kapitel Problemlösungen (Troubleshooting) hinzugefügt, Kapitel TLS-Serverzertifikat des TI-Clients hinzugefügt, Abschnitt Anpassen des WireGuard-ListenPorts hinzugefügt, Abschnitt TLS-Serverzertifikat hinzugefügt, Abschnitt Anmeldedaten hinzugefügt, Abschnitt Anpassen der Vertraulichkeitsstufe des öffentlichen Schlüssels hinzugefügt, Screenshots angepasst, Umstellung auf neues Handbuch-Design
2.4.0	13.03.2025	RISE	Kapitel Betriebssystem angepasst, Kapitel Bezug des Public Keys hinzugefügt, Kapitel Docker angepasst, Linux Installationsprozess-Links angepasst, Kapitel Docker hinzugefügt, Kapitel Event-Proxy hinzufügen angepasst, RU-Handbuch erstellt, Kapitel Telemetrie hinzugefügt, Screenshots angepasst, Services starten Beschreibung hinzugefügt, KT Firmware angepasst, Abschnitt Netzwerkeinstellungen angepasst
2.3.1	03.12.2024	RISE	Pingbeschreibung hinzugefügt
2.3.0	05.11.2024	RISE	macOS Versionen aktualisiert, Webbrowser Versionen aktualisiert, Log Levels Refactoring, Startinformationen macOS hinzugefügt, TIC Port Option hinzugefügt, Remote PIN+ hinzugefügt
2.1.1	23.09.2024	RISE	TI-Client unter Linux in Betrieb nehmen, Server Port ändern, Hinweis auf Notwendigkeit von der Einrichtung des vKonns im TI-Client
2.1.0	10.09.2024	RISE	KT-IP in der Firewall freischalten hinzugefügt, Port Ranges angegeben, Cert Check Hinweis angepasst, Kapitel 'Clientsysteme' aus dem HSK Handbuch übernommen und angepasst, Konfigurationsseite beschrieben
2.1.0-rc.1	15.07.2024	RISE	Screenshots erneuert, Ersetzen von "HSK-Client" durch "TI-Client", Beschreibung des GUIs, Firewall Infos geupdatet

2.1.0-alpha	21.06.2024	RISE	Beschreibung des TI-Client GUIs, Updating OS- und Browser-Versionen, allgemeine Korrekturen
2.0.1	06.05.2024	RISE	Erweiterung Beschreibung TRACE Loggging, Erweiterung Hinweis zur Installation von Updates, Korrektur Wordings
2.0.0	05.04.2024	RISE	Beschreibung des Zertifikats-CLI-Utilities, Allgemeine Präzisierungen, Korrektur Wordings
2.0.0-rc.2	22.12.2023	RISE	Prüfung der Server Zertifikate
2.0.0-rc.1	07.12.2023	RISE	Initiale Erstellung

Inhaltsverzeichnis

1 Einleitung

Diese Bedienungsanleitung beschreibt den *RISE Telematikinfrastruktur-Client*, kurz *RISE TI-Client*. Die Applikation dient zur Kommunikation mit dem TIaaS Rechenzentrum (RZ) und den dort zur Verfügung stehenden vKonnektoren (*HSK-Instanzen*).

Der TI-Client ist eine eigenständige Softwarekomponente, welche in der Einsatzumgebung des sogenannten Leistungserbringers/der Leistungserbringerin (LE) verwendet wird. Über einen mitinstallierten VPN-Client verbindet sich die Software zu einem remote erreichbaren RISE vKonnektor und kann so seine Funktionalität nutzen. Dazu muss der/die LE eine den Anforderungen entsprechende korrekte und sichere Betriebsumgebung bereitstellen.

Diese Bedienungsanleitung enthält wichtige Informationen zur sicheren Installation, zum operativen Betrieb und zur Deinstallation. Lesen Sie die Bedienungsanleitung sorgfältig durch, bevor Sie die Software in den produktiven Einsatz bringen.

Diese Bedienungsanleitung wird vom Anbieter über einen sicheren Weg in der jeweils aktuellen Version zur Verfügung gestellt und richtet sich generell an Leistungserbringer, die RISE TI-Gateway nutzen und an die Administratoren im Speziellen.

> **Hinweis**
>
> Der TI-Client bietet Ihnen die Möglichkeit, das Handbuch in der jeweils aktuellen Version herunterzuladen. Gehen Sie dazu in der Benutzeroberfläche des TI-Clients unter dem Menüpunkt *Informationen* zum Reiter *Benutzerhandbuch*.

Bei den in diesem Dokument verwendeten Bildern handelt es sich um Symbolbilder, die nur zur Veranschaulichung dienen. Die Darstellungen können sich, abhängig von der verwendeten Betriebssystem-, Software- und Browser-Version, unterscheiden.

1.1 Benutzerspezifische Änderungshistorie

Dieses Kapitel enthält Änderungen, die für Benutzer relevant sind und ggf. aktive Anpassungen erfordern. Im Gegensatz zur allgemeinen Änderungshistorie umfasst diese Liste benutzerspezifische Auswirkungen, wie bspw. geändertes Verhalten, Bedienung oder Konfiguration.

Version	Änderungen
2.5.1	Der TI-Client ist nun unter *https://localhost:<PORT>* und nicht mehr unter *http://localhost:<PORT>* erreichbar (siehe Abschnitt 4.3).
	Die URL des APT-Repository für die Installation des TI-Clients unter Linux wurde geändert (siehe Abschnitt 2.6.2.1).
	Einführung eines TI-Client-Service-Benutzers, mit automatischer, täglicher Passwortrotation. Die manuelle Änderung des vKonnektor-Benutzer-Passworts alle 60 Tage entfällt. Sollte das vKonnektor-Benutzer-Passwort bereits abgelaufen sein, muss der vKonnektor im TI-Client neu eingerichtet werden. Ansonsten findet die Migration automatisiert statt (siehe Abschnitt 3.5.1.3).

2 Installation

In diesem Abschnitt werden die Systemvoraussetzungen, der Installationsprozess sowie Vorgaben und Hinweise für die Installation beschrieben.

2.1 Systemvoraussetzungen

Der TI-Client besitzt einige Anforderungen, welche der/die LE durch Komponenten, das lokale Netzwerk oder die Betriebsumgebung erfüllen muss, um einen vollständigen, ordnungsgemäßen und sicheren Betrieb zu ermöglichen.

2.1.1 Hardware

Um die Funktionalität des TI-Clients nutzen zu können, müssen entsprechende Kartenterminals und Chipkarten gemäß Bedienungsanleitung des RISE High-Speed-Konnektors bereitgestellt werden.

2.1.2 Netzwerkeinstellungen

Die nachfolgende Information zu Netzwerkeinstellungen betrifft nur Windows-Betriebssysteme. Unter macOS und Linux werden durch den Installer keine Netzwerkeinstellungen vorgenommen.

Im Zuge der Installation des TI-Clients unter Windows werden automatische Ausnahmen für eingehende Verbindungen in der internen Firewall des Betriebssystems hinzugefügt.

Die Ausnahmen lauten wie folgt:

- Für die IP-Adresse des vKonnektors wird eine *TCP*- und eine *UDP*-Ausnahme hinzugefügt.
- Für die Kartenterminal-Ports, welche während der Installation festgelegt werden, wird eine *TCP*- und eine *UDP*-Ausnahme hinzugefügt.

> **Hinweis**
>
> Werden in Ihrem Netzwerk weitere Firewalls verwendet, die die Funktion des TI-Clients beeinflussen, wenden Sie sich an Ihren Netzwerkadministrator.

> **Wichtig**
>
> Nach der Deinstallation werden alle Ausnahmen, welche während der Installation angelegt worden sind, wieder entfernt. Zusätzliche Ausnahmen müssen händisch entfernt werden.

2.1.3 Betriebssystem

Aktuell unterstützt der TI-Client folgende Betriebssysteme:

- Windows 10 (64-bit) 22H2
- Windows 11 (64-bit) 24H2
- Windows Server 2022
- Windows Server 2025
- macOS 14 (Sonoma)
- macOS 15 (Sequoia)
- Ubuntu 22.04.4 LTS Server
- Ubuntu 24.04.2 LTS Server
- Docker ab Version 27.2.1 unter Linux mit Architektur *AMD64*

2.1.4 Webbrowser

Für die korrekte Nutzung des TI-Clients wird aktuell die Verwendung des Clients mit folgenden Webbrowsern empfohlen:

- Google Chrome ab Version 134.0.6998.118
- Microsoft Edge ab Version 134.0.3124.51
- Mozilla Firefox ab Version 136.0.2
- Apple Safari ab Version 18.3

2.1.5 Korrekte Systemzeit

Für einen fehlerfreien Betrieb ist sicherzugehen, dass die Systemzeit korrekt eingestellt ist. Es wird empfohlen, das *Network Time Protocol* dafür zu verwenden. Sollte die Systemzeit nicht richtig eingestellt sein, kann die Richtigkeit der Zertifikatsprüfungen nicht gewährleistet werden.

2.1.6 Voraussetzungen für einen sicheren Betrieb

Zusätzlich zu den beschriebenen funktionalen Anforderungen muss auch die Sicherheit der Betriebsumgebung des TI-Clients gewährleistet und eingehalten werden. Daher sind vor jedem Start der Anwendung folgende sicherheitsrelevanten Vorgaben zu beachten und sicherzustellen:

- **Schutz des Netzwerks vor Angriffen:**
  Der/Die LE hat dafür Sorge zu tragen, dass das lokale Netzwerk gegen unbefugten Zugriff bzw. Nutzung geschützt ist. Des Weiteren müssen die verbundenen Systeme im Netzwerk immer auf dem aktuellsten Stand sein (regelmäßige Updates), um Sie gegen Schadsoftware zu schützen und somit auch das lokale Netzwerk.
- **Sichere Administration:**
  Der/Die LE muss dafür sorgen, dass administrative Tätigkeiten in Übereinstimmung mit der Produktdokumentation durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen geheim halten bzw. dürfen diese nicht an Unberechtigte weitergeben.
- **Schutz des privaten Schlüssels:**
  Der/Die LE muss dafür sorgen, dass der private Schlüssel, welcher sich in der Konfigurationsdatei (*.zip*-Archivdatei) und nach der Installation in der WireGuard-Konfigurationsdatei befindet, geheim gehalten wird. Der private Schlüssel wird zur Entschlüsselung von Daten als auch als Identifikation des LE verwendet. Bei Verlust oder Veröffentlichung des privaten Schlüssels ist umgehend Kontakt mit dem Support Ihres TI-Gateway-Anbieters über die E-Mail-Adresse *support@rise-ti.de* aufzunehmen, um den Schlüssel sperren zu lassen.
- **Schutz der Betriebsumgebung:**
  Es liegt in der Verantwortung des Benutzers, für eine sichere Betriebsumgebung zu sorgen und sicherzustellen, dass Daten geschützt bleiben, bspw. durch Installation von Betriebssystem-Updates, den Einsatz einer Firewall, Antiviren-Software usw. Die Maßnahmen müssen den aktuellen Stand der Technik erfüllen oder diesen übertreffen.
  Der TI-Client schreibt Logdateien, die eine Analyse der technischen Vorgänge erlauben. Der Benutzer muss durch geeignete Maßnahmen sicherstellen, dass diese Logdateien nur für autorisierte Personen zugänglich sind.
- **Installation von sicherheitsrelevanten Updates:**
  Im Falle von Sicherheitsaktualisierungen wird vom TI-Gateway-Anbieter unverzüglich eine aktualisierte TI-Client-Version zur Verfügung gestellt. Es liegt in der Verantwortung des Benutzers, die aktualisierte Version zeitnahe zu installieren.

2.1.7 Bezug des Public Keys

Zusätzlich zu den beschriebenen, funktionalen Anforderungen muss auch die Sicherheit der Betriebsumgebung des TI-Clients gewährleistet und eingehalten werden. Daher ist vor der Einrichtung der Anwendung folgende sicherheitsrelevante Vorgabe zu beachten und sicherzustellen:

Die Artefakte für Linux und das Docker-Image sind mit einem Schlüssel von *RISE* signiert. Um die Authentizität der Artefakte sicherzustellen, wird dringend empfohlen die Signaturen zu prüfen. Hierfür muss der öffentliche Schlüssel bezogen, verifiziert und eingerichtet werden.

2.1.7.1 Bezug und Verifizierung des öffentlichen Schlüssels:

1. Laden Sie den öffentlichen Schlüssel zum Verifizieren der Signatur herunter:

   ```
   $ curl -fsSLo rise-ti-client-pu.gpg https://client.ti-gateway.de/installer-tigw/gpg-pu/
   rise-ti-client-pu.gpg
   ```

2. Lassen Sie sich die Details des GPG-Schlüssels anzeigen:

   ```
   $ gpg --show-keys rise-ti-client-pu.gpg
   ```

3. Überprüfen Sie, ob der Fingerprint des GPG-Schlüssels mit dem folgenden Fingerprint übereinstimmt:

   ```
   8E4F3B1075A54CC061118F363A17A2FA1EACFAB1
   ```

> **Wichtig**
>
> Nachfolgende Schritte dürfen nur nach positivem Abgleich des Fingerprints ausgeführt werden. Sollten die Fingerprints nicht übereinstimmen, wenden Sie sich an Ihren Systemadministrator oder an den RISE-Support.

2.1.7.2 Einrichtung des öffentlichen Schlüssels zur Verifizierung der Artefakte aus dem APT-Repository für Linux:

Verschieben Sie den Schlüssel in das entsprechende Verzeichnis:

```
$ sudo mv rise-ti-client-pu.gpg /usr/share/keyrings/rise-ti-client-pu.gpg
```

2.1.7.3 Import des öffentlichen Schlüssels in die GPG-Keychain des öffentlichen Systems für Docker-Container:

Importieren Sie den Schlüssel in die GPG-Keychain:

```
$ gpg --import rise-ti-client-pu.gpg
```

2.1.7.4 Anpassen der Vertraulichkeitsstufe des öffentlichen Schlüssels

1. Öffnen Sie die Bearbeitung des GPG-Schlüssels:

   ```
   $ gpg --edit-key 8E4F3B1075A54CC061118F363A17A2FA1EACFAB1
   ```

2. Um den Vertrauensgrad des GPG-Schlüssels zu setzen, geben Sie den Befehl *trust* ein. Bestätigen Sie die Eingabe mit *Enter*.
3. Im nachfolgenden Dialog werden Ihnen die möglichen Vertrauensstufen angezeigt. Um die Vertrauensstufe „ultimate trust" einzustellen geben Sie 5 ein. Bestätigen Sie die Eingabe mit *Enter*.
4. Die nachfolgende Frage, ob Sie wirklich die gewählte Vertrauensstufe einstellen wollen, beantworten Sie indem Sie *j* eingeben. Bestätigen Sie die Eingabe mit *Enter*.
5. Drücken Sie die Tastenkombination *Strg+C*, um die Konsole zu schließen.

2.2 Kompatibilität

Der TI-Client wurde erfolgreich mit folgenden, von der gematik zugelassenen Kartenterminals getestet:

- Ingenico ORGA 6141 (Firmware-Version 3.9.0)

- CHERRY ST-1506 (Firmware-Version 4.0.25)

> **Wichtig**
>
> Bitte halten Sie Ihre Kartenterminal-Firmware stets aktuell.

> **Hinweis**
>
> Bitte stellen Sie sicher, dass die aktuelle TSL-Version auf Ihrem Kartenterminal installiert ist.

2.3 Vorbereitung

Eine URL zum sicheren Download des TI-Client-Installationspakets wird vom TI-Gateway-Anbieter zur Verfügung gestellt. Vor der Installation des TI-Clients müssen alle Systemanforderungen überprüft und die Betriebsumgebung entsprechend vorbereitet werden.

> **Wichtig**
>
> Achten Sie darauf, dass alle verwendeten Ports eindeutig sind. Kombinationen aus IP-Adresse und Port dürfen nicht mehrfach vergeben werden, da dies zu Konflikten bei der Netzwerkkommunikation führt und den ordnungsgemäßen Betrieb des TI-Clients beeinträchtigt.

> **Wichtig**
>
> Der erlaubte Bereich für die freizugebenden Ports ist 1024-65535.

> **Hinweis**
>
> Die ausgewählten Ports sollten nicht auf eine 0 enden, um Kollisionen mit anderen Programmen zu vermeiden.

2.4 Konfigurationspaket

Das Konfigurationspaket, welches für die Installation des TI-Clients benötigt wird, enthält sensible Daten, welche unter keinen Umständen an Dritte weitergeben werden dürfen. Wird ein Konfigurationspaket nicht mehr benötigt oder ist dessen Geheimhaltung nicht mehr gewährleistet, ist sofort die Deaktivierung bzw. Löschung des Konfigurationspaketes beim Support Ihres TI-Gateway-Anbieters unter der E-Mail-Adresse *support@rise-ti.de* zu beauftragen.

2.5 Deinstallation einer älteren RISE TIaaS Client Version

Ist auf dem System ein RISE TIaaS Client installiert, muss dieser zuerst deinstalliert werden, da dieser nicht mit dem TI-Client kompatibel ist.

2.5.1 Windows und macOS

Wird die Installationsdatei des TI-Clients ausgeführt, wird geprüft, ob ein TIaaS Client installiert ist. Sollte dies der Fall sein, wird angeboten, diesen automatisch zu deinstallieren. Nach der Deinstallation wird automatisch die Installation des TI-Clients fortgesetzt.

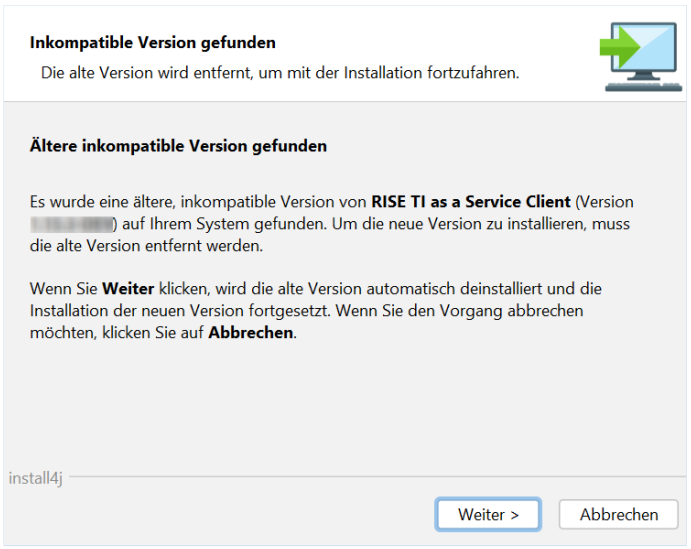

Abbildung 1: Automatische Deinstallation von inkompatibler Version

2.6 Installationsprozess

2.6.1 Windows und macOS

Zum Start der Installation des TI-Clients führen Sie die zu Ihrem Betriebssystem passende Installationsdatei *RISE_TI-Client* aus.

> **Wichtig**
>
> Die Installationsdatei darf nicht mit Administrator- oder root-Berechtigung ausgeführt werden.

Kurz nach dem Start der Installation wird der Setup-Assistent vorbereitet (siehe Abbildung 2).

> **Wichtig**
>
> Es wird dringend abgeraten, die Installation über den Windows Task-Manager bzw. die macOS Aktivitätsanzeige abzubrechen, da dies zu unerwarteten Fehlern führen kann.

Folgende Schritte sind nun zum Abschluss der Installation notwendig:

1. **Startseite:** Folgen Sie den Anweisungen, um den Installationsprozess des TI-Clients zu starten.

Abbildung 2: Startseite des Setup-Assistenten zur Installation des TI-Clients

2. **Installationsart auswählen:** Wählen Sie zwischen der vollständigen- und einer benutzerdefinierten Installation aus. Die vollständige Installation beeinhaltet den TI-Client, den RISE WireGuard-Client und das RISE KIM-Clientmodul.

> **Hinweis**
>
> RISE KIM ist ein von der gematik zugelassener Kommunikationsdienst innerhalb der Telematikinfrastruktur (TI). Es ermöglicht sicheren, verschlüsselten Austausch von medizinischen Dokumenten wie Arztbriefen, eAU, eRezepten oder Laborberichten zwischen Leistungserbringern im Gesundheitswesen. Weitere Informationen finden Sie unter folgender Adresse: https://www.rise-kim.de

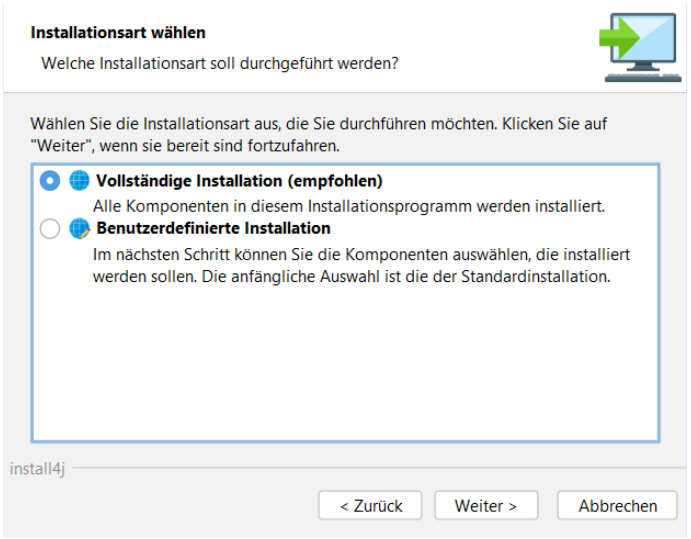

Abbildung 3: Auswahl der Installationsart

3. **Komponenten auswählen:** Bei der benutzerdefinierten Installation können Sie auswählen, ob Sie den RISE WireGuard-Client bzw. das RISE KIM-Clientmodul zusammen mit dem TI-Client installieren möchten.

> **Hinweis**
>
> Wenn Sie einen gesonderten WireGuard-Client nutzen, haben Sie hier die Möglichkeit, die Installation des mitgelieferten WireGuard-Clients zu überspringen. Bitte bedenken Sie dabei, dass dies eine manuelle Konfiguration des WireGuard-Clients erfordert.

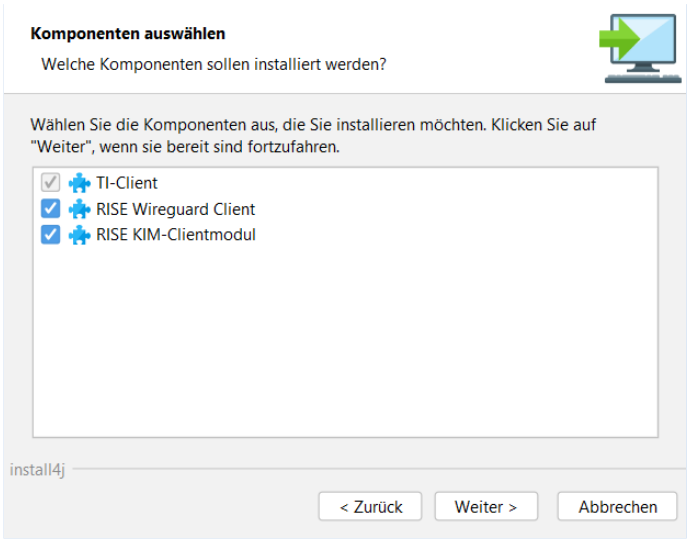

Abbildung 4: Auswahl der zu installierenden Komponenten

4. **Zielverzeichnis für den TI-Client auswählen:** Es wird empfohlen, das Standard-Installationsverzeichnis nicht zu ändern.

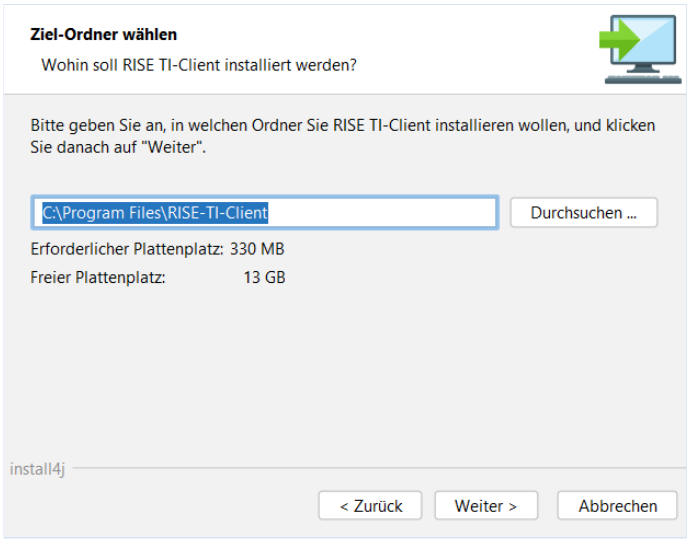

Abbildung 5: Auswahl des Installationsverzeichnisses für den TI-Client

5. **Installationsoptionen:** Während der Installation können Sie folgende Einstellungen vornehmen:

> **Wichtig**
>
> Bei der Auswahl der verwendeten Ports sind die allgemeinen Vorgaben unter Abschnitt 2.3 zu berücksichtigen.

   - **Port der Benutzeroberfläche:** Mit dieser Option können Sie den Port festlegen, unter dem die Benutzeroberfläche des TI-Clients lokal erreichbar ist.

- **Firewall eingehende Ports (nur für Windows):** Hier müssen die Ports angegeben werden, welche an der Firewall des Betriebssystems für die Verbindung der Kartenterminals und der Praxisverwaltungssysteme (PVS) freigeschaltet werden sollen. Pro Kartenterminal, welches mit dieser Client-Installation verwendet werden soll, muss ein Port freigegeben werden, wenn der TI-Client und der WireGuard-Client auf demselben Gerät betrieben werden. Sollte der WireGuard-VPN-Tunnel von einem anderen Gerät aufgebaut werden, müssen pro Kartenterminal zwei Ports freigeschaltet werden. Geben Sie die Ports entweder einzeln kommasepariert an (5051,5052) oder nutzen Sie zur Angabe eines Portbereichs einen Bindestrich (5051-5059).
- **WireGuard ListenPort setzen:** Hier können Sie optional den ListenPort-Parameter des WireGuard-Profils setzen. Falls Sie diese Möglichkeit nicht nutzen und das WireGuard-Profil Ihres Konfigurations-Paketes einen ListenPort-Wert beinhaltet, wird dieser gelöscht.
- **Update-Zeitpunkt:** Hier können Sie den täglichen Update-Zeitpunkt festlegen. Ist eine neue Version des TI-Clients verfügbar, so wird diese zum festgelegten Zeitpunkt installiert.

> **Hinweis**
>
> Wird der TI-Client vor dem definierten Update-Zeitpunkt beendet, wird die Installation des Updates beim nächsten Start der Applikation durchgeführt.

> **Warnung**
>
> Im Zuge eines Updates muss der TI-Client neu gestartet werden. Es ist somit zum ausgewählten Update-Zeitpunkt mit einer möglichen Dienst-Unterbrechung zu rechnen.

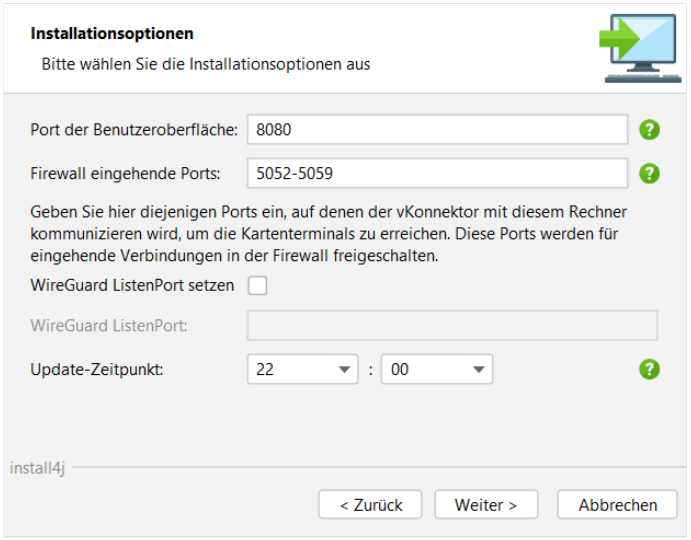

Abbildung 6: Installationsoptionen des TI-Clients

6. **Konfigurationsdatei importieren:** Geben Sie den Pfad zum Konfigurationspaket des TI-Clients an, das Sie mit dem Installationspaket bereitgestellt bekommen haben. Es handelt sich um eine .zip-Archivdatei. Falls die Archivdatei passwortgeschützt ist, haben Sie hier die Möglichkeit, das Passwort einzugeben.

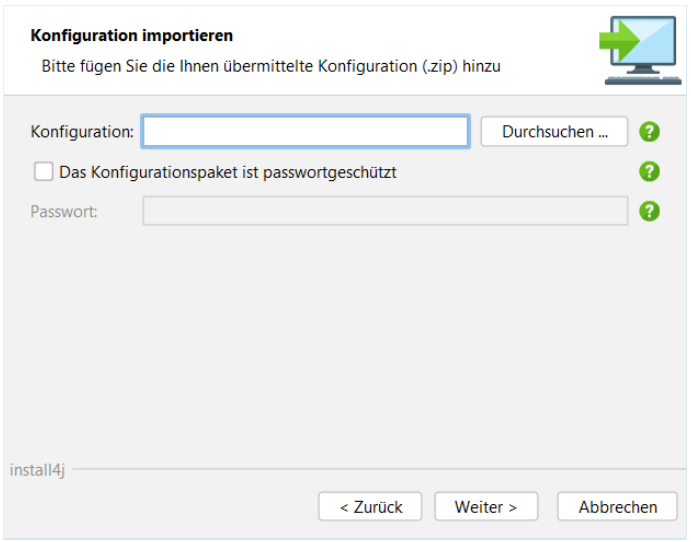

Abbildung 7: Konfigurationsdatei importieren

7. **Firewallregeln erstellen (nur für Windows):** Es wird eine Übersicht der Firewallregeln angezeigt, welche im Zuge der Installation angelegt werden. Bestätigen Sie diese, wenn Sie damit einverstanden sind und mit der Installation fortfahren möchten.

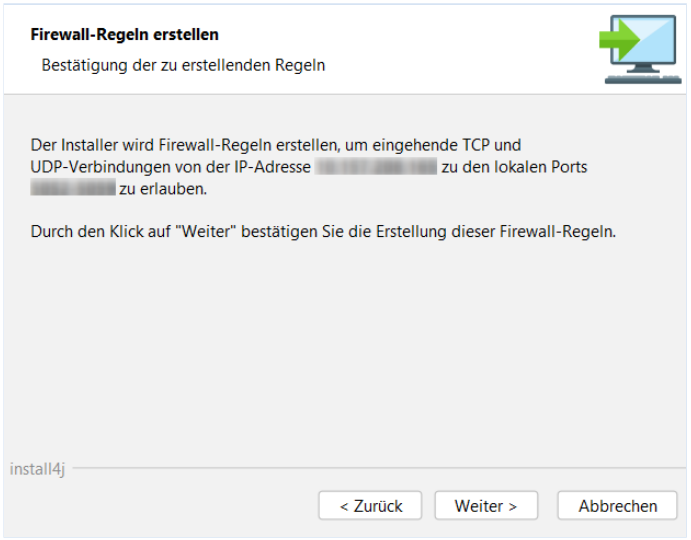

Abbildung 8: Bestätigung der Firewallregeln

8. **Installation RISE KIM-Clientmodul** Dieser Punkt ist nur relevant, wenn Sie die vollständige Installation (siehe Abbildung 3) oder im Rahmen der benutzerdefinierten Installation (siehe Abbildung 4) die Installation des RISE KIM-Clientmoduls ausgewählt haben. Folgen Sie dazu den Anweisungen unter Abschnitt 2.7.
9. **Abschluss der Installation:** Die Installation wurde erfolgreich beendet.

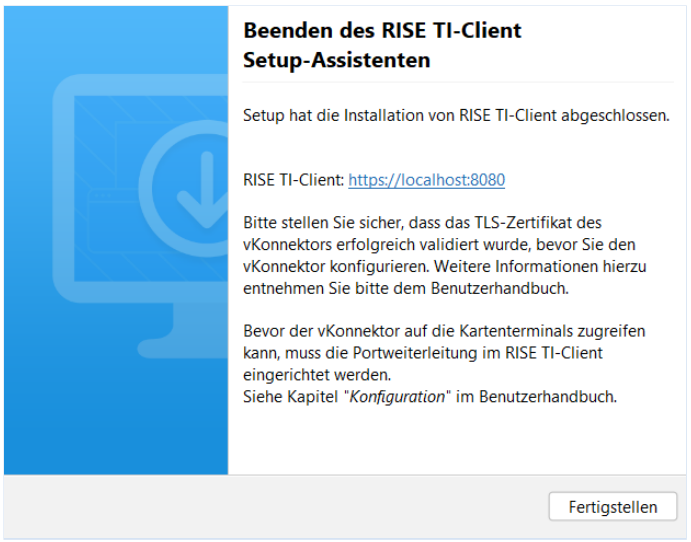

Abbildung 9: Installation erfolgreich abgeschlossen

2.6.2 Linux

2.6.2.1 Installation des TI-Clients

Das TI-Client-Debian-Paket kann direkt über den Paketmanager *APT* installiert werden. Führen Sie dafür folgende Schritte durch:

1. Beziehen Sie den öffentlichen Schlüssel und richten Sie ihn ein, wie unter Abschnitt 2.1.7 beschrieben.
2. Fügen Sie das APT-Repository Ihrem System hinzu:

   ```
   $ echo "deb [signed-by=/usr/share/keyrings/rise-ti-client-pu.gpg] https://client.ti-gateway.de/update-tigw-pu/apt-repo/ stable main" | sudo tee /etc/apt/sources.list.d/rise-ti-client.list
   ```

3. Aktualisieren Sie die Paketquellen:

   ```
   $ sudo apt update
   ```

4. Installieren Sie den TI-Client:

   ```
   $ sudo apt install rise-ti-client
   ```

5. Kopieren Sie die Datei mit der Endung *.yml* aus Ihrem Konfigurationspaket, welches Sie im Laufe der Bestellung erhalten haben, in das Verzeichnis */etc/rise/ti-client/* und benennen Sie die Datei in *application.yml* um. Vergeben Sie anschließend die erforderlichen Rechte durch das Ausführen des folgenden Befehls:

   ```
   $ sudo chown rise-ti-client:rise-ti-client application.yml
   ```

   > **Hinweis**
   >
   > Sollten Sie einen anderen Benutzernamen als den Standardnutzernamen *rise-ti-client* für die Installation des TI-Clients verwenden, ersetzen Sie *rise-ti-client* durch den von Ihnen gewählten Benutzernamen.

6. Kopieren Sie die Datei mit der Endung *.conf* aus Ihrem Konfigurationspaket, welches Sie im Laufe der Bestellung erhalten haben, in das Verzeichnis */etc/rise/ti-client/* und benennen Sie die Datei in *tigw-vpn.conf* um. Vergeben Sie anschließend die erforderlichen Rechte durch das Ausführen der folgenden Befehle:

   ```
   $ sudo chown root:root tigw-vpn.conf
   $ sudo chmod 600 tigw-vpn.conf
   ```

7. Aktivieren und starten Sie das Service für den VPN-Tunnel:

```
$ sudo systemctl enable rise-tigw-vpn.service
$ sudo systemctl start rise-tigw-vpn.service
```

8. Aktivieren und starten Sie das Service für den TI-Client:

```
$ sudo systemctl enable rise-ti-client-service.service
$ sudo systemctl start rise-ti-client-service.service
```

9. Aktivieren und starten Sie das Service für das Maintenance-Service vom TI-Client:

```
$ sudo systemctl enable rise-ti-client-maintenance-service.service
$ sudo systemctl start rise-ti-client-maintenance-service.service
```

2.6.2.2 Aktualisieren des TI-Clients

Zum Aktualisieren des TI-Clients führen Sie folgende Befehle aus:

```
$ sudo apt update
$ sudo apt install rise-ti-client
```

2.6.2.3 Zugriff auf die Benutzeroberfläche des TI-Clients

Falls Ihr System eine grafische Oberfläche und einen Webbrowser besitzt, können Sie unter der URL https://localhost:8080 auf die Benutzeroberfläche des TI-Clients zugreifen.

Falls Ihr System keine grafische Oberfläche und keinen Webbrowser besitzt, so können Sie über ein SSH-Port-Forwarding von einem entfernten Host (im Weiteren als Guest-Host bezeichnet) auf die Benutzeroberfläche des TI-Clients wie folgt zugreifen.

1. Stellen Sie sicher, dass sich der TI-Client-Host und der Guest-Host im selben Netzwerk befinden.
2. Öffnen Sie einen SSH-Tunnel mit einem Port-Forwarding vom Guest-Host zum TI-Client-Host durch Eingabe des folgenden Befehls:

   ```
   $ ssh -L 8080:127.0.0.1:8080 <TI-CLIENT_HOST_USER>@<TI-CLIENT_HOST_IP>
   ```

   Ersetzen Sie *<TI-CLIENT_HOST_USER>* durch den Benutzernamen Ihres Benutzers am TI-Client Host und *<TI-CLIENT_HOST_IP>* durch die IP-Adresse des TI-Client-Hosts.
3. Folgen Sie den Login-Instruktionen.
4. Nach einem erfolgreichen Login kann mittels des Port-Forwards die Benutzeroberfläche des TI-Clients vom Guest-Host unter Eingabe folgender URL im Webbrowser aufgerufen werden:
   https://localhost:8080

Zur weiteren Konfiguration folgen Sie der Beschreibung im Abschnitt 3.

2.6.2.4 Zugriff zum vKonnektor

Um den Zugriff zum vKonnektor von anderen Geräten (bspw. PVS) im selben Netzwerk zu erlauben, muss auf dem System, auf dem der TI-Client installiert ist, ein NAT eingerichtet werden. Führen Sie dafür folgende Schritte durch:

1. Konfigurieren Sie das NAT und aktivieren Sie die Portweiterleitung:

   ```
   $ sudo iptables -t nat -A POSTROUTING -o tigw-vpn -j MASQUERADE
   $ echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
   ```

2. Um die Einstellungen zu persistieren, bearbeiten Sie die Datei */etc/sysctl.conf* und entfernen den Kommentar in der Zeile *net.ipv4.ip_forward=1*, sodass die Option eingelesen wird. Führen Sie zusätzlich folgenden Befehl aus und folgen den Anweisungen:

   ```
   $ sudo apt install iptables-persistent
   ```

3. Erstellen Sie auf den Systemen, welche über das System, auf dem der TI-Client installiert ist, auf den vKonnektor zugreifen sollen, für jede IP-Adresse aus der Liste *AllowedIPs* in der Datei *tigw-vpn.conf* eine Route, indem Sie den für Ihr Betriebssystem entsprechenden Befehl ausführen:
   Für Windows:

```
> route ADD <IP_AUS_ALLOWEDIPS> MASK <SUBNETZMASKE_DER_IP> <IP_DES_SYSTEM_WO_DER_TI-CLIENT_INSTALLIERT_IST>
```

Für Linux:

```
$ sudo route add -net <IP_AUS_ALLOWEDIPS> netmask <SUBNETZMASKE_DER_IP> gw <IP_DES_SYSTEM_WO_DER_TI-CLIENT_INSTALLIERT_IST>
```

Ein Beispiel für den Befehl sieht folgendermaßen aus:

```
$ sudo route add -net 10.20.30.0 netmask 255.255.255.0 gw 192.168.1.123
```

4. Sollten Firewalls aktiviert bzw. im Netzwerk eingebunden sein, sind gegebenenfalls Regeln einzurichten.

2.6.3 Docker

Das für die Installation benötigte Docker-Setup-Paket kann unter folgendem Link bezogen werden: https://client.ti-gateway.de/installer-tigw/docker-setup-paket.zip

2.6.3.1 Installation des TI-Clients

Für die Installation des TI-Clients als Docker-Container sind folgende Voraussetzungen zu erfüllen:

- Docker ab Version 27.2.1 und Docker Compose ab Version 2 ist installiert.
- Docker wird nicht als *rootless* betrieben.
- Der Docker-Container muss mit root-Berechtigungen ausgeführt werden.
- Das Docker-Setup-Paket ist vorhanden.
- Das Installationspaket, das über die Bestellung erhalten wurde, ist vorhanden.
- WireGuard-VPN-Tunnel außerhalb des Docker-Containers

> **Wichtig**
>
> Bitte beachten Sie, dass Docker-Installationen keine Auto-Update-Funktionalitäten bieten und im Falle einer neuen Version manuell aktualisiert werden müssen.

2.6.3.1.1 Bezug und Einrichtung des öffentlichen Schlüssels

Beziehen Sie den öffentlichen Schlüssel und richten Sie ihn, wie unter Abschnitt 2.1.7 beschrieben, ein.

2.6.3.1.2 Prüfung der Signatur des Docker-Setup-Paketes

1. Die Signatur zur Prüfung des Docker-Setup-Paketes kann unter folgendem Link bezogen werden: https://client.ti-gateway.de/installer-tigw/docker-setup-paket.zip.sig
2. Prüfen Sie die Signatur des Docker-Setup-Paketes:

   ```
   $ gpg --verify docker-setup-paket.zip.sig docker-setup-paket.zip
   ```

3. Wenn die Signatur valide ist, wird folgende Meldung ausgegeben:

   ```
   $ gpg: Good signature from "PuK.UTILITY1.SIG <keymanagement@rise-konnektor.de>"
   ```

2.6.3.1.3 Login in die RISE-Docker-Registry

Um das Docker-Image zu beziehen, loggen Sie sich in die RISE-Docker-Registry ein:

```
$ docker login releases.rise-world.com/docker-ti-client-public --username ti-client-user
```

> **Hinweis**
>
> Als Passwort wird ein Access Token benötigt, welcher auf Anfrage beim RISE-Support an Sie übermittelt wird.

2.6.3.1.4 Prüfung der Signatur des Docker-Containers

1. Um die nachfolgenden Schritte auszuführen, installieren Sie *cosign* und *jq* auf Ihrem System:
   - Informationen zur Installation von *cosign* finden Sie unter folgender Adresse: https://docs.sigstore.dev/cosign/system_config/installation/#with-the-cosign-binary-or-rpmdpkg-package
   - Informationen zur Installation von *jq* finden Sie unter folgender Adresse: https://jqlang.org/download/
2. Beziehen Sie die Docker-Signaturdateien aus der RISE-Docker-Registry und speichern Sie diese in der Datei *signatures.json*:

   ```
   $ cosign download signature releases.rise-world.com/docker-ti-client-public/tigw/ti-client/
   public/ti-client:latest > signatures.json
   ```

3. Extrahieren Sie den Payload aus der Docker-Signaturdatei und speichern Sie diesen in der Datei *payload.json*:

   ```
   $ cat signatures.json | tail -1 | jq -r .Payload | base64 -d > payload.json
   ```

4. Extrahieren Sie die Signatur des Payloads aus der Docker-Signaturdatei und speichern Sie diese in der Datei *payload.json.sig*:

   ```
   $ cat signatures.json | tail -1 | jq -r .Base64Signature | base64 -d > payload.json.sig
   ```

5. Prüfen Sie die Signatur der Datei *payload.json*:

   ```
   $ gpg --verify payload.json.sig payload.json
   ```

6. Prüfen Sie, ob die SHA256-Prüfsumme des Images aus der Datei *payload.json* mit der SHA256-Prüfsumme des heruntergeladenen Docker-Images übereinstimmt:
   - Prüfung nach einem frischen Pull des Docker-Images:

     ```
     $ docker pull releases.rise-world.com/docker-ti-client-public/tigw/ti-client/public/
     ti-client:latest
     ```

   - Prüfung nach einem bereits getätigten Pull des Docker-Images:

     ```
     $ docker images --digests | grep ti-client
     ```

2.6.3.1.5 WireGuard-VPN-Tunnel einrichten

> **Wichtig**
>
> Für die Inbetriebnahme des TI-Clients als Docker-Container ist es erforderlich, einen WireGuard-VPN-Tunnel außerhalb des Containers aufzubauen.

Dieses Kapitel beschreibt die Installation des WireGuard-VPN-Tunnels. Folgende Voraussetzungen sind zu erfüllen:

- Auf dem System ist Linux als Betriebssystem installiert.
- Sie verwenden für die Installation die von uns zur Verfügung gestellten WireGuard-Binaries.
- Der Docker-Container wird anschließend auf diesem System in Betrieb genommen.

Sollten Sie die Voraussetzungen nicht erfüllen, wenden Sie sich an Ihren Netzwerkadministrator für eine individuelle Lösung.

Sollten Sie die Voraussetzungen erfüllen, führen Sie folgende Schritte für die Installation des WireGuard-VPN-Tunnels durch:

1. Erstellen Sie auf Ihrem System ein Verzeichnis, in dem die WireGuard-Dateien anschließend abgelegt werden. In den folgenden Schritten wird dieses Verzeichnis als *Ihr WireGuard-Verzeichnis* bezeichnet.

2. Falls Sie es noch nicht gemacht haben, entpacken Sie Ihr Installationspaket, welches Sie im Rahmen der Bestellung erhalten haben.
3. Kopieren Sie die Datei mit der Endung *.conf* aus dem Installationspaket in Ihr WireGuard-Verzeichnis und benennen Sie diese in *VPN.conf* um.
4. In dem Docker-Setup-Paket befindet sich im Verzeichnis *wg* die Datei *start_vpn.sh*. Kopieren Sie die Datei in Ihr WireGuard-Verzeichnis.
5. In dem Docker-Setup-Paket befindet sich das Verzeichnis *wg*. Kopieren Sie die beiden Dateien *wg* und *wireguard* aus dem Verzeichnis in Ihr WireGuard-Verzeichnis.
6. Bearbeiten Sie die Datei mit der Endung *.conf* in Ihrem WireGuard-Verzeichnis und kommentieren Sie die Zeile mit *Address* aus, indem Sie am Anfang der Zeile eine Raute (*#*) einfügen. Speichern Sie die Änderungen.
7. In der Datei *start_vpn.sh* sind die Befehle eingetragen, welche ausgeführt werden müssen, um den VPN-Tunnel zu starten.

   > **Hinweis**
   >
   > Die Datei dient lediglich als Anleitung, welche Befehle und in welcher Reihenfolge diese ausgeführt werden müssen. Es wird empfohlen, ein Skript für Ihr Betriebssystem anzulegen und die Befehle dort zu hinterlegen. Bitte beachten Sie die Hinweise in der Datei.

   > **Tipp**
   >
   > Damit der VPN-Tunnel automatisch mit dem System startet, wird empfohlen, ein Service für den VPN-Tunnel zu erstellen. Wenden Sie sich dafür an Ihren Systemadministrator.

8. Setzen Sie die Skripte auf ausführbar:

   ```
   $ chmod +x start_vpn.sh wg wireguard
   ```

9. Führen Sie das Start-Skript *start_vpn.sh* mit root-Berechtigungen aus:

   ```
   $ sudo ./start_vpn.sh
   ```

10. Stellen Sie sicher, dass der WireGuard-VPN-Tunnel erfolgreich gestartet wurde:

    ```
    $ sudo ./wg show all
    ```

    Das Ergebnis wird anschließend in der Kommandozeile ausgegeben. In der Zeile *transfer* muss sowohl bei *received* als auch bei *send* ein Wert größer als 0 angezeigt werden. Das komplette Ergebnis kann wie folgt aussehen:

    ```
    latest handshake: 3 minutes ago
    latest handshake duration: 123 ms
    latest received: 36 seconds ago
    transfer: 396 B received, 372 B sent
    ```

> **Hinweis**
>
> Wenn der WireGuard-VPN-Tunnel installiert wurde, kann der TI-Client-Container in Betrieb genommen werden. Folgen Sie dazu den Anweisungen unter Abschnitt 4.1.4.

2.7 Installationsprozess RISE KIM-Clientmodul

2.7.1 Windows und macOS

> **Wichtig**
>
> Bei der Installation des RISE KIM-Clientmoduls müssen Sie die vom Installer benötigten zusätzlichen Berechtigungen im Zuge eines Sicherheitsprompts des Betriebssystems bestätigen.

1. **Ältere- oder bereits installierte Version:** Wird die Installation des RISE KIM-Clientmoduls ausgeführt, wird geprüft, ob bereits eine Version des RISE KIM-Clientmoduls installiert ist. Sollte dies der Fall sein, wird diese automatisch deinstalliert.

   > **Hinweis**
   >
   > Im Falle einer bestehenden Installation eines *Arvato/RISE KIM-1.0-Clientmoduls* oder eines *Arvato KIM-1.5-Clientmoduls* wird das mitgelieferte RISE KIM-1.5-Clientmodul nicht installiert. Die bestehende Installation der genannten Produkte bleibt erhalten. Installationen von KIM-Clientmodulen etwaiger Drittanbieter können nicht automatisch erkannt werden und es wird empfohlen, diese vor Beginn der Installation manuell zu entfernen.

2. **Zielverzeichnis auswählen:** Es wird empfohlen, das Standard-Installationsverzeichnis nicht zu ändern.

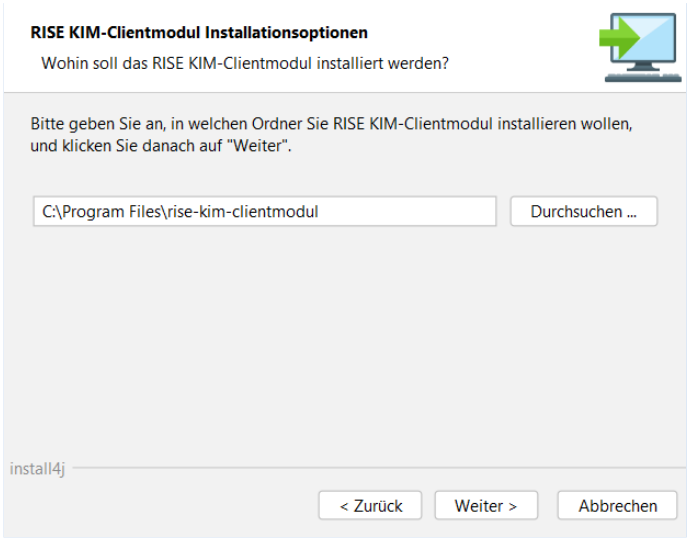

Abbildung 10: Auswahl des Installationsverzeichnisses für das RISE KIM-Clientmodul

3. **Konfiguration der Ports und Firewall:** Hier können Sie die Ports des RISE KIM-Clientmoduls konfigurieren. Sollte sich Ihr E-Mail-Client nicht auf dem gleichen Gerät, auf welchem das RISE KIM-Clientmodul installiert ist, befinden, können Sie über das Aktivieren der Option *Firewall-Regeln hinzufügen* die notwendigen eingehenden Ports auf der Firewall freischalten.

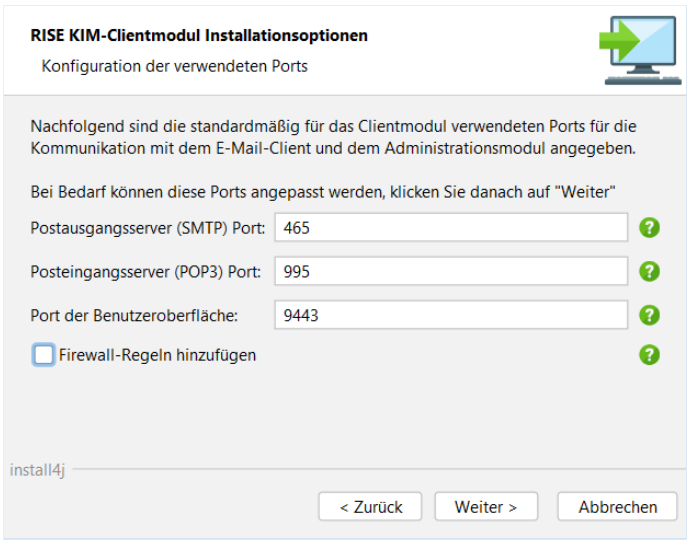

Abbildung 11: Konfiguration der Ports für das RISE KIM-Clientmodul

4. **Konfiguration des Zugangs zum Administrationsbereich:** Legen Sie hier das Passwort für den Zugang zum Administrationsbereich des RISE KIM-Clientmoduls fest.

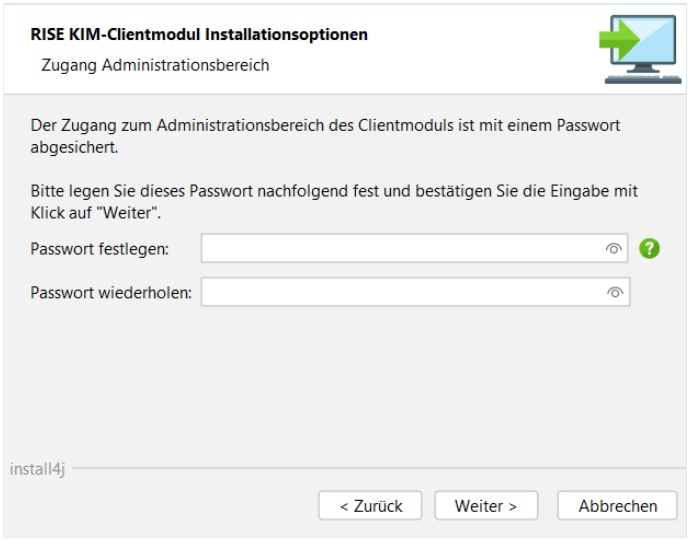

Abbildung 12: Konfiguration des Zugangs zum RISE-KIM-Clientmodul Administrationsbereich

5. **Konfiguration des Hostname:** Geben Sie hier den *Hostname* des aktuell verwendeten Computers ein. Dieser wird später im Parameter *common-name* des vom RISE KIM-Clientmodul generierten TLS-Server-zertifikats verwendet. Wenn Sie das RISE KIM-Clientmodul ausschließlich auf diesem Computer nutzen möchten, empfiehlt es sich, den voreingestellten Wert *localhost* beizubehalten.

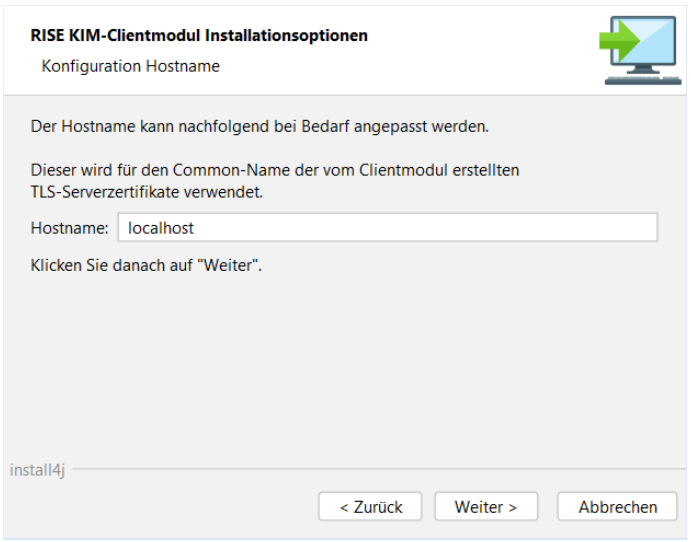

Abbildung 13: Konfiguration des RISE KIM-Clientmodul Hostname

6. **Abschluss der Installation:** Die Installation wurde erfolgreich beendet.

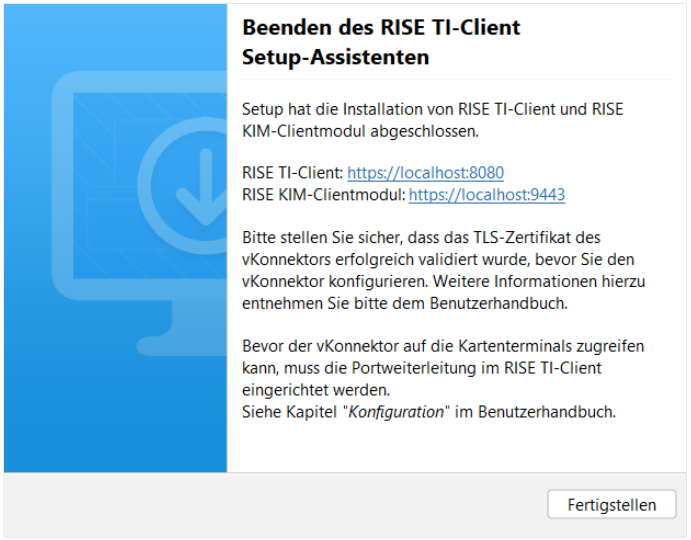

Abbildung 14: Installation erfolgreich abgeschlossen

2.7.2 Linux

> **Hinweis**
>
> Für die Installation des RISE KIM-Clientmoduls unter Linux wird ein separates Debian-Paket benötigt, welches Sie über das TI-Portal bestellen können.

3 Konfiguration

In diesem Abschnitt werden die Konfigurationsmöglichkeiten für den TI-Client beschrieben.

> **Hinweis**
>
> Die Konfiguration ist erst nach der Installation (siehe Abschnitt 2) möglich.

3.1 Informationen des VPN-Tunnels

Falls Sie Informationen über den VPN-Tunnel benötigen, erhalten Sie diese, indem Sie den Schritten für Ihr Betriebssystem folgen.

3.1.1 Windows

1. Öffnen Sie die Applikation *PowerShell* mit Administratorrechten.
2. Navigieren Sie in der PowerShell in das Verzeichnis *WireGuard* im Installationsverzeichnis des TI-Clients.
3. Führen Sie in der PowerShell folgenden Befehl aus:

```
> .\wg.exe show all
```

3.1.2 macOS

1. Öffnen Sie die Applikation *Terminal*.
2. Aktivieren Sie die sudo-Berechtigungen:

```
$ sudo -s
```

3. Navigieren Sie im Terminal in das Verzeichnis *WireGuard* im Installationsverzeichnis des TI-Clients.
4. Führen Sie im Terminal folgenden Befehl aus:

```
$ ./wg show all
```

3.1.3 Linux

1. Öffnen Sie die Applikation *Terminal*.
2. Navigieren Sie im Terminal in das Installationsverzeichnis des TI-Clients.
3. Führen Sie im Terminal folgenden Befehl aus:

```
$ sudo ./wg show all
```

3.2 Kartenterminal-Proxy hinzufügen

Um ein Kartenterminal verbinden und pairen zu können, müssen Sie zuerst einen Kartenterminal-Proxy hinzufügen. Gehen Sie dazu in der Benutzeroberfläche des TI-Clients unter Menüpunkt *Kartenterminal* auf *Proxys*. Wählen Sie hier *Hinzufügen* aus.

Folgende Werte müssen konfigurieren werden:

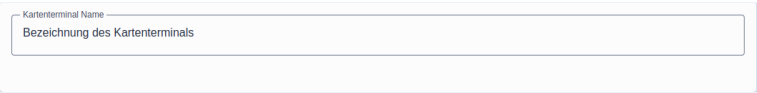

Abbildung 15: Konfiguration Kartenterminal Name

- **Kartenterminal Name:** Hier können Sie optional eine Bezeichnung für das Kartenterminal eingeben (bspw. Ordination-1).

Abbildung 16: Konfiguration WireGuard

- **WireGuard IP:** Standardmäßig wird die WireGuard-IP-Adresse aus der Datei *application.yml* automatisch eingetragen. Der Wert lässt sich durch manuelle Eingabe überschreiben.

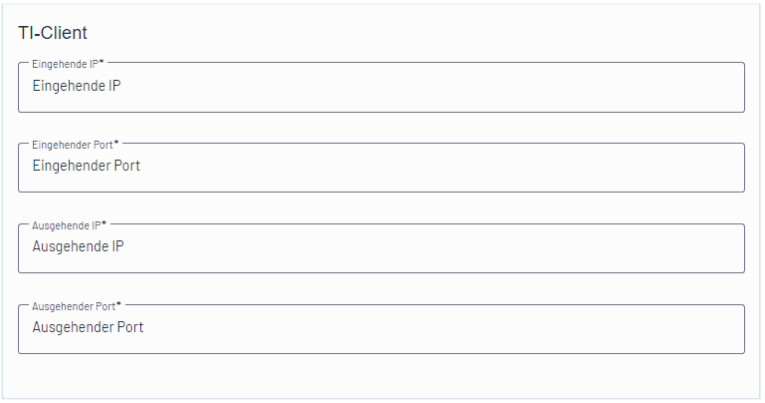

Abbildung 17: Konfiguration TI-Client

- **Eingehende IP:** Standardmäßig wird im Eingabefeld *Eingehende IP-Adresse* automatisch die WireGuard-IP-Adresse aus der Datei *application.yml* hinterlegt. Dieser Wert lässt sich manuell überschreiben, wobei Folgendes zu beachten ist:
  - Wenn der VPN-Tunnel lokal aufgebaut wird, wählen Sie die WireGuard-IP-Adresse.
  - Sollten Sie den VPN-Tunnel auf einem externen Gerät konfiguriert haben, dann wählen Sie die IP-Adresse des lokalen Netzwerkinterfaces aus, welches das Gerät, auf dem der VPN-Tunnel konfiguriert ist, erreichen kann.
- **Eingehender Port:** Wählen Sie einen Port, der bei der Installation angegeben wurde und der auf der lokalen Firewall freigeschaltet ist.
- **Ausgehende IP:** Wählen Sie aus der Liste vorhandener physischer und virtueller Netzwerke jene IP-Adresse, auf der der TI-Client installiert ist.
- **Ausgehender Port:** Wählen Sie einen Port, der bei der Installation angegeben wurde und der auf der lokalen Firewall freigeschaltet ist. Der eingehende und der ausgehende Port müssen unterschiedlich sein, wenn der VPN-Tunnel über ein externes Gerät betrieben wird.

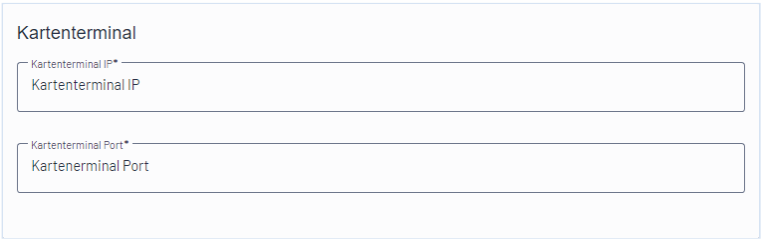

Abbildung 18: Konfiguration Kartenterminal

- **Kartenterminal IP:** Geben Sie hier die lokale IP-Adresse des Kartenterminals ein. Diese können Sie am Kartenterminal im Administrationsmenü ablesen.

- **Kartenterminal Port:** Geben Sie hier den lokalen Port des Kartenterminals ein. Diesen können Sie am Kartenterminal im Administrationsmenü ablesen. Bei Kartenterminals von CHERRY und Ingenico ist der lokale Port standardmäßig 4742.

> **Wichtig**
>
> Bei der Angabe von Portnummern wird empfohlen, dass diese nicht auf einer 0 enden, um Kollisionen mit anderen Programmen zu vermeiden. Ist dies der Fall, kann der TI-Client über diese keine Kommunikation zu den entsprechenden Services aufnehmen.

> **Wichtig**
>
> Bitte stellen Sie sicher, dass die Verfügbarkeit der Kartenterminals vom Host des TI-Clients durch *ICMP-Echo-Requests (Pings)* geprüft werden kann. Der TI-Client überwacht die Erreichbarkeit der Kartenterminals und setzt bestimmte Aktionen nur, wenn diese verfügbar sind.

Abschließend wählen Sie *Speichern*, um die Konfiguration zu speichern. Danach wird der Eintrag in die Liste der Kartenterminal-Proxys angezeigt und Sie können durch Auswahl des neuen Eintrags eine grafische Übersicht anzeigen.

Abbildung 19: Übersicht Kartenterminal-Proxy

3.3 Konfiguration für Remote PIN+ hinzufügen

Die Funktion Remote PIN+ erlaubt das automatische Verifizieren von Karten mit einer hinterlegten PIN.

> **Wichtig**
>
> Die Funktion Remote PIN+ ist nur in Zusammenhang mit lokalen Kartenterminals möglich. Bei *Remote-Kartenterminals* und *Remote-PIN-Kartenterminals* kann die automatische PIN-Verifikation aus technischen Gründen nicht durchgeführt werden (siehe auch Abschnitt 9.2)

> **Wichtig**
>
> Falls Sie ein *Ingenico ORGA Kartenterminal* verwenden, muss sichergestellt werden, dass eine *GSMC-KT* (gerätespezifische Security-Module-Card des Kartenterminals) ab der Generation 2.1 verwendet wird. Remote PIN+ wird nicht unterstützt, wenn ein *Ingenico ORGA Kartenterminal* mit einer *GSMC-KT* der Generation 2.0.0 verwendet wird. Kartenterminals von CHERRY sind von dieser Einschränkung nicht betroffen.

Um die Funktion nutzen zu können, müssen am *lokalen* Kartenterminal die Remote-Schnittstelle und die Remote-PIN-Eingabe für den entsprechenden Kartensteckplatz aktiviert sein. Des Weiteren ist eine eingerichtete Arbeitsumgebung am vKonnektor erforderlich.

Zum Einrichten sind die PIN der Karte und die Admin-PIN des Kartenterminals notwendig. Die PINs werden verschlüsselt im TI-Client hinterlegt.

Um eine Konfiguration für Remote PIN+ einzurichten, gehen Sie dazu in der Benutzeroberfläche des TI-Clients unter Menüpunkt *Kartenterminal* auf *Remote PIN+*. Wählen Sie hier *Hinzufügen* aus. Wählen Sie aus der Liste der verfügbaren Karten die Karte, für die Sie Remote PIN+ einrichten möchten, aus. Nach dem Auswählen einer Karte werden Ihnen die Informationen der Karte angezeigt. Geben Sie anschließend die beiden PINs ein und speichern Sie die Konfiguration. In der Liste mit den Konfigurationen für Remote PIN+, werden diese mit dem Status *AKTIV* angezeigt.

Der TI-Client prüft im Rahmen der Hintergrundaufgaben (siehe Abschnitt 3.5.1.1) alle 5 Minuten, ob der Status der Karte verifizierbar ist. Sollte das der Fall sein, verifiziert der TI-Client die Karte mit den hinterlegten PINs. Jede angelegte Konfiguration für Remote PIN+ beginnt im Status *PENDING*. Je nachdem, ob die Verifizierung erfolgreich ist, wechselt der Status entweder auf *AKTIV* oder auf *FEHLER*. Falls der Status *FEHLER* erscheint, bearbeiten Sie die Konfiguration für Remote PIN+ über das Kontextmenü auf der rechten Seite und geben Sie die PINs erneut korrekt ein. Nach dem Speichern wechselt der Status wieder auf *PENDING*.

Nachfolgend finden Sie eine detaillierte Beschreibung zum jeweiligen Status:

- **AKTIV:** Der Verifizierungsprozess war erfolgreich.
- **FEHLER:** Der Verifizierungsprozess ist fehlgeschlagen. Die PIN+-Verifizierung wird erst wieder durchgeführt, wenn der Fehler manuell behoben wurde.
- **PENDING:** Wird bei jedem Start des Verifikationsprozesses für die Konfiguration angezeigt. Dieser Status bleibt auch im Falle einer Zeitüberschreitung bei der Kommunikation bestehen. In diesem Fall wird die Verifikation später erneut ausgeführt.

3.4 Event-Proxy hinzufügen

Für das PVS der Ordination ist das Einrichten einer Portweiterleitung notwendig, da vom vKonnektor nur die WireGuard-IP-Adresse erreichbar ist. Durch die Konfiguration eines Event-Proxys können eingehende Events vom vKonnektor zum jeweiligen PVS weitergeleitet werden. Das PVS muss sich am vKonnektor mit der WireGuard-IP-Adresse und einem eindeutigen Port für Events registrieren.

> ⚠ **Warnung**
>
> Das PVS muss die Eingabe der WireGuard-IP-Adresse unterstützen, da sonst die Anbindung des PVS an den vKonnektor nicht möglich ist.

Gehen Sie dazu in der Benutzeroberfläche des TI-Clients unter Menüpunkt *vKonnektor* auf *Event-Proxys*. Wählen Sie hier *Hinzufügen* aus.

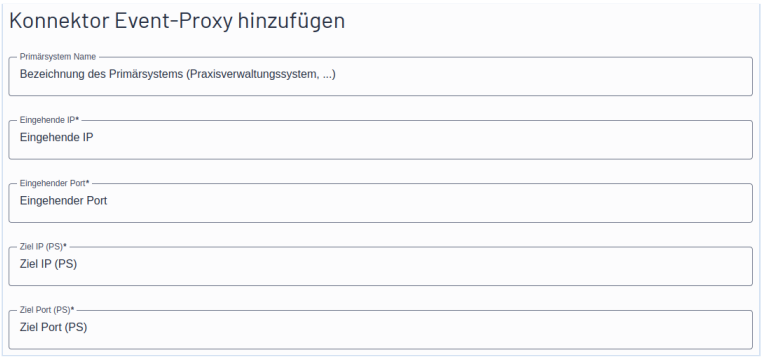

Abbildung 20: Event-Proxy hinzufügen

- **Eingehende IP:** Standardmäßig wird im Eingabefeld *Eingehende IP-Adresse* automatisch die WireGuard-IP-Adresse aus der Datei *application.yml* hinterlegt. Dieser Wert lässt sich manuell überschreiben, wobei Folgendes zu beachten ist:

- Wenn der VPN-Tunnel lokal aufgebaut wird, wählen Sie die WireGuard-IP-Adresse.
- Sollten Sie den VPN-Tunnel auf einem externen Gerät konfiguriert haben, dann wählen Sie die IP-Adresse des lokalen Netzwerkinterfaces aus, welches das Gerät, auf dem der VPN-Tunnel konfiguriert ist, erreichen kann.

- **Eingehender Port:** Wählen Sie einen Port, der bei der Installation angegeben wurde und der auf der lokalen Firewall freigeschaltet ist.
- **Ziel IP (PS):** Wählen Sie hier die IP-Adresse, auf dem das PVS erreichbar ist.
- **Ziel Port (PS):** Wählen Sie hier den Port des PVS, auf den die eingehenden Daten weitergeleitet werden sollen.

> **Wichtig**
>
> Sollte das PVS keine Möglichkeit bieten, den *Ziel Port* anzupassen, muss der *Eingehende Port* ident zum *Ziel Port* eingegeben werden.

Im nachfolgenden Diagramm sehen Sie ein Beispiel für die Einrichtung der Portweiterleitung aus Sicht des PVS.

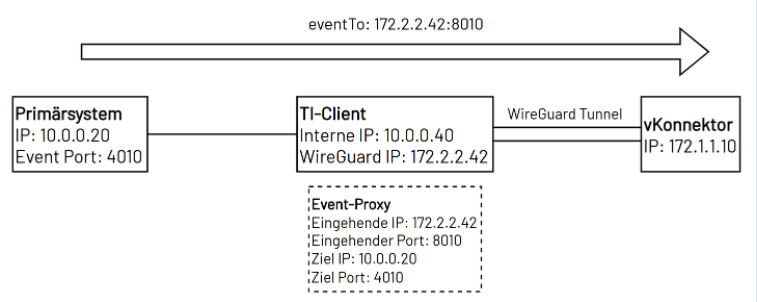

Abbildung 21: Event-Proxy Diagramm

3.5 vKonnektor

3.5.1 Konfiguration

> **Hinweis**
>
> Die Konfiguration des TLS-Serverzertifikates und der Anmeldedaten für den vKonnektor ist die Voraussetzung für die erfolgreiche Durchführung von Hintergrundaufgaben (bspw. das automatische Wiederverbinden von Kartenterminals) und aller Funktionen, die eine direkte Kommunikation mit dem vKonnektor erfordern.

3.5.1.1 Hintergrundaufgaben

Mit dem Schalter *Hintergrundaufgaben* in der oberen rechten Ecke der Benutzeroberfläche des TI-Clients, können die Funktionen, welche eine Kommunikation mit dem vKonnektor über die vKonnektor-Schnittstelle benötigen, aktiviert bzw. deaktiviert werden.

> **Wichtig**
>
> Die vKonnektor-API lässt nur eine aktive Verbindung zu. Dies führt dazu, dass es bei gleichzeitig aktivierten Hintergrundaufgaben und dem Einstieg in die vKonnektor-Benutzoberfläche zum Ablauf der Sitzung kommen kann und die Sitzung automatisch beendet wird. Es wird daher empfohlen, die Hintergrundaufgaben vor dem Einsteigen in die vKonnektor-Benutzeroberfläche zu deaktivieren und nach dem Ausstieg aus der vKonnektor-Benutzeroberfläche wieder zu aktivieren. Sollten Sie über den Menüpunkt *Verwaltung* auf die vKonnektor-Benutzeroberfläche zugreifen, übernimmt der TI-Client diesen Schritt automatisch.

> **Wichtig**
>
> Werden mehrere VPN-Profile zur Verbindung mit einem vKonnektor verwendet, muss beachtet werden, dass der Hintergrundaufgaben-Schalter auf der Konfigurationsseite abgeschaltet ist, damit die Verbindung zur vKonnektor-Oberfläche nicht verloren geht.

3.5.1.2 TLS-Serverzertifikat

Um erfolgreich und sicher mit dem vKonnektor kommunizieren zu können, müssen im TI-Client ein oder mehrere TLS-Zertifikate hinterlegt werden, welche für die Kommunikation verwendet werden sollen. Dafür stehen zwei Möglichkeiten zur Verfügung:

- **Von Konnektor laden:** Mit der Schaltfläche *Von Konnektor laden* wird eine Verbindung zum vKonnektor aufgebaut und das Zertifikat, welches aktuell im vKonnektor verwendet wird, heruntergeladen und im TI-Client hinterlegt.
- **Zertifikat hochladen:** Mit der Schaltfläche *Hochladen* in der rechten unteren Ecke können Sie ein eigenes Zertifikat oder einen eigenen Keystore hochladen. Wenn ein einzelnes Zertifikat hochgeladen wird, werden die Informationen des Zertifikates angezeigt und dieses für die Kommunikation verwendet.

Wenn ein Keystore hochgeladen wird, werden bei einem Verbindungsaufbau zum vKonnektor alle Zertifikate in dem Keystore nacheinander mit dem Zertifikat vom vKonnektor geprüft. Sollte eines der Zertifikate mit dem vKonnektor-Zertifikat übereinstimmen, ist eine sichere Kommunikation möglich. Beim Hochladen eines Keystores werden die Informationen des ersten Zertifikats in dem Keystore anzeigt.

> **Hinweis**
>
> Der TI-Client akzeptiert nur unverschlüsselte Dateien.

> **Warnung**
>
> Sollten sich in dem Keystore, welcher in den TI-Client hochgeladen werden soll, auch private Schlüssel befinden, werden diese ebenfalls in den TI-Client hochgeladen und abgelegt. Es wird daher empfohlen, nur Keystores ohne private Schlüssel hochzuladen.

3.5.1.3 Anmeldedaten

Die Anmeldedaten für den vKonnektor können in der Eingabemaske unter *vKonnektor Anmeldedaten* eingeben werden, um sich bei der Schnittstelle des vKonnektors identifizieren zu können. Sollten keine Anmeldedaten im TI-Client gespeichert sein, werden beim Aufruf der Konfigurationsseite beide Felder leer angezeigt. Sollten bereits Anmeldedaten hinterlegt sein, werden der Benutzername und ein Passwort-Platzhalter angezeigt.

> **Hinweis**
>
> Das Erstellen der Anmeldedaten erfolgt beim erstmaligen Aufruf der vKonnektor-Seite.

Das Passwort der Anmeldedaten für den vKonnektor hat eine standardmäßige Gültigkeitsdauer von 60 Tagen. Die Gültigkeitsdauer kann in der Benutzeroberfläche des vKonnektors angepasst werden. Wir empfehlen Ihnen, dies nur im Rahmen Ihrer eigenen Sicherheitsrichtlinien zu tun.

> **Wichtig**
>
> Die Änderung der Gültigkeitsdauer des Passworts wird erst bei der nächsten Änderung des Passworts aktiv und gilt ab diesem Zeitpunkt für das neu gesetzte Passwort.

Nach dem Auswählen der Schaltfläche *Service-Benutzer erstellen* legt der TI-Client automatisch einen Service-Benutzer am vKonnektor an. Dieser Service-Benutzer hat einen Benutzernamen, der mit einem vordefinierten Präfix (standardmäßig *TI-Client-Service-Benutzer*) und einem Minuszeichen beginnt, gefolgt von fünf zufällig gewählten Großbuchstaben.

> **Wichtig**
>
> Bitte stellen Sie sicher, dass Sie diesen Service-Benutzer nicht löschen.

> **Hinweis**
>
> Der TI-Client ändert das Passwort für diesen Service-Benutzer jeden Tag auf einen automatisch generierten Wert.

3.5.1.4 Werksreset des vKonnektors

Falls ein Zurücksetzen des vKonnektors (Werksreset) durchgeführt wurde, muss auf der Benutzeroberfläche des TI-Client der vKonnektor neu konfiguriert sowie der Service-Benutzer neu angelegt werden. Führen Sie dazu folgende Schritte durch:

1. Gehen Sie in der Benutzeroberfläche des TI-Clients unter Menüpunkt *vKonnektor* auf *Konfiguration*.
2. Löschen Sie den hinterlegten Service-Benutzer, indem Sie die Schaltfläche *Service-Benutzer löschen* auswählen.
3. Konfigurieren Sie das TLS-Serverzertifikat für den vKonnektor. Folgen Sie dazu den Anweisungen unter Abschnitt 3.5.1.2.
4. Geben Sie die Anmeldedaten für den vKonnektor ein. Folgen Sie dazu den Anweisungen unter Abschnitt 3.5.1.3.
5. Legen Sie einen neuen Service-Benutzer an, indem Sie die Schaltfläche *Service-Benutzer erstellen* auswählen.
6. Testen Sie die Verbindung zum vKonnektor, indem Sie die Schaltfläche *Verbindung testen* auswählen.

> **Hinweis**
>
> Prüfen Sie, ob etwaige andere Konfigurationen (Kartenterminal-Proxys, Event-Proxys, Konfiguration für Remote PIN+, usw.) aufgrund der oben ausgeführten Schritte angepasst werden müssen.

3.6 Konfigurationsdatei

Die Konfigurationsdatei *application.yml* befindet sich unter Windows im Installationsverzeichnis des TI-Clients im Verzeichnis *config* und unter macOS und Linux unter */etc/rise/ti-client/*. Die Datei sollte mit einem einfachen Texteditor bearbeitet werden. Dabei ist darauf zu achten, dass der Texteditor mit Administratorrechten gestartet wird, da erhöhte Schreibrechte notwendig sind.

> **Hinweis**
>
> Nach dem Bearbeiten der Konfigurationsdatei muss der TI-Client neu gestartet werden, damit die Änderungen übernommen werden (siehe Abschnitt 4).

3.6.1 Grundlagen zur Bearbeitung von Konfigurationsdateien

Bevor Sie mit der Konfiguration des TI-Clients beginnen, ist es wichtig, ein grundlegendes Verständnis von YAML-Dateien zu haben. YAML steht für *YAML Ain't Markup Language* und ist ein benutzerfreundliches Datenformat zur Konfiguration von Software. Es zeichnet sich durch seine Lesbarkeit und Einfachheit aus. Hier sind einige wichtige Hinweise, die Sie bei der Bearbeitung beachten müssen:

- **Einrückungen:** YAML verwendet Einrückungen zur Strukturierung von Daten. Achten Sie darauf, dass Sie Einrückungen konsistent verwenden, da eine falsche Einrückung zu Fehlern führen kann.
- **Schlüssel-Wert-Paare:** Konfigurationsparameter werden in Form von Schlüssel-Wert-Paaren dargestellt. Der Schlüssel (vor dem Doppelpunkt) identifiziert die Einstellung, und der Wert (nach dem Doppelpunkt) gibt den zugehörigen Wert an.
- **Konfigurationsblöcke:** Zusammenhängende Konfigurationselemente werden oft in Blöcken gruppiert. Ein Block wird durch Einrückungen definiert, die anzeigen, welche Zeilen zur selben Gruppe gehören.
- **Kommentare:** Alles, was innerhalb einer Zeile rechts von einem # steht, wird als Kommentar betrachtet und von der Software ignoriert. Kommentare sind nützlich, um Erinnerungen oder Erklärungen zu bestimmten Konfigurationen hinzuzufügen.

3.6.2 Bearbeiten des Log-Levels

Standardmäßig werden Informationen zum Betrieb des TI-Clients geloggt. Durch das Anpassen des Log-Levels ist es möglich, mehr oder weniger Information als die reine Betriebsinformation zu loggen.

Um das Log-Level des TI-Clients zu ändern, sind folgende Zeilen auf der ersten Ebene in der Konfigurationsdatei einzufügen:

```
logging:
  level:
    com.rise_world: <LOG_LEVEL>
```

Ersetzen Sie *<LOG_LEVEL>* durch das gewünschte Log-Level.

Folgende Log-Level stehen zur Auswahl:

- **off:** Es werden keine Informationen geloggt.

  > **Hinweis**
  >
  > Die Logdatei wird dennoch erstellt und der Applikationstitel wird hineingeschrieben.

- **info:** Standard-Log-Level. Es werden Informationen zum Betrieb sowie ggf. auch sensible Daten, wie bspw. Karten-IDs (ICCSN), geloggt.

> **Hinweis**
>
> Im Falle von Bedenken zu den unter diesem Log-Level aufgezeichneten Informationen, können Sie den Log-Level auf *off* ändern. Bitte beachten Sie, dass dadurch Supportfälle erschwert werden könnten, da keine Informationen geloggt werden.

> **Hinweis**
>
> Wird der oben angegebene Text wieder entfernt, wird automatisch dieses Log-Level verwendet.

- **trace:** Es werden neben den betrieblichen Informationen auch die Netzwerkpakete, welche vom Kartenterminal-Forwarder weitergeleitet werden, geloggt.

> **Wichtig**
>
> In diesem Logging-Modus werden sämtliche Netzwerkpakete, und damit ggf. auch sensible Daten, wie bspw. Karten-IDs (ICCSN) und MAC-Adressen, geloggt. Daher wird dringend empfohlen, das Log-Level durch das Entfernen der entsprechenden Zeilen nach der Fehlersuche wieder zu deaktivieren und die in diesem Modus angelegten Log-Dateien zu löschen (siehe Abschnitt 6).

3.6.3 Bearbeiten des Ports der Benutzeroberfläche

Um den Port zu ändern, unter welchem die TI-Client-Benutzoberfläche zu erreichen ist, sind folgende Zeilen auf der ersten Ebene einzufügen:

```
server:
  port: <PORT>
```

Ersetzen Sie *<PORT>* durch Ihren gewünschten Port.

3.7 Bearbeiten der WireGuard-Konfigurationsdatei

Die Konfigurationsdatei für den WireGuard-VPN-Tunnel wird standardmäßig während der Installation des TI-Clients unter Windows und macOS im Verzeichnis *WireGuard* im Installationsverzeichnis des TI-Clients und unter Linux im Verzeichnis */etc/rise/ti-client/* abgelegt.

> **Wichtig**
>
> Zum Öffnen des Ordners bzw. Bearbeiten der Konfigurationsdatei sind Administratorberechtigungen erforderlich.

Wenn die gesamte WireGuard-Konfigurationsdatei ausgetauscht werden muss, ist wie folgt vorzugehen:

1. Die alte TI-Client-VPN-Konfigurationsdatei in dem Verzeichnis durch die neue ersetzen.
2. Das Service für den VPN-Tunnel neu starten. Folgen Sie dazu den Anweisungen unter Abschnitt 4.1.

3.7.1 Anpassen des WireGuard-ListenPorts

Falls Sie den ListenPort des WireGuard-Clients nachträglich anpassen möchten, gehen Sie wie folgt vor:

1. Öffnen Sie die WireGuard-Konfigurationsdatei. Folgen Sie dazu den Anweisungen unter Abschnitt 3.7.
2. Nachfolgend finden Sie ein Beispiel des Inhalts der WireGuard-Konfigurationsdatei (Die Werte wurden teilweise unkenntlich gemacht).

```
[Interface]
#Address = 172.XX.32.XXX/32
#ListenPort = XXX
PrivateKey = eH4/iaXXXXXXGkeGPdUAeMhewXXXXXXXXXX

[Peer]
PublicKey = b+Z6ajj7wI6pKAK5N2XXXXXXXXXXXXXXXXXX
AllowedIPs = 10.XXX.XXX.0/20, 10.XX.XXX.0/24
Endpoint = 213.XXX.92.XX:60XX1
PersistentKeepalive = 25
```

3. Wenn im Abschnitt *Interface* der Konfigurationsdatei noch kein Eintrag *ListenPort = xxx* vorhanden ist, fügen Sie diesen manuell hinzu. Ersetzen Sie *xxx* durch den gewünschten Port.
   Ist der Eintrag *ListenPort = xxx* bereits vorhanden, kann der Port direkt angepasst werden, indem Sie den bestehenden Wert durch den neuen Port ersetzen.
4. Wenn Sie möchten, dass der WireGuard-Client automatisch einen freien Port wählt, entfernen Sie die gesamte Zeile *ListenPort = …* aus der Konfiguration. In diesem Fall übernimmt WireGuard die Wahl des Ports bei jedem Start selbst.

Wichtig

Beachten Sie, dass ggf. eine Firewall-Freigabe für den gewählten Port erforderlich ist, damit eingehende Verbindungen zugelassen werden.

3.8 Hinzufügen notwendiger Firewall-Regeln in der Windows Defender Firewall

3.8.1 IP-Adressen der Kartenterminals

Für das Pairing von Kartenterminals ist es zurzeit notwendig, die während der Installation eingerichteten Firewall-Ausnahmen um die IP-Adressen der Kartenterminals zu erweitern.

Hierzu gehen Sie bitte wie folgt vor:

1. Öffnen Sie den Dialog *Ausführen*, indem Sie die Tastenkombination Windows-Taste + R betätigen.
2. Geben Sie *wf.msc* in das Textfeld ein und bestätigen Sie Ihre Eingabe mit *OK*. Es öffnet sich ein Fenster *Windows Defender Firewall*.
3. Suchen Sie unter *Eingehende Regeln* den Eintrag *RISE TI-Client Service (UDP-In)* und öffnen diesen durch einen Doppelklick.

Wichtig

Es ist hierbei wichtig, den Eintrag mit *UDP-In* zu wählen und nicht jenen mit *TCP-In*.

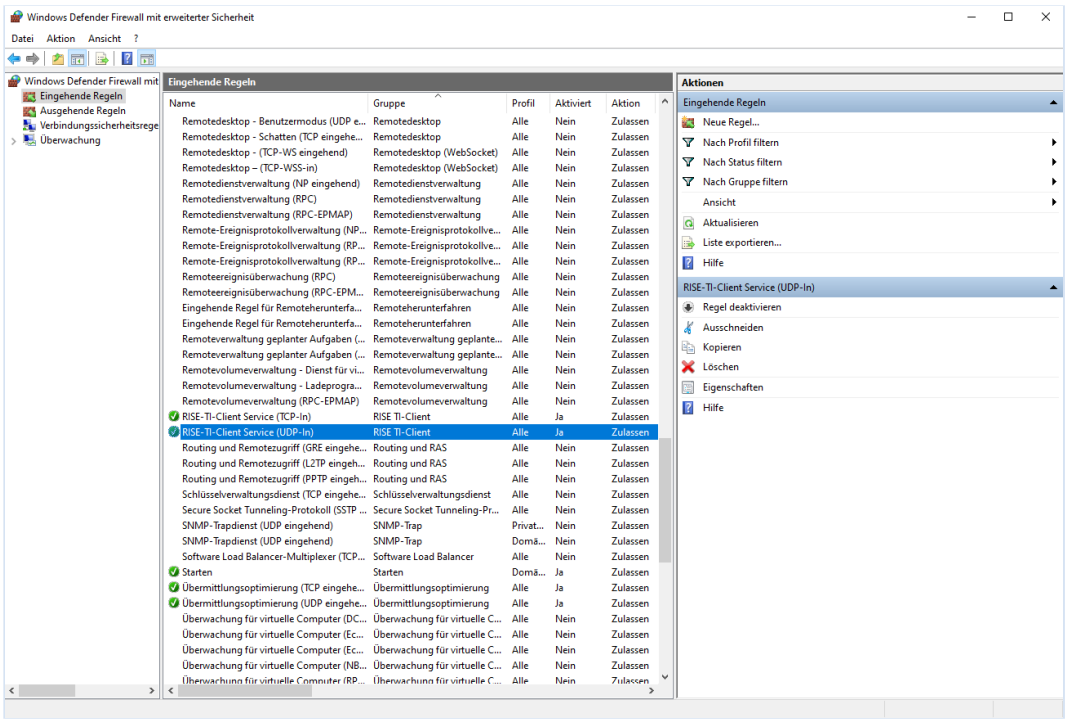

Abbildung 22: Auswahl der erstellten TI-Client Windows Defender Firewall Regel

4. Im Register *Bereich* fügen Sie für jedes Kartenterminal dessen IP-Adresse als *Remote-IP-Adresse* hinzu und übernehmen die neuen Einstellungen.

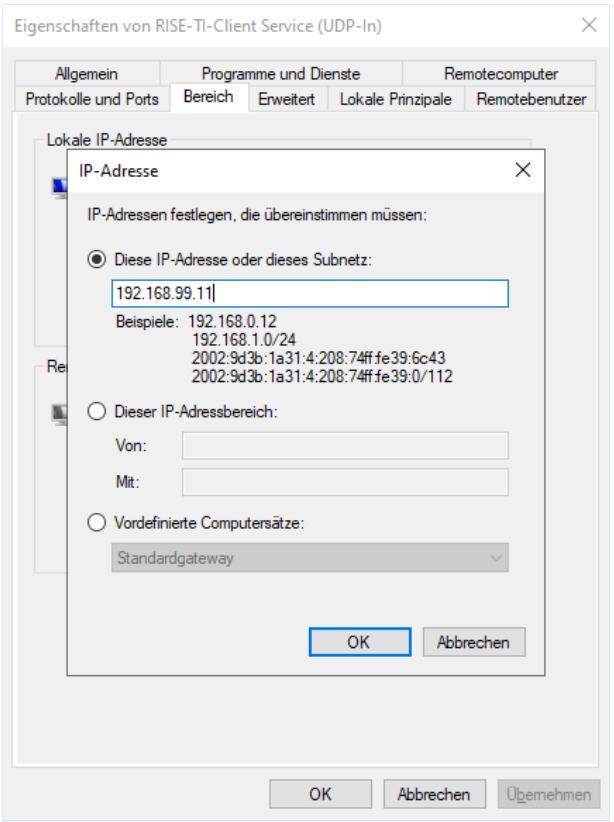

Abbildung 23: Adaptierung der Windows Defender Firewall Regel

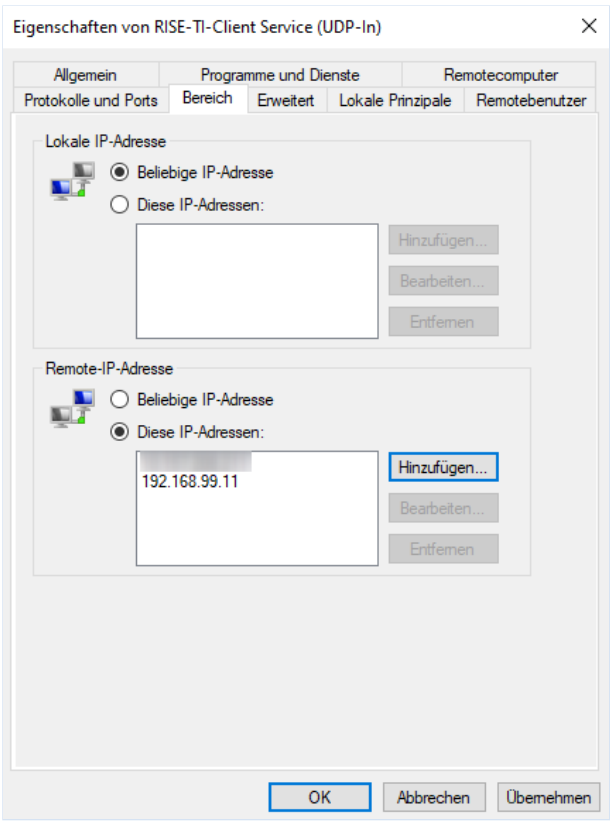

Abbildung 24: Adaptierte Windows Defender Firewall Regel

Falls die Windows Defender Firewall von der Standard-Konfiguration abweicht und ausgehender Traffic blockiert wird, so müssen Sie für den TI-Client eine entsprechende ausgehende Regel in der Windows Defender Firewall zusätzlich definieren.

3.8.2 Zugriff auf den gematik Zertifikatsserver

Es muss sichergestellt werden, dass der Verbindungsaufbau zum gematik-Zertifikatsserver (*download.tsl.ti-dienste.de*) bzw. das Beziehen von Dateien freigegeben ist, damit die CA-Zertifikate bezogen und die vKonnektor-Zertifikate verifiziert werden können. (Für die Testumgebung ist *download-test.tsl.ti-dienste.de* freizuschalten.)

3.9 RISE KIM-Clientmodul

3.9.1 Sicherheitskonfiguration des RISE KIM-Clientmoduls

> **Hinweis**
>
> Die Konfiguration des KIM-Clientmodul-Ports, des TLS-Serverzertifikates und der Anmeldedaten, ist die Voraussetzung für die erfolgreiche Einrichtung des RISE KIM-Clientmoduls aus dem TI-Client.

Für die Einrichtung des KIM-Clientmodul-Ports, des TLS-Serverzertifikates und der Anmeldedaten, gehen Sie dazu in der Benutzeroberfläche des TI-Clients unter Menüpunkt *KIM-Clientmodul* auf *Konfiguration*.

3.9.1.1 KIM-Clientmodul Anmeldedaten

Geben Sie in der Eingabemaske unter *Anmeldedaten* den bei der Installation des RISE KIM-Clientmoduls angegebenen Port und das Admin-Passwort ein und wählen Sie die Schaltfläche *Speichern* aus. Sollten keine Anmeldedaten im TI-Client gespeichert sein, werden beim Aufruf der Konfigurationsseite beide Felder leer angezeigt. Sollten Anmeldedaten bereits hinterlegt sein, wird ein Port und ein Passwort-Platzhalter angezeigt.

> **Wichtig**
>
> Das erfolgreiche Speichern der Anmeldedaten ist Voraussetzung für die anschließende Einrichtung des TLS-Serverzertifikates. Dies wird Ihnen durch ein entsprechendes Status-Symbol angezeigt.

> **Hinweis**
>
> Sollten Sie die im TI-Client gespeicherten Anmeldedaten nach der Ersteinrichtung ändern wollen, können Sie dies über die Schaltfläche *Anmeldedaten ändern* tun.

3.9.1.2 TLS-Serverzertifikat

Um erfolgreich und sicher mit dem RISE KIM-Clientmodul kommunizieren zu können, muss im TI-Client ein TLS-Zertifikat hinterlegt werden, welches für die Kommunikation verwendet werden soll.

- **Von KIM laden:** Mit der Schaltfläche *Von KIM laden* wird eine Verbindung zum RISE KIM-Clientmodul aufgebaut und das Zertifikat, welches dort aktuell verwendet wird, heruntergeladen und im TI-Client hinterlegt.

  > **Wichtig**
  >
  > Das erfolgreiche Hinterlegen des Zertifikates ist Voraussetzung für den anschließend durchzuführenden Verbindungstest. Dies wird Ihnen durch ein entsprechendes Status-Symbol angezeigt.

- **Verbindung testen:** Mit der Schaltfläche *Verbindung testen* können Sie sicherstellen, dass die Einrichtung der Sicherheitskonfiguration für das KIM-Clientmodul erfolgreich abgeschlossen ist.

3.9.2 RISE KIM-Clientmodul Ersteinrichtung

In diesem Abschnitt wird die Ersteinrichtung des RISE KIM-Clientmoduls beschrieben. Um die Ver- und Entschlüsselung der Nachrichten mittels vKonnektor zu ermöglichen, muss das KIM-Clientmodul die Erreichbarkeitsdaten des vKonnektors bzw. die für die vKonnektor-Aufrufe notwendigen Aufrufkontexte kennen.

Um die Ersteinrichtung durchzuführen, gehenn Sie dazu in der Benutzeroberfläche des TI-Clients unter Menüpunkt *KIM-Clientmodul* auf *Verwaltung*.

> **Wichtig**
>
> Der Menüpunkt *Verwaltung* wird erst nach erfolgreicher Einrichtung der KIM-Clientmodul-Sicherheitskonfiguration aktiviert (siehe Abschnitt 3.9).

3.9.2.1 Abrufen der Aufrufkontexte vom vKonnektor

Beim Aufruf der Seite *Ersteinrichtung des KIM-Clientmoduls* unter Menüpunkt *Verwaltung* werden automatisch alle auf dem vKonnektor verfügbaren Aufrufkontexte abgerufen und in einer tabellarischen Ansicht dargestellt.

> **Wichtig**
>
> Um den Abruf der Aufrufkontexte vom vKonnektor auszuführen, wird einerseits die erfolgreiche Einrichtung der vKonnektor-Konfiguration vorausgesetzt sowie andererseits die Einrichtung des Infomodells am vKonnektor.

3.9.2.2 Übertragung der Aufrufkontexte zum RISE KIM-Clientmodul

Um die Übertragung der Aufrufkontexte vorzubereiten, folgen Sie den beschriebenen Schritten auf der Seite *Ersteinrichtung des KIM-Clientmoduls*. Um die Übertragung durchzuführen, wählen Sie die Schaltfläche *Ersteinrichtung starten* aus.

> **Wichtig**
>
> Überprüfen Sie vor der Durchführung der Übertragung, ob bereits eine Konfiguration der Aufrufkontexte am RISE KIM-Clientmodul besteht, da diese mit der Durchführung der Übertragung gelöscht wird.

3.9.3 Link zur Benutzeroberfläche des RISE KIM-Clientmoduls

Um die Benutzeroberfläche des RISE KIM-Clientmoduls aufzurufen, gehen Sie dazu in der Benutzeroberfläche des TI-Clients unter Menüpunkt *KIM-Clientmodul* auf *Verwaltung*.

> **Wichtig**
>
> Diese Funktion ist erst nach erfolgreicher Einrichtung der KIM-Clientmodul-Sicherheitskonfiguration verfügbar (siehe Abschnitt 3.9).

4 Start der Anwendung

4.1 Starten des TI-Clients

4.1.1 Windows

Der TI-Client startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Sollten Sie den TI-Client manuell starten oder beenden wollen, gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den Dialog *Ausführen*, indem Sie die Tastenkombination Windows-Taste + R betätigen.
2. Geben Sie *services.msc* in das Textfeld ein und bestätigen Sie Ihre Eingabe mit *OK*. Es öffnet sich ein Fenster *Dienste*.
3. Suchen Sie den Dienst *RISE-TI-Client Service* in der Liste.
4. Wählen Sie den Dienst mittels Rechtsklick aus und wählen Sie anschließend die gewünschte Option aus: *Starten*, *Beenden* oder *Neu starten*.

Das TI-Client Maintenance Service startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Sollten Sie das TI-Client Maintenance Service manuell starten oder beenden wollen, gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den Dialog *Ausführen*, indem Sie die Tastenkombination Windows-Taste + R betätigen.
2. Geben Sie *services.msc* in das Textfeld ein und bestätigen Sie Ihre Eingabe mit *OK*. Es öffnet sich ein Fenster *Dienste*.
3. Suchen Sie den Dienst *RISE-TI-Client Maintenance Service* in der Liste.
4. Wählen Sie den Dienst mittels Rechtsklick aus und wählen Sie anschließend die gewünschte Option aus: *Starten*, *Beenden* oder *Neu starten*.

Das TI-Client WireGuard Service startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Sollten Sie das TI-Client WireGuard Service manuell starten oder beenden wollen, gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den Dialog *Ausführen*, indem Sie die Tastenkombination Windows-Taste + R betätigen.
2. Geben Sie *services.msc* in das Textfeld ein und bestätigen Sie Ihre Eingabe mit *OK*. Es öffnet sich ein Fenster *Dienste*.
3. Suchen Sie den Dienst *RISE-TI-Client WireGuard Service* in der Liste.
4. Wählen Sie den Dienst mittels Rechtsklick aus und wählen Sie anschließend die gewünschte Option aus: *Starten*, *Beenden* oder *Neu starten*.

4.1.2 macOS

Der TI-Client startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Wenn Sie den TI-Client manuell starten oder neu starten wollen, können Sie das mit folgendem Befehl durchführen:

```
$ sudo launchctl kickstart -k system/com.rise-world.ti-client.manager-service
```

Das TI-Client Maintenance Service startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Wenn Sie das TI-Client Maintenance Service manuell starten oder neu starten wollen, können Sie das mit folgendem Befehl durchführen:

```
$ sudo launchctl kickstart -k system/com.rise-world.ti-client.maintenance-service
```

Das TI-Client *WireGuard* Service startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Wenn Sie das TI-Client *WireGuard* Service manuell starten oder neu starten wollen, können Sie das mit folgendem Befehl durchführen:

```
$ sudo launchctl kickstart -k system/com.rise-world.ti-client.wireguard.autostart
```

4.1.3 Linux

Der TI-Client startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Wenn Sie den TI-Client manuell neu starten wollen, können Sie das mit folgendem Befehl durchführen:

```
$ sudo systemctl restart rise-ti-client-service.service
```

Das TI-Client Maintenance Service startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Wenn Sie das TI-Client Maintenance Service manuell neu starten wollen, können Sie das mit folgendem Befehl durchführen:

```
$ sudo systemctl restart rise-ti-client-maintenance-service.service
```

Das TI-Client *WireGuard* Service startet als Dienst beim Start des Betriebssystems automatisch im Hintergrund. Wenn Sie das TI-Client *WireGuard* Service manuell neu starten wollen, können Sie das mit folgendem Befehl durchführen:

```
$ sudo systemctl restart rise-tigw-vpn.service
```

4.1.4 Docker

> **Wichtig**
>
> Vor Inbetriebnahme des Docker-Containers muss der WireGuard-VPN-Tunnel eingerichtet und erfolgreich gestartet werden. Folgen Sie dazu den Anweisungen unter Abschnitt 2.6.3.1.5

> **Wichtig**
>
> Vor Inbetriebnahme des Docker-Containers muss überprüft werden, ob die entsprechenden Ports auf der Firewall freigeschalten sind.

Führen Sie folgende Schritte durch, um den TI-Client-Docker-Container in Betrieb zu nehmen:

1. Erstellen Sie auf Ihrem System ein Verzeichnis, in dem die TI-Client-Dateien anschließend abgelegt werden. In den folgenden Schritten wird dieses Verzeichnis als *Ihr TI-Client-Verzeichnis* bezeichnet.
2. Erstellen Sie in Ihrem TI-Client-Verzeichnis das Verzeichnis *config*.
3. Kopieren Sie die Datei mit der Endung *.yml* aus Ihrem Installationspaket, welches Sie im Laufe der Bestellung erhalten haben, in das Verzeichnis *config* in *Ihrem TI-Client-Verzeichnis* und benennen Sie die Datei in *application.yml* um.
4. Kopieren Sie die Datei *docker-compose.yml* aus Ihrem Docker-Setup-Paket in Ihr TI-Client-Verzeichnis.
5. Erstellen Sie in Ihrem TI-Client-Verzeichnis die Datei *master_key.txt* und tragen dort einen Schlüssel zum Verschlüsseln der Daten im Docker-Container ein. Beim Erstellen des Schlüssels wird empfohlen, eine Länge von mindestens 16 Zeichen und eine Mischung aus Groß-, Kleinbuchstaben und Zahlen zu verwenden. Speichern Sie die Änderungen.
6. Die angelegte Verzeichnisstruktur sollte wie folgt aussehen:

```
/
├── docker-compose.yml
├── master_key.txt
└── config
    └── application.yml
```

> **Achtung**
>
> Es wird empfohlen, ein Backup des Schlüssels zu erstellen, da bei Verlust des Schlüssels die verschlüsselten Daten nicht mehr zugänglich sind.

7. Führen sie die Datei *docker-compose.yml* aus, indem Sie folgenden Befehl im Terminal in Ihrem TI-Client-Verzeichnis ausführen:

```
$ docker compose up
```

8. Die Benutzeroberfläche des TI-Clients kann anschließend über https://localhost:8080 aufgerufen werden.

> **Hinweis**
>
> Falls Ihr System keine grafische Benutzeroberfläche und keinen Webbrowser besitzt, folgen Sie den Anweisungen unter Abschnitt 2.6.2.3

4.2 Überprüfung des Serverzertifikates

Es wird dringend empfohlen, nach dem Start des TI-Clients die vKonnektor-Zertifikate zu überprüfen. Für die Überprüfung steht Ihnen ein Certificate Verifier zur Verfügung. Das Tool prüft sowohl das RSA- also auch das ECC-Zertifikat.

Für Windows navigieren Sie in der Kommandozeile in das Installationsverzeichnis und führen die Datei *cert-check.exe* aus, indem Sie folgenden Befehl eingeben:

```
> cert-check.exe VKONNEKTOR_IP -p VKONNEKTOR_PORT
```

Für macOS und Linux navigieren Sie im Terminal in das Installationsverzeichnis und führen die Datei *cert-check* aus, indem Sie folgenden Befehl eingeben:

```
$ ./cert-check VKONNEKTOR_IP -p VKONNEKTOR_PORT
```

Ersetzen Sie *VKONNEKTOR_IP* und *VKONNEKTOR_PORT* durch die IP-Adresse und den Port des vKonnektors, zu dem Sie sich verbinden wollen. Bestätigen Sie die Eingabe mit *Enter*.

> **Hinweis**
>
> Die VKONNEKTOR_IP ist der Konfigurationsdatei (siehe Abschnitt 3.6) unter *client > konnektor > url* zu entnehmen.

> **Hinweis**
>
> Der Standardport des vKonnektors ist *8443*.

Das Ergebnis der beiden Zertifikatsüberprüfung wird anschließend in der Kommandozeile ausgegeben.
Sollte das Zertifikat gültig sein, wird die Information *Das vKonnektor-TLS-Serverzertifikat wurde erfolgreich geprüft* ausgegeben. Das komplette Ergebnis für eine gültige Überprüfung eines Zertifikates kann wie folgt aussehen:

```
Checking Konnektor <ZERTIFIKATSTYP> certificate...
++++++++++++++++++++++++++++++++++++++
      Certificate check result
++++++++++++++++++++++++++++++++++++++
eeCertSha256Fingerprint: 5635ffc296563b8axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Das vKonnektor-TLS-Serverzertifikat wurde erfolgreich geprueft
++++++++++++++++++++++++++++++++++++++
```

Bei *ZERTIFIKATSTYP* wird die Art des Zertifikats angezeigt.

> **Hinweis**
>
> Die Werte des Ergebnisses wurden teilweise unkenntlich gemacht.

Sollte das Zertifikat nicht gültig sein, wird die Information *Prüfung des vKonnektor-TLS-Serverzertifikats fehlgeschlagen* ausgegeben. Das komplette Ergebnis für eine ungültige Überprüfung kann wie folgt aussehen:

```
Checking Konnektor <ZERTIFIKATSTYP> certificate...
++++++++++++++++++++++++++++++++++++
      Certificate check result
++++++++++++++++++++++++++++++++++++
caCertChainingValid: OK
caCertTimeValid: OK
eeCertTimeValid: OK
eeCertTypeValid: OK
eeCertSignatureValid: OK
eeCertOcspStatusValid: OK
eeCertSha256Fingerprint: 5635ffc296563b8axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
referenceTime: 2024-02-02T13:54:00.961659Z
caCertNotBefore: 2021-11-08T14:34:19Z
caCertNotAfter: 2029-11-06T14:34:18Z
eeCertNotBefore: 2022-10-10T22:00:00Z
eeCertNotAfter: 2027-10-10T21:59:59Z
eeCertTypeOID: 1.2.276.0.76.4.79
ocspStatus: UNKNOWN
++++++++++++++++++++++++++++++++++++
Pruefung des vKonnektor-TLS-Serverzertifikats fehlgeschlagen
++++++++++++++++++++++++++++++++++++
```

> **Hinweis**
>
> Die Werte des Ergebnisses wurden teilweise unkenntlich gemacht.

> **Achtung**
>
> Es wird dringend geraten, nach dem Verbindungsaufbau zur vKonnektor-Administrations-Benutzeroberfläche die SHA-256-Fingerabdrücke (*eeCertSha256Fingerprint*) aus der vorangegangenen Serverzertifikatsüberprüfung und von der Admin-Oberfläche im Webbrowser abzugleichen.
>
> Den SHA-256-Hashwert des Zertifikats der angesteuerten vKonnektor-Administrations-Benutzeroberfläche erhalten Sie über die zusätzlichen Informationen zur Verbindungssicherheit, die über die Adressleiste im Webbrowser zugänglich sind.
>
> Die Prüfung des Zertifikates mit dem SHA-256-Fingerabdruck von der Website muss erfolgreich sein. Ansonsten darf die Verbindung zur vKonnektor-Administrations-Benutzeroberfläche nicht aufgebaut und keine Informationen angegeben werden.
>
> Falls die Überprüfung nicht erfolgreich bzw. ungültig ist oder der SHA-256-Fingerabdruck der Website zu keinem der beiden Zertifikate passen sollte, wenden Sie sich bitte an den TI-Gateway-Anbieter.

4.3 TLS-Serverzertifikat des TI-Clients

Die *HTTP-Schnittstellen* des TI-Clients (inklusive der TI-Client-Benutzeroberfläche) sind mit einem TLS-Serverzertifikat abgesichert, welches während des ersten Applikationsstarts generiert wird. Das Zertifikat wird mit einer Gültigkeitsdauer von einem Jahr erstellt. Da es sich um ein selbstsigniertes Zertifikat handelt, erscheint beim Zugriff über den Browser eine entsprechende Sicherheitswarnung. Bei jedem Start des Systems werden die Zerti-

fikatsdaten sowie der SHA-256-Fingerabdruck im Log protokolliert. Es wird ausdrücklich empfohlen, den im Log protokollierten SHA-256-Fingerabdruck mit dem im Browser angezeigten zu vergleichen, um die Authentizität des Zertifikats zu verifizieren. Nachdem die Authentizität des Zertifikates sichergestellt wurde, kann das Zertifikat zu dem Truststore des Browsers hinzugefügt werden, damit die oben genannte Sicherheitswarnung nicht mehr angezeigt wird.

> **Hinweis**
>
> Überprüfen Sie Ihre im Browser gespeicherten Lesezeichen, die auf die Benutzeroberfläche des TI-Clients verweisen. Falls diese Lesezeichen mit *http* beginnen, ändern Sie den Link auf *https*, um eine verschlüsselte Verbindung sicherzustellen. Beachten Sie auch, dass alte *http-Links* ins Leere führen, da der TI-Client ausschließlich über *https* erreichbar ist.

5 vKonnektor-Benutzeroberfläche

Dieser Abschnitt befasst sich mit den Einstellungen des vKonnektors, welche für den Betrieb des TI-Clients essenziell sind.

Die Benutzeroberfläche kann über die IP-Adresse des vKonnektors mit dem Port *8443* aufgerufen werden. Einen direkten Link dazu finden Sie auch in der Benutzeroberfläche des TI-Clients. Gehen Sie dazu unter Menüpunkt *vKonnektor* auf *Verwaltung*.

> **Hinweis**
>
> Wenn Sie direkt über die IP-Adresse des vKonnektors auf dessen Benutzeroberfläche zugreifen, müssen sie die Hintergrundaufgaben stoppen und nach dem Verlassen der Benutzeroberfläche wieder starten (siehe Abschnitt 3.5.1.1).
>
> Wenn Sie über den direkten Link in der Benutzeroberfläche des TI-Clients auf die vKonnektor-Benutzeroberfläche einsteigen, übernimmt der TI-Client diese Aufgabe automatisch.

5.1 TLS-Zertifikate

Die Einstellungen für die TLS-Zertifikate für die Kommunikation zwischen vKonnektor und Clientsystemen können über den Menüpunkt *Clientsysteme* (siehe Abbildung 25) erreicht werden.

Die Anbindung der Clientsysteme erfolgt optional mittels TLS. Dabei können am Clientsystem Konfigurationen und Zertifikate modifiziert werden. Bitte beachten Sie, dass Sie Clientsysteme zuvor in der Arbeitsumgebung definieren müssen. Der in der Arbeitsumgebung vergebene Name (entspricht der ID eines Clientsystems) wird an dieser Stelle weiter verwendet.

5.1.1 Konfiguration

Im Reiter *Konfiguration* zeigt die Benutzermaske die Konfigurationsparameter der Clientsysteme (siehe Abbildung 25). Hierbei können Konfigurationen vorgenommen werden, um die Kommunikation mit den Clients mittels TLS abzusichern, um die verpflichtende Authentifizierung von Clientsystemen zu aktivieren bzw. zu deaktivieren und alternative Zertifikate zur Authentifizierung des vKonnektors gegenüber Clientsystemen verwaltet werden.

Ist TLS aktiviert, so authentifiziert sich der vKonnektor gegenüber Clientsystemen mit dem im Abschnitt 5.1.1.3 festgelegten vKonnektor-Zertifikat. Um eine TLS-Verbindung zwischen dem Clientsystem und dem vKonnektor zu konfigurieren, kann dieses vKonnektor-Zertifikat manuell heruntergeladen werden:

1. Rufen Sie dazu die Adresse *https://<IP-Adresse_des_RISE_vKonnektors>/connector.sds* auf.
2. Laden Sie das Zertifikat, beispielsweise durch Anzeigen der Seiteninformationen im Browser, als *pem-Datei* herunter.
3. Importieren Sie das Zertifikat anschließend in das Clientsystem, welches auf den vKonnektor zugreift. Ziehen Sie dafür ggf. das Handbuch für Ihr Clientsystem heran.

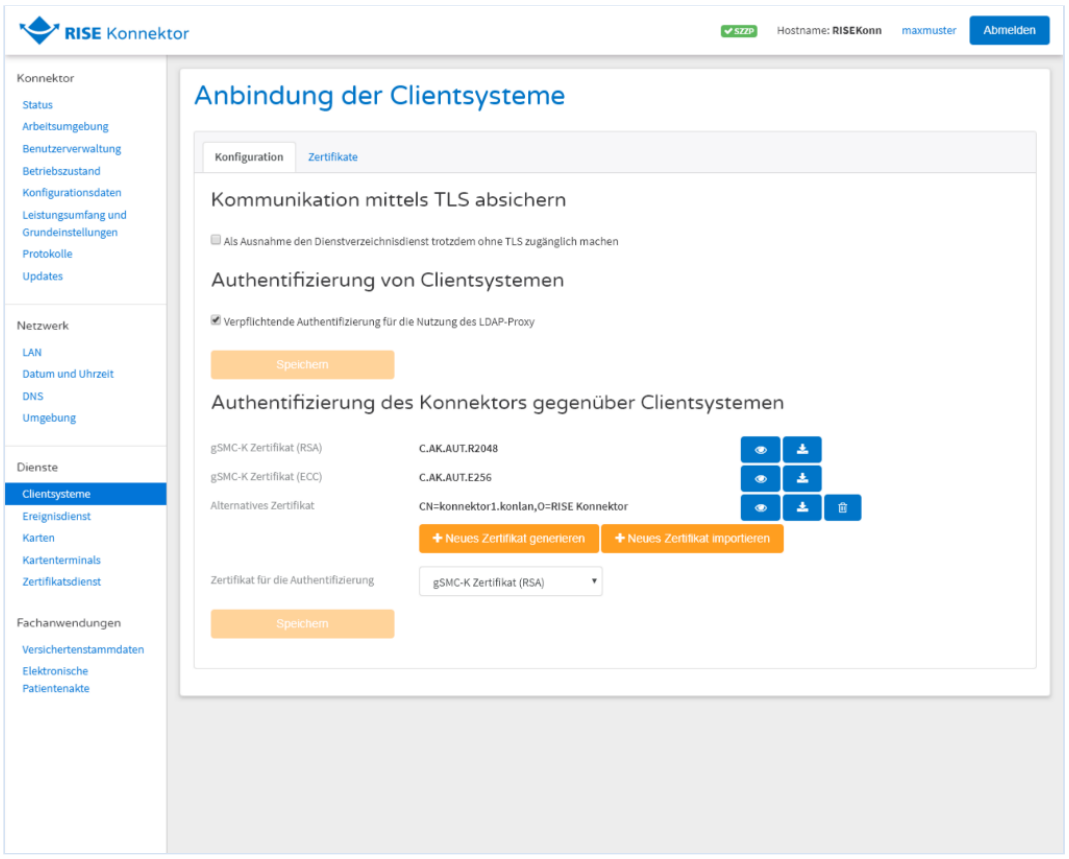

Abbildung 25: Clientsysteme Konfiguration

5.1.1.1 Kommunikation mittels TLS absichern

In diesem Abschnitt hat der Administrator die Möglichkeit, festzulegen, ob der Zugriff auf den Dienstverzeichnisdienst auch dann über einen ungesicherten HTTP-Kanal erfolgen kann, wenn TLS verpflichtend verwendet werden muss.

5.1.1.2 Authentifizierung von Clientsystemen

In diesem Abschnitt hat der Administrator die Möglichkeit, festzulegen, ob die verpflichtende Authentifizierung der Clientsysteme für die Nutzung des LDAP-Proxys aktiviert (Zertifikats-basiert) oder deaktiviert sein soll.

5.1.1.3 Authentifizierung des vKonnektors gegenüber Clientsystemen

In diesem Abschnitt besteht die Möglichkeit, in einem Dropdown-Menü auszuwählen, mittels welchem Zertifikat die Authentifizierung des vKonnektors gegenüber der Clientsysteme erfolgen soll. Zur Auswahl steht dabei das AK.AUT-Zertifikat der gSMC-K (*gSMC-K Zertifikat*) und ein importiertes beziehungsweise generiertes Zertifikat (*Alternatives Zertifikat*). Es kann genau ein importiertes oder generiertes Zertifikat gespeichert werden, das heißt, wird ein neues Zertifikat generiert oder importiert, so wird ein vorhandener, bestehender Eintrag überschrieben. Zu den angezeigten Zertifikatseinträgen besteht die Möglichkeit, das jeweilige Zertifikat anzuzeigen, zu exportieren und, im Falle des alternativen Zertifikats, zu löschen. Um ein neues Zertifikat zu importieren, muss ein passender PKCS#12-Keystore hochgeladen und gegebenenfalls dessen Passwort eingegeben werden.

> **Hinweis**
>
> Nach einer Änderung der Clientsystem-Konfiguration kommt es zu einem Neustart einzelner Services. Dadurch kann es zu einer Verzögerung bei der Persistierung dieser Konfigurationswerte und auch zu einer kurzzeitigen Unterbrechung der Erreichbarkeit des vKonnektors kommen. Des Weiteren ist es dem Betreiber des Highspeed-Konnektors / TI-Gateways möglich, diese Service-Neustarts anhand des Status der virtuellen Konnektor-Instanz erkennen.

Wichtig

Um ein neues *Alternatives Zertifikat* zu generieren oder zu importieren, muss die Authentifizierung des vKonnektors gegenüber Clientsystemen zuvor auf *gSMC-K Zertifikat* gesetzt und diese Konfiguration gespeichert werden, ansonsten kommt es zu einer Fehlermeldung.

Wichtig

Ohne Authentisierung des vKonnektors durch das Clientsystem (d. h. TLS-Client-Authentication über X.509-Zertifikate) können CETP-Nachrichten möglicherweise nicht authentisch, integer und vertraulich empfangen werden. Für die Authentisierung muss ein X.509-Zertifikat am Clientsystem eingebracht werden.

Wichtig

Der Administrator muss die Nutzer darüber informieren, welche Art von Verbindung zwischen Clientsystem und vKonnektor existiert.

Achtung

Eine ungesicherte Verbindung zwischen Clientsystem und vKonnektor bietet keinen Schutz gegen Man-in-the-middle-Angriffe.

Achtung

Keine oder einseitige authentisierte TLS-Verbindungen des vKonnektors können dazu führen, dass unbemerkt qualifizierte Signaturen über von Angreifern vorgegeben Dokumente erstellt werden.

Achtung

Die Konfiguration *Authentifizierung des vKonnektors gegenüber Clientsystemen* betrifft ausschließlich die Authentifizierung des vKonnektors gegenüber eines Clientsystem. Die Gegenrichtung ist davon nicht betroffen. Abhängig von dieser Konfiguration wird dabei zur Authentifizierung entweder das Kartenmaterial (AK.AUT) oder ein importiertes / generiertes Zertifikat verwendet. Wird ein RSA-Zertifikat importiert oder generiert, dessen Schlüssellänge weniger als 3000 Bit beträgt, so wird der Betriebszustand EC_TLS_Client_Certificate_Security gesetzt. Es liegt in der Verantwortung des Administrators, dass entsprechend geeignete Zertifikate ausgewählt werden.

5.1.2 Zertifikate

Im Reiter *Zertifikate* zeigt die Benutzermaske Einstellungsmöglichkeiten der zertifikatsbasierten Authentisierung von Clientsystemen (siehe Abbildung 26). Als Client-Zertifikate werden sowohl selbst signierte Zertifikate als auch nicht selbst signierte Zertifikate, welche Teil einer Kette innerhalb der importierten CA-Zertifikate sind, unterstützt. Zunächst sind im Abschnitt *Liste importierter Clientsystem-Zertifikate* alle Clientsysteme aufgelistet, für welche Zertifikate im vKonnektor gespeichert sind. In dieser Liste befindet sich einerseits der Name des Clientsystems, neben einem *Auge*-Symbol (Details zum Zertifikat können damit angezeigt werden) sowie einem *Mülleimer*-Symbol (damit kann der Eintrag gelöscht werden). Mithilfe des Buttons *Neues Zertifikat hinzufügen* können weitere Zertifikate für Clientsysteme hinzugefügt/generiert werden bzw. auch bereits bestehende Zertifikate importiert werden. Des Weiteren finden sich im Abschnitt *Liste importierter Certificate Authorities (CAs)* eine Auflistung der importierten CA-Zertifikate, welche für die Validierung der nicht selbst signierten Zertifikate

herangezogen werden. Dafür muss das entsprechend benötigte CA-Zertifikat zuerst importiert werden und danach kann ein zugehöriges nicht selbst signiertes Clientsystem-Zertifikat importiert werden. Anforderungen an CA-Zertifikate:

- nicht abgelaufen
- entweder selbst signiert oder Teil einer Kette innerhalb der importierten CA-Zertifikate
- valide Signatur
- vom Typ CA, erkennbar an der Extension *Basiseinschränkungen* mit den Werten *Kritisch: Ja* und *Zertifizierungsinstanz: Ja*

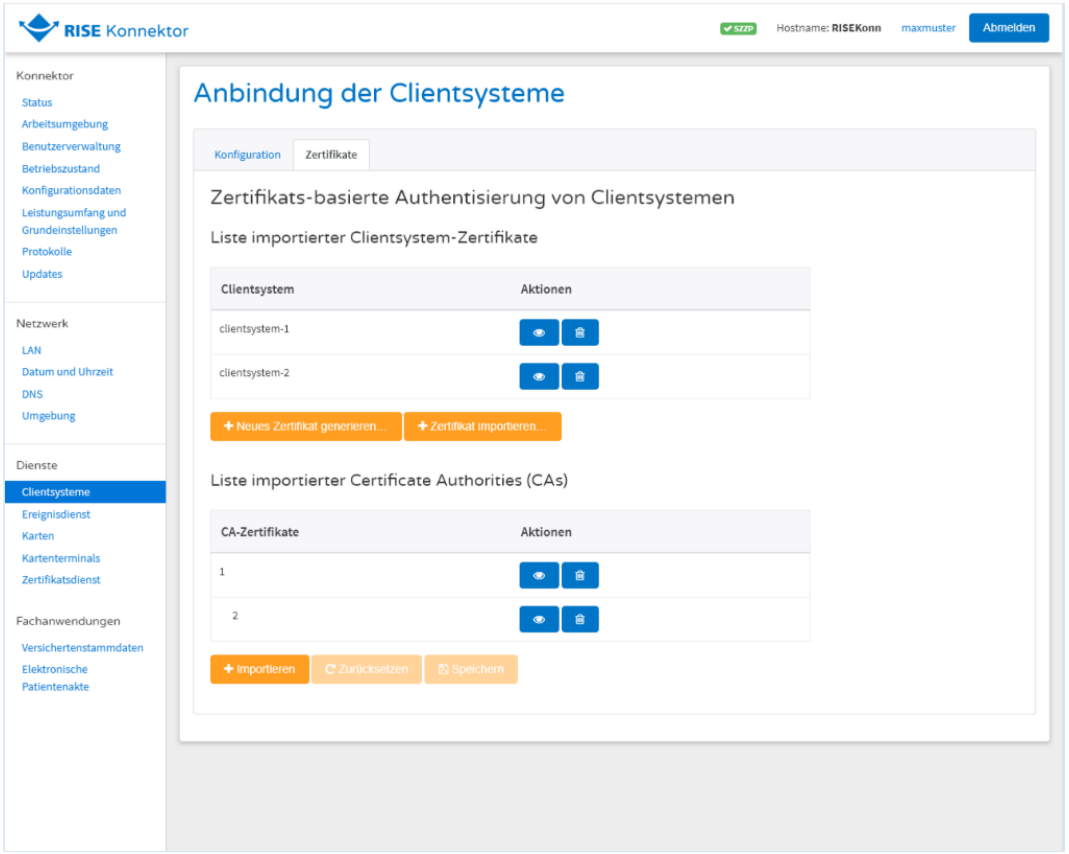

Abbildung 26: Clientsysteme Zertifikate

5.2 Kartenterminals

Dieser Abschnitt befasst sich mit der Verwaltung von Kartenterminals.

> **Hinweis**
>
> Das Verwalten der Kartenterminals ist erst nach der Konfiguration (siehe Abschnitt 3) möglich. Greifen Sie erst auf die vKonnektor-Benutzeroberfläche zu, nachdem Sie die Ergebnisse der Serverzertifikatsprüfung eingesehen haben (siehe Abschnitt 4.2).

Unter dem Menüpunkt *Kartenterminal* können Sie die verbundenen und gepairten Kartenterminals einsehen und diese verwalten.

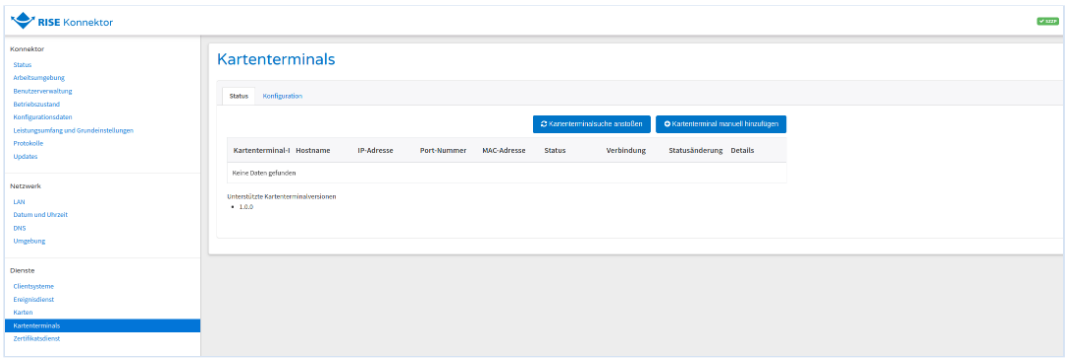

Abbildung 27: Benutzeroberfläche des vKonnektors

5.2.1 Kartenterminal hinzufügen

Um ein Kartenterminal im vKonnektor hinzuzufügen, wählen Sie *Kartenterminals manuell hinzufügen* aus. Füllen Sie die Felder wie folgt aus:

- **IP-Adresse:** Geben Sie die WireGuard-IP-Adresse der TI-Gateway-VPN-Verbindung des Gerätes an, auf dem der TI-Client installiert ist.
- **Hostname:** Geben Sie den Hostname des zu verbindenden Kartenterminals an. (*Optional*)
- **Port-Nummer:** Geben Sie die Port-Nummer an, welche Sie bei der Erstellung des Kartenterminal-Proxys als *Eingehender Port* festgelegt haben.
- **MAC-Adresse:** Geben Sie die MAC-Adresse des zu verbinden Kartenterminals an. (*Optional*)

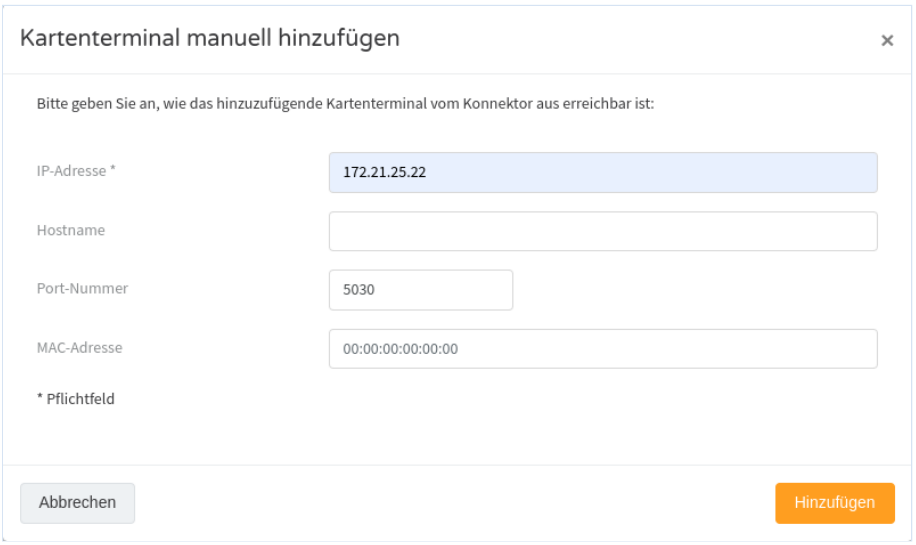

Abbildung 28: Hinzufügen des Kartenterminals

Bestätigen Sie die eingegebenen Daten durch Auswählen von *Hinzufügen*. Bei erfolgreichem Hinzufügen erscheint das Kartenterminal in der Liste und eine Erfolgsmeldung wird ausgegeben.

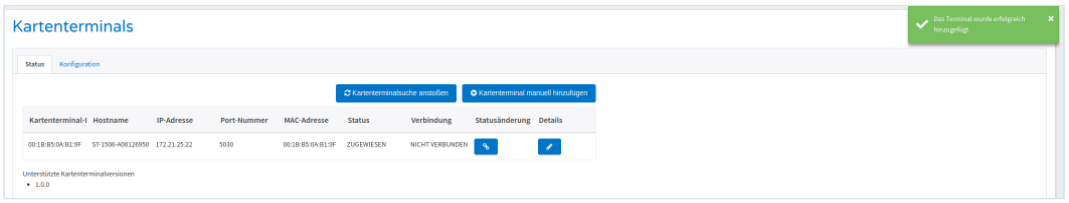

Abbildung 29: Kartenterminal erfolgreich hinzugefügt

5.2.2 Kartenterminal pairen

Um ein im vKonnektor hinzugefügtes Kartenterminal zu pairen, wählen Sie *Pairing* (Schaltfläche in der Spalte *Statusänderung*) aus.

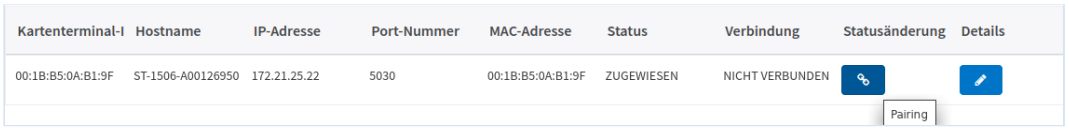

Abbildung 30: Pairen des Kartenterminals

Ein Dialog erscheint und zeigt die MAC-Adresse und den Fingerprint des Kartenterminal-Zertifikats an.

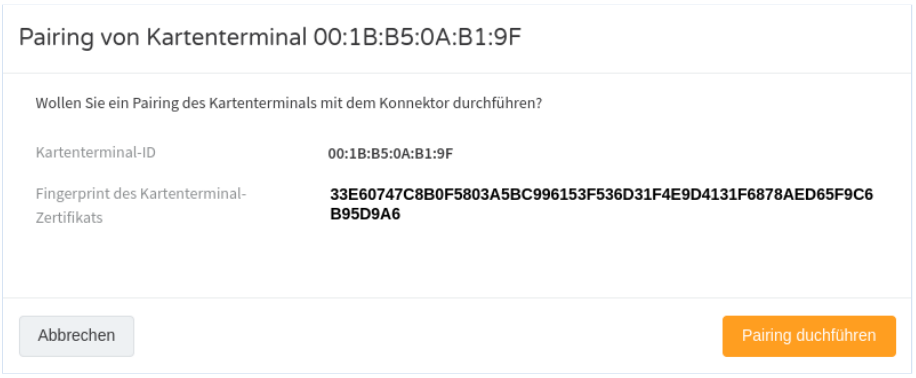

Abbildung 31: Pairingdialog

Bestätigen Sie das Pairing durch Auswahl von *Pairing durchführen*. Am Kartenterminal erscheint eine Meldung, ob das Pairing mit dem vKonnektor durchgeführt werden soll. Vergleichen Sie den Fingerprint und sofern dieser ident ist, bestätigen Sie den Vorgang. Bei erfolgreichem Pairing des Kartenterminals ändert sich das Symbol der Schaltfläche in der Spalte *Statusänderung* und eine Erfolgsmeldung wird ausgegeben.

5.3 Karten

Unter dem Menüpunkt *Karten* erhalten Sie eine Übersicht der gesteckten Karten über alle Ihre Kartenterminals und können diese verwalten. Entsprechend dem Kartentyp stehen im zugehörigen Kontextmenü unterschiedliche Aktionen zur Auswahl.

6 Logging

Der TI-Client schreibt Logdateien, die eine Analyse und ein Nachvollziehen der technischen Vorgänge ermöglichen.

Der TI-Client legt für jeden Tag eine neue Logdatei an, das Datum ist Teil des Dateinamens. Es werden die Logdateien der letzten 30 Tage gespeichert, ältere Dateien werden automatisch gelöscht. Die Logdateien können sensiblen Daten enthalten (siehe Abschnitt 3.6.2).

Kommt es im Betrieb des TI-Clients zu Problemen, kann Sie der TI-Gateway-Anbieter im Zuge des Produktsupports bitten, diese Logdateien mit einem Texteditor zu öffnen, um die Fehlersuche zu vereinfachen.

6.1 Windows

Sämtliche Logdateien der Applikation befinden sich im Verzeichnis *<installationsverzeichnis>\data\log*, wobei *<installationsverzeichnis>* dem von Ihnen bei der Installation gewählten Pfad entspricht, standardmäßig *C:\Program Files\RISE-TI-Client*. Sämtliche Logdateien, welche mit der Installation bzw. dem Update des TI-Clients zu tun haben, befinden sich unter *C:\Users\<Benutzer>\AppData\Local\Temp*, wobei *<Benutzer>* dem Namen des Benutzerkontos entspricht, mit dem die Installation bzw. das Update durchgeführt worden ist.

6.2 Linux und macOS

Sämtliche Logdateien der Applikation befinden sich im Verzeichnis */var/log/rise/ti-client/*.

7 Deinstallation

7.1 Windows und macOS

7.1.1 Windows

Die Deinstallation des TI-Clients erfolgt über die *Apps und Features*-Liste. Zur Deinstallation gehen Sie bitte in folgender Reihenfolge vor:

1. Öffnen Sie die Windows *Einstellungen* (*Windows Startmenü* > *Einstellungen* oder Windows-Taste + I).
2. Wählen Sie den Menüpunkt *Apps* aus.
3. Suchen Sie in der Liste nach der Applikation *RISE TI-Client* und wählen Sie den Eintrag aus.

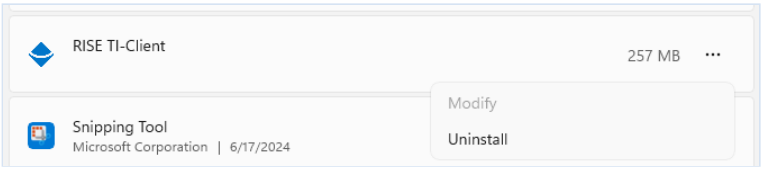

Abbildung 32: TI-Client Eintrag in Apps

4. Wählen Sie *Deinstallieren* und bestätigen Sie den Vorgang.
5. Folgen Sie den Anweisungen des Deinstallationsassistenten (siehe Abschnitt 7.1.3).
6. Entfernen Sie eventuell zusätzlich erstellte oder veränderte Regeln in der *Windows Defender Firewall* (siehe Abschnitt 3.8).

7.1.2 macOS

1. Führen Sie die Deinstallationsdatei *RISE TI-Client Deinstallationsprogramm* im Verzeichnis /opt/rise/ti-client aus.
2. Folgen Sie den Anweisungen des Deinstallationsassistenten (siehe Abschnitt 7.1.3).

7.1.3 Deinstallationsassistent

Wählen Sie aus, welche Dateien, die im Zuge der Installation und des Betriebes des TI-Clients erstellt wurden, nach der Deinstallation weiterhin verfügbar sein sollen (siehe Abbildung 33).

- **Konfigurationsordner entfernen**: Löscht die Konfiguration des TI-Clients aus dem Installationsverzeichnis.
- **Log-Dateien entfernen**: Löscht alle Logdateien, die im Zuge des Betriebes erstellt wurden.

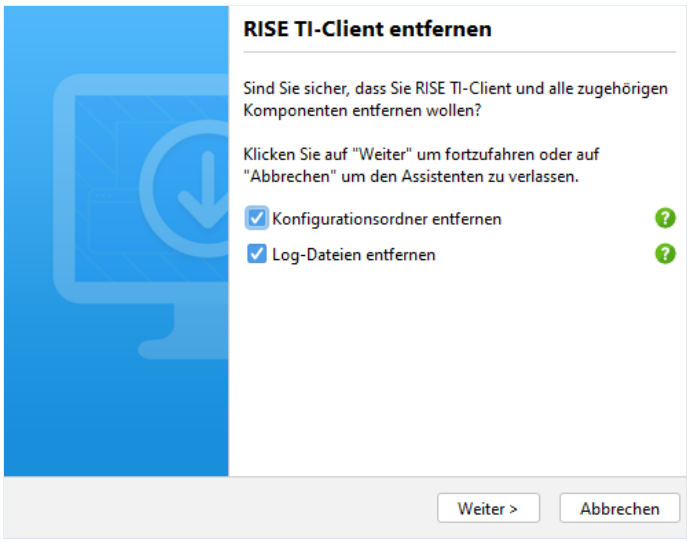

Abbildung 33: Deinstallationsoptionen des TI-Clients

7.2 Linux

Zum Deinstallieren des TI-Clients gehen Sie in folgender Reihenfolge vor:

1. Deinstallieren Sie den TI-Client:

   ```
   $ sudo apt purge rise-ti-client
   ```

2. Entfernen Sie das NAT, falls Sie eines während der Installation konfiguriert haben.
3. Entfernen Sie alle Routen von den Geräten, welche auf den vKonnektor zugreifen mussten, falls Sie während der Installation welche erstellt haben.

7.3 Docker

Um den TI-Client als Docker-Container zu deinstallieren, führen Sie folgende Schritte durch:

1. Stoppen Sie den TI-Client, falls dieser noch läuft, indem Sie folgenden Befehl im Terminal in Ihrem TI-Client-Verzeichnis (das Verzeichnis, in dem der TI-Client installiert worden ist in Abschnitt 4.1.4) ausführen:

   ```
   $ docker compose down
   ```

2. Stoppen Sie alle Services, die Sie während der Installation erstellt haben und entfernen Sie diese.
3. Entfernen Sie Ihr TI-Client-Verzeichnis vollständig.
4. Entfernen Sie das TI-Client-Docker-Image und den TI-Client-Docker-Container von Ihrem System, in dem Sie folgenden Befehl ausführen:

   ```
   $ docker rmi releases.rise-world.com/docker-ti-client-public/tigw/ti-client/public:<TI-CLIENT_VERSION>
   $ docker rm TI_Client
   ```

8 Telemetriedaten

Um eine Erfüllung der Sicherheitsanforderungen der Telematik-Infrastruktur zu gewährleisten, übermittelt jede TI-Client-Instanz regelmäßig Daten an den RISE-Support. Die Daten werden dazu genutzt, um im Rahmen des Supports bei etwaigen Update-Problemen zu unterstützen sowie statistische Berichte zu bestehenden Installationen zu erstellen. Es werden keine weiteren, als in diesem Abschnitt genannten, Daten übermittelt.

Nachfolgend finden Sie eine Übersicht, bei welchen Events welche Daten abgerufen und übermittelt werden:

8.1 Windows und macOS

Bei jedem Start der TI-Client-Anwendung und anschließend nach jeweils 24 Stunden Laufzeit:

- Betriebssystem-Typ
- Version des Betriebssystems
- Typ der Java-Laufzeitumgebung
- Version der Java-Laufzeitumgebung
- TI-Client-Version
- Status von Remote PIN+
- vKonnektor Ping Status
- WireGuard-IP-Adresse

Bei jedem Start des TI-Client Maintenence Services und anschließend nach jeweils 24 Stunden Laufzeit:

- Betriebssystem-Typ
- Version des Betriebssystems
- Typ der Java-Laufzeitumgebung
- Version der Java-Laufzeitumgebung
- TI-Client-Version
- Automatisches Update Status
- vKonnektor Ping Status
- WireGuard-IP-Adresse

Jedes Mal, wenn das Wiederverbinden eines Kartenterminals fehlschlägt:

- Betriebssystem-Typ
- Version des Betriebssystems
- Typ der Java-Laufzeitumgebung
- Version der Java-Laufzeitumgebung
- TI-Client-Version
- WireGuard-IP-Adresse

Jedes Mal, wenn ein Update-Vorgang gestartet wird:

- Betriebssystem-Typ
- Version des Betriebssystems
- Typ der Java-Laufzeitumgebung
- Version der Java-Laufzeitumgebung
- TI-Client-Version
- WireGuard-IP-Adresse
- Antwort der vKonnektor-Management-APIs

8.2 Linux

Unter Linux werden, mit einer Ausnahme, die gleichen Daten wie im Abschnitt 8.1 beschrieben, abgerufen und übermittelt.

Bei *Start des TI-Client Maintenence Services*, kann unter Linux der Status des automatischen Updates nicht abgerufen werden, da für das automatische Update kein Service installiert wird.

9 Problemlösungen (Troubleshooting)

In diesem Kapitel werden bekannte Fehlermeldungen sowie typische Störungen beschrieben, die während der Nutzung des RISE TI-Clients auftreten können. Zu jedem Eintrag werden mögliche Ursachen aufgeführt und entsprechende Lösungsschritte angeboten.

Das Ziel dieses Kapitels ist es, Benutzerinnen und Benutzern eine schnelle und nachvollziehbare Hilfestellung zur eigenständigen Problembehebung zu bieten. Dieses Kapitel wird fortlaufend aktualisiert und um weitere Einträge ergänzt, sobald neue relevante Fehlermeldungen identifiziert und analysiert wurden.

9.1 Fehler bei der Entschlüsselung der Keystores

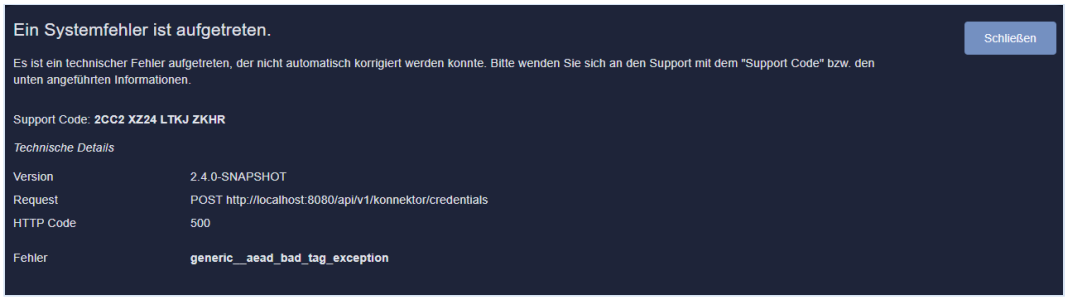

Abbildung 34: Fehler bei der Entschlüsselung der Keystores

Die Fehlermeldung aus Abbildung 34 kann erscheinen, wenn es ein Problem bei der Entschlüsselung gesicherter Informationen, wie bspw. Passwörtern oder Zertifikaten, gibt. Diese Informationen werden in *dockerisierten* Umgebungen mit dem konfigurierten *Master-Key* verschlüsselt und bei *nicht-dockerisierten* Umgebungen mit einem Schlüssel der aus den aktuellen Hardwarekomponenten abgeleitet wird. Daher kann diese Fehlermeldung darauf hindeuten, dass entweder der *Master-Key* oder die Hardwarekonfiguration des aktuell verwendeten Computers geändert wurde. In diesem Fall müssen alle PINs, Passwörter und Zertifikate neu gespeichert werden. Sollten Sie weitere Unterstützung benötigen, kontaktieren Sie bitte den Support Ihres TI-Gateway-Anbieters.

9.2 Remote PIN+ Ladeindikator bleibt dauerhaft aktiv - Kartenterminal verbleibt im Status PENDING

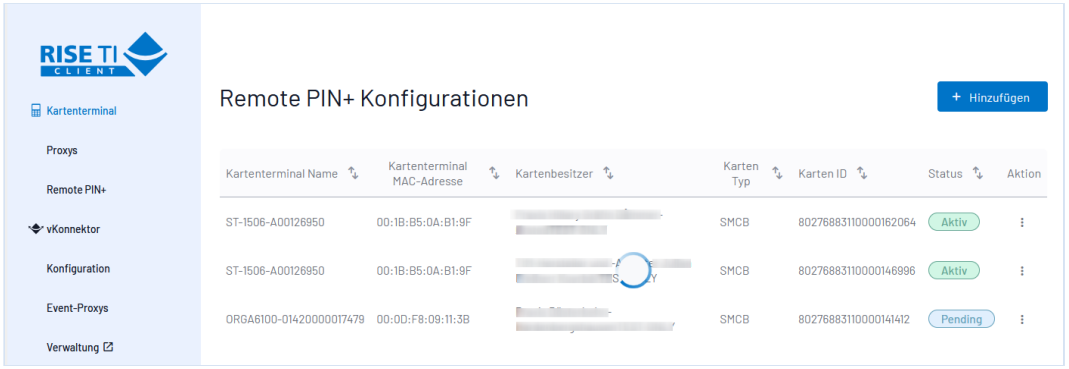

Abbildung 35: Remote PIN+ Ladeindikator dauerhaft aktiv

Der in Abbildung 35 angezeigte Fehler tritt auf, wenn im vKonnektor ein Kartenterminal als *Remote-PIN-Kartenterminal* konfiguriert wurde. In diesem Fall ist die Funktion Remote-PIN+ nicht ausführbar.

Zur Lösung des Problems, muss die Konfiguration des entsprechenden Kartenterminals als *Remote-PIN-Kartenterminal* am vKonnektor sowie die Konfiguration für Remote-PIN+ im TI-Client entfernt werden. Gehen Sie dazu folgendermaßen vor:

1. Gehen Sie in der TI-Client-Benutzeroberfläche unter Menüpunkt *vKonnektor* auf *Verwaltung* um die vKonnektor-Benutzeroberfläche in Ihrem Browser zu öffnen.
2. Entfernen Sie die Konfiguration für *Remote-PIN-Kartenterminal* des entsprechenden Kartenterminals.
3. Wechseln Sie zurück zur Registerkarte, in der die TI-Client-Benutzeroberfläche geöffnet ist. Die Registerkarte mit der vKonnektor-Benutzeroberfläche muss geöffnet bleiben und darf nicht geschlossen werden, da sie weiterhin benötigt wird.
4. Gehen Sie in der TI-Client-Benutzeroberfläche unter Menüpunkt *Kartenterminal* auf *Remote PIN+*.
5. Der Ladeindikator sollte nicht mehr angezeigt werden.
6. Entfernen Sie den Eintrag der Konfiguration für Remote PIN+ für das Kartenterminal im Status *Pending* über das 3-Punkte-Menü in der entsprechenden Zeile.
7. Schließen Sie die Registerkarte in welcher die vKonnektor-Benutzeroberfläche geöffnet wurde.
8. Richten Sie die Konfiguration für Remote PIN+ für das entfernte Kartenterminal neu ein. Folgen Sie dazu den Anweisungen unter Abschnitt 3.3.

10 Kontakt

Bei Fragen und Problemen zum TI-Client, welche nicht von Ihrem Vertragshändler bzw. Infrastrukturdienstleister beantwortet werden können, wenden Sie sich bitte per E-Mail oder telefonisch an den TI-Gateway-Anbieter.

Es wird empfohlen, in erster Instanz immer Unterstützung von Ihrem direkten Vertragshändler und Infrastrukturdienstleister einzuholen. Falls auf diesem Weg keine zufriedenstellende Lösung gefunden werden kann, ist es möglich, Kontakt zum TI-Gateway-Anbieter aufzunehmen. Auf der RISE TI-Gateway Webseite befinden sich sämtliche Kontaktinformationen.

Bilderverzeichnis

Concorde BusinessPark F
2320 Schwechat
Austria, Europe

Firmenbuch: FN 280353i
Landesgericht Korneuburg
UID: ATU62886416

www.rise-world.com
welcome@rise-world.com

RISE