Optica

RISE TIaaS Client Handbuch

Einfach. Begeisternd.

RISE TI as a service

RISE TIaaS Client

Stand: 19.09.2022
Version: 1.4.0

Inhaltsverzeichnis

1 Einleitung

Diese Bedienungsanleitung beschreibt den *RISE TI as a Service (TIaaS) Client* zur Kommunikation mit dem TIaaS Rechenzentrum (RZ) und den dort zur Verfügung stehenden Konnektoren (*vKonnektor*) sowie zur Kommunikation mit der *RISE Konnektor Verwaltungssoftware (KVS)*. Der TIaaS 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 Konnektor 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 TIaaS nutzen, und an die Administratoren im Speziellen.

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.

2 Installation

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

2.1 Systemvoraussetzungen

Der TIaaS 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 ermöglichen zu können.

2.1.1 Hardware

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

2.1.2 Netzwerkeinstellungen

Im Zuge der Installation des TIaaS Clients werden automatisch Ausnahmen für die Betriebssystem-eigene Firewall hinzugefügt. Bei der Deinstallation werden diese Ausnahmen wieder entfernt.

Werden in Ihrem Netzwerk weitere Firewalls verwendet, die die Funktion des TIaaS Clients beeinflussen, wenden Sie sich an Ihren Netzwerkadministrator.

2.1.3 Betriebssystem

Aktuell unterstützt der TIaaS Client folgende Betriebssysteme:

- Windows 10 (64-bit)
- macOS Version 11 (Big Sur) und 12 (Monterey)

2.1.4 Webbrowser

Für die korrekte Nutzung des TIaaS Clients empfehlen wir aktuell die Verwendung des Clients mit folgenden Webbrowsern:

- Google Chrome ab Version 101.0.4951.54 (64-bit)
- Microsoft Edge ab Version 101.0.1210.32 (64-Bit)
- Firefox ab Version 100.0 (64-Bit)
- Safari ab Version 15

2.1.5 Third-Party Software

Für die Installation des TIaaS Clients unter macOS ist es nötig, Homebrew zu installieren (siehe Abschnitt 2.3.1).

2.1.6 Voraussetzungen für einen sicheren Betrieb

Zusätzlich zu den beschriebenen funktionalen Anforderungen muss auch die Sicherheit der Betriebsumgebung des TIaaS 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 der Betriebsumgebung:**
  Der Benutzer ist dafür verantwortlich, dass nur gültige und vertrauenswürdige Zertifikate importiert

werden. Es finden keine technischen Prüfungen der Zertifikate durch den TIaaS Client statt. Zertifikate, denen nicht mehr vertraut wird, müssen vom Benutzer über die Konfigurationseinstellungsoberfläche ausgetauscht werden.
Der TIaaS Client speichert Zertifikate und Zugangsdaten für die verschlüsselte Kommunikation in einem Schlüsselspeicher. Das Passwort wird für jede Installation individuell generiert. Es liegt in der Verantwortung des Benutzers für eine sichere Betriebsumgebung zu sorgen und sicherzustellen, dass diese Daten geschützt bleiben, bspw. durch Installation von Betriebssystem-Updates, den Einsatz einer Firewall, Antiviren-Schutzsoftware, usw. Die Maßnahmen müssen jeweils State-Of-The-Art Standards bzw. darüber hinaus erfüllen.
Der TIaaS 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.

2.2 Kompatibilität

Der TIaaS Client wurde erfolgreich mit folgenden von der gematik zugelassenen Kartenterminals getestet:

- Ingenico Orga 6141 (Firmware Versionen 3.8.1 und 3.8.2)
- CHERRY eGK-Tastatur G87-1505 (Firmware Version 3.0.1)
- CHERRY ST-1506 (Firmware Versionen 2.0.17, 3.0.0 und 3.0.24)

Hinweis: Bitte halten Sie Ihre Kartenterminal-Firmware stets aktuell.

2.3 Vorbereitung

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

2.3.1 macOS: Installation von Homebrew

Damit der TIaaS Client unter macOS installiert werden kann, muss bereits Homebrew am Computer installiert sein. Die Installation von Homebrew erfolgt über die Kommandozeile (durch Verwendung der Applikation *Terminal*).

Um zu überprüfen, ob Homebrew bereits installiert ist, lässt sich der Befehl *which brew* in der Kommandozeile ausführen. Wird ein Dateipfad ausgegeben, so ist Homebrew bereits installiert.

Zur Installation nutzen Sie den Kommandozeilenbefehl

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Bestätigen Sie die Installation mit Enter. Bei erfolgreicher Installation zeigt das Terminal die Zeile ==> *Installation successful!* an.

2.4 Installationsprozess

Zum Start der Installation des TIaaS Clients führen Sie die, zu Ihrem Betriebssystem passende, Installationsdatei *RISE_TIaaS_Client* aus. Kurz nach dem Start der Installation wird der Setup-Assistent vorbereitet (siehe Abbildung 1).

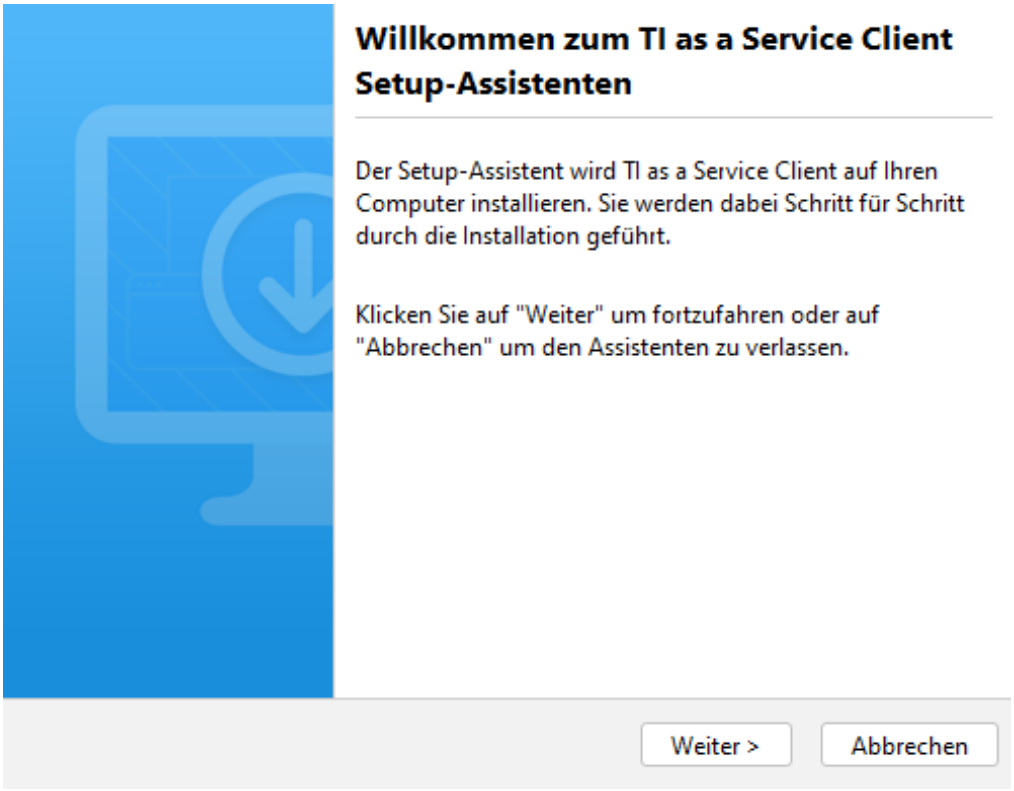

Abbildung 1: Vorbereitung des Setup-Assistenten zur Installation des TIaaS Clients

Folgende Schritte sind nun zum Abschluss der Installation notwendig:

1. **Startseite:** Folgen Sie den Anweisungen um den Installationsprozess des TIaaS Clients zu starten.
2. **Zielverzeichnis auswählen:** Es wird empfohlen, das Standard-Installationsverzeichnis nicht zu ändern.
   Warnung: TIaaS Client Installationen außerhalb des Standardverzeichnisses benötigen für jedes Update der Software manuelle Administratorberechtigung.
3. **TIaaS Client Konfigurationsdatei auswählen:** Geben Sie den Pfad zur TIaaS Client Konfigurationsdatei an, die Sie mit dem Installationspaket bereitgestellt bekommen haben. Es handelt sich um eine *.zip*-Archivdatei.
4. **Passwort für die Konfigurationsdatei eingeben:** Es handelt sich hierbei um den Bereitstellungscode, welcher im Rahmen der Produktbestellung festgelegt wurde.
5. **Administratorberechtigung für die Installation erteilen:** Für die korrekte Installation und Funktion des TIaaS Clients wird eine Administratorberechtigung benötigt.
6. **WireGuard Managementoberfläche (nur unter Windows):** Mit der TIaaS Client Installation wird auch der WireGuard VPN Client installiert. Dieses Tool wird für die Verbindung zum TIaaS RZ und

somit zum Konnektor benötigt. Die WireGuard Managementoberfläche erscheint kurz. Es ist keine Eingabe erforderlich.

7. **Abschluss der Installation (nur unter Windows):** Wählen Sie aus, ob der TIaaS Client nach Abschluss der Installation gestartet werden soll.

8. Nach der Installation wird der TIaaS Client automatisch bei der Betriebssystem-Benutzeranmeldung nach jedem Neustart im Hintergrund gestartet.

Hinweis: Der TIaaS Client wird als Applikation im Hintergrund gestartet. Um die grafische Benutzeroberfläche aufzurufen und die restlichen Konfigurationsschritte durchzuführen, die für die Verwendung des Clients notwendig sind, fahren Sie mit Abschnitt 3 und Abschnitt 8 fort.

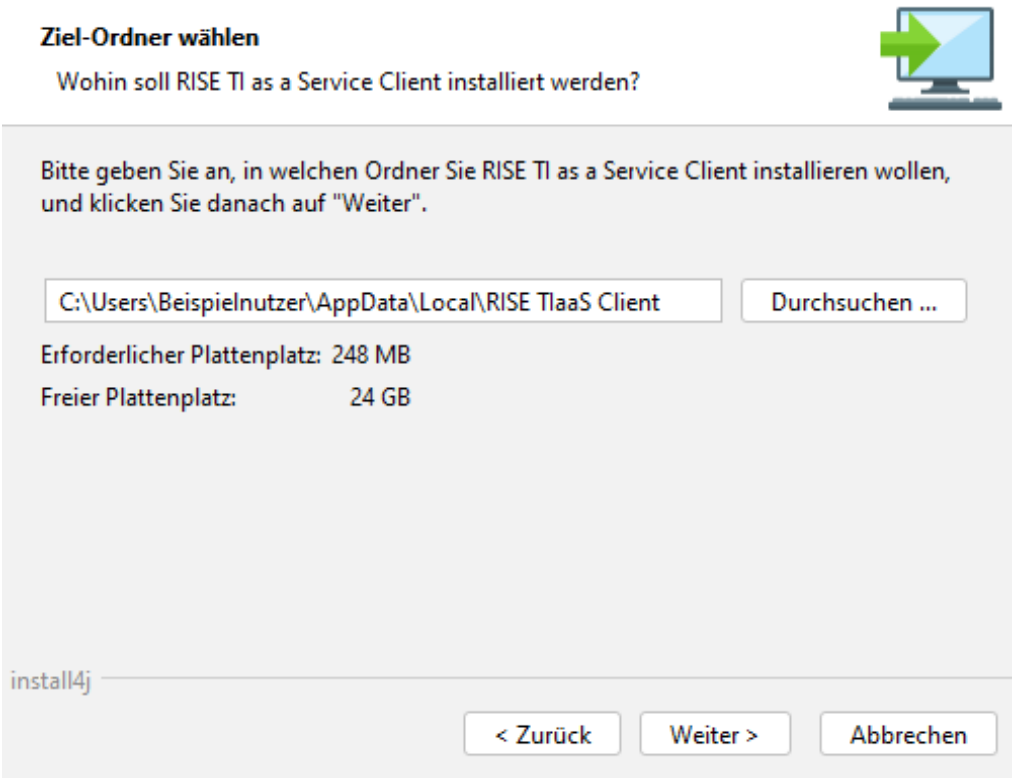

Abbildung 2: Auswahl des Installationsverzeichnisses unter Windows

Hinweis: Die eingespielte Konfigurationsdatei darf nicht an Dritte weitergegeben werden. Aus Sicherheitsgründen wird empfohlen die Konfigurationsdatei nach der Installation zu löschen.

3 Start und Überblick der Anwendung

Standardmäßig startet der TIaaS Client als Anwendung bei der Benutzer-Anmeldung auf dem Betriebssystem automatisch im Hintergrund. Sollte dies nicht der Fall sein oder sollten Sie den TIaaS Client beendet haben, müssen Sie den Client manuell starten indem Sie das Startmenü öffnen. Starten Sie dann die Anwendung *RISE TIaaS Client* durch Auswahl des entsprechenden Listeneintrags.

Hinweis: Es ist immer nur die Ausführung *einer* Instanz des TIaaS Clients erlaubt. Sollte die Anwendung bereits (im Hintergrund) laufen, ist kein erneuter Start möglich.

Nach dem Start der Anwendung kann die grafische Benutzeroberfläche des TIaaS Clients angezeigt werden. Dazu rufen Sie die URL *localhost:8080* über einen Webbrowser (siehe Abschnitt 2.1.4) auf.

3.1 Startseite

Nach dem Öffnen der Anwendung im Webbrowser wird die Startseite des TIaaS Clients angezeigt wie in Abbildung 3 dargestellt. Von hier aus können die folgenden Menüpunkte erreicht werden:

- **Kartenterminals**: Hier können Sie ein Kartenterminal hinzufügen oder entfernen (siehe Abschnitt 5).
- **Karten**: Hier erhalten Sie eine Übersicht der gesteckten Karten und können sie verwalten (siehe Abschnitt 6).
- **Konnektor**: Hier können Sie den Verbindungsstatus zu Ihrem vKonnektor einsehen (siehe Abschnitt 4).
- **Konfiguration**: Hier können Sie Zertifikate für die Verbindung zum TIaaS RZ importieren und speichern (siehe Abschnitt 8).

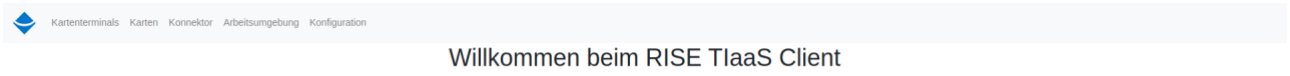

Abbildung 3: Begrüßungsbildschirm

Bitte beachten Sie:

- Beim Schließen der Benutzeroberfläche wird der TIaaS Client weiterhin im Hintergrund ausgeführt.
- Der TIaaS Client wird nach jedem Neustart des Betriebssystems automatisch nach der Benutzer-Anmeldung gestartet.

4 Konnektor

Unter dem Menüpunkt *Konnektor* lässt sich der aktuelle Verbindungsstatus zum vKonnektor im TIaaS RZ einsehen. Der Verbindungsstatus mit dem vKonnektor wird regelmäßig im Hintergrund überprüft und gemeinsam mit dem Datum und der Uhrzeit der letzten Abfrage in der Benutzeroberfläche dargestellt (siehe Abbildung 4 und Abbildung 5). Bei Verfügbarkeit des vKonnektors wird ein grünes, bei Nichtverfügbarkeit ein rotes Symbol angezeigt. Zudem kann über Auswahl von *Status manuell abfragen* die Prüfung des Verbindungsstatus jederzeit manuell gestartet werden.

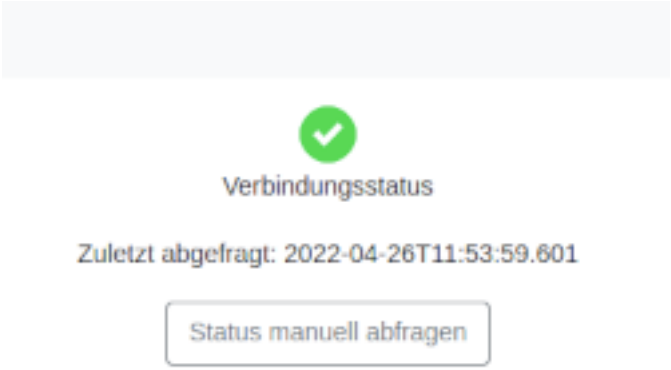

Abbildung 4: Erfolgreicher Verbindungsstatus des Konnektors

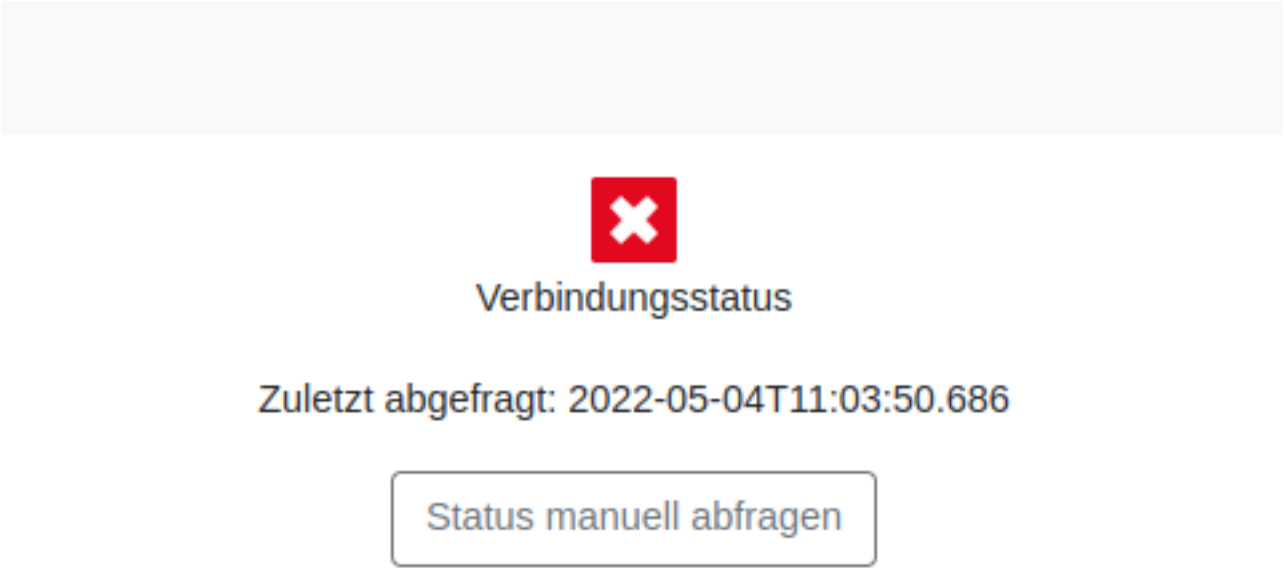

Abbildung 5: Nicht erfolgreicher Verbindungsstatus

5 Kartenterminals

Unter dem Menüpunkt *Kartenterminals* können Kartenterminals hinzugefügt und mit dem vKonnektor gepaired werden. Dafür muss das entsprechende *Netzwerkinterface* ausgewählt und die IP-Adresse des Kartenterminals eingegeben werden (siehe Abbildung 6).

Abbildung 6: Kartenterminals hinzufügen

5.1 Kartenterminalübersicht

Wenn Kartenterminals mit dem TIaaS Client verbunden sind, werden diese in der Kartenterminalübersicht dargestellt, siehe Abbildung 7. Es können bis zu 20 Kartenterminals mit dem TIaaS Client verbunden sein.

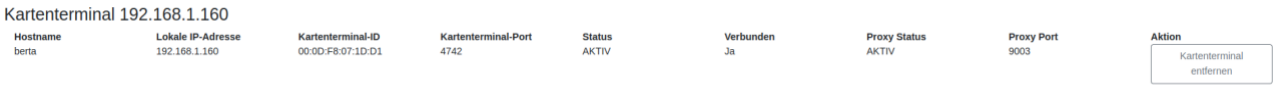

Abbildung 7: Kartenterminalübersicht

Hinweis: Es werden nur Kartenterminals aufgelistet, die mit der aktiven TIaaS Client Installation verbunden sind.

5.2 Kartenterminal hinzufügen und pairen

Um ein Kartenterminal hinzuzufügen, muss sowohl ein *Netzwerkinterface* als auch die *Kartenterminal IP-Adresse* angegeben werden (siehe Abbildung 8).

- **Netzwerkinterface**: Name und IP-Adresse des Netzwerkinterfaces, mit dem das Kartenterminal erreichbar ist. Die IP-Adresse des Netzwerkinterfaces befindet sich üblicherweise im selben Sub-Netz wie das Kartenterminal (beispielsweise *192.168.1.x*).

- **Kartenterminal IP-Adresse**: Die IP-Adresse, über die das oberhalb ausgewählte Netzwerkinterface das Kartenterminal erreichen kann. Wenden Sie sich an Ihren Netzwerkadministrator, wenn Sie nicht über Ihre Kartenterminal IP-Adresse verfügen.

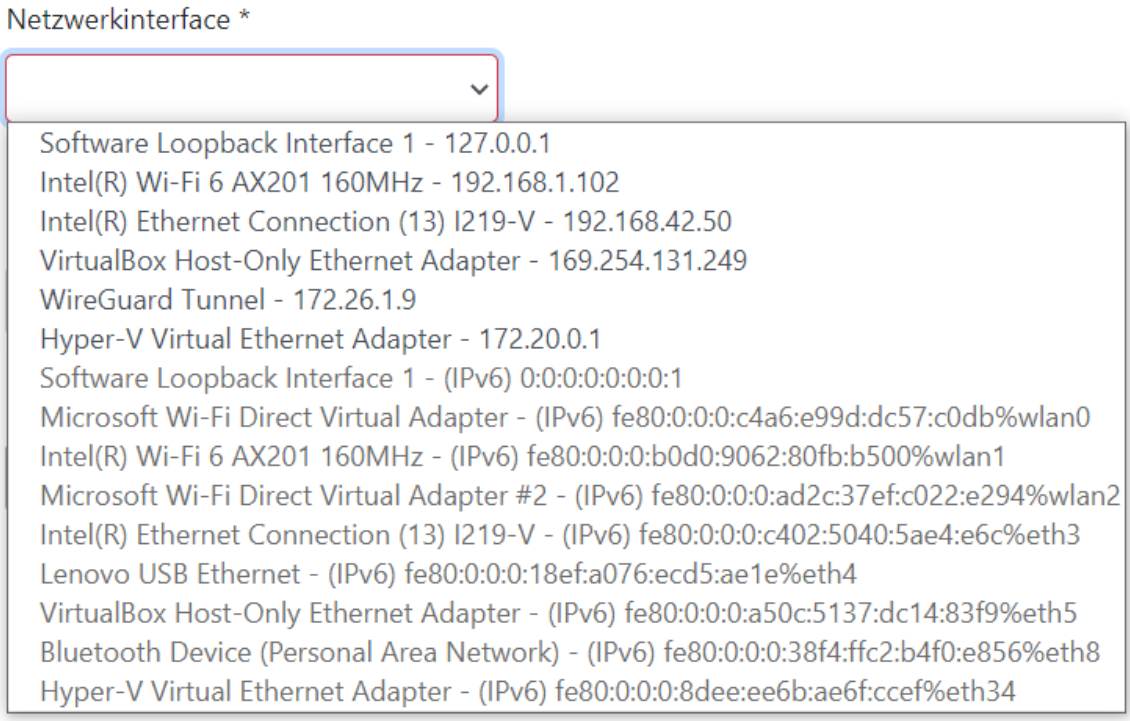

Abbildung 8: Auswahl des Netzwerkinterfaces

Um ein Kartenterminal mit den eingegebenen Daten zu verbinden, starten Sie den Prozess über die Auswahl von *Hinzufügen und Pairing starten*. Dabei werden folgende Schritte vom TIaaS Client durchgeführt:

1. Anhand der eingegebenen IP-Adresse wird ein SICCT Service Discovery Paket an das Kartenterminal gesendet.
2. Das Kartenterminal antwortet dem TIaaS Client mit einem SICCT Service Announcement.
3. Der TIaaS Client entnimmt dem SICCT Service Announcement vom Kartenterminal die für das Pairing benötigten Informationen.
4. Danach startet der TIaaS Client die Verbindung und das Pairing des Kartenterminals mit dem vKonnektor. Eine Meldung am Display des Kartenterminals bestätigt das erfolgreiche Pairing.
5. Nach dem erfolgreichen Pairing erscheint ein Dialog zur Hinterlegung der SICCT Admin-Session PIN.[1]
6. Es erscheint ein Hinweis zur Hinterlegung des Informationsmodells; dieses muss im TIaaS Client konfiguriert sein, damit das Kartenterminal erfolgreich mit dem vKonnektor kommunizieren kann.

[1] SICCT Admin-Session PIN: Die Kartenterminal-PIN für die SICCT Admin-Session, die vom Konnektor bei Kartenterminal-Firmware Updates aufgebaut wird.

7. Das erfolgreich hinzugefügte und verbundene Kartenterminal wird in der Kartenterminalübersicht angezeigt.

Sollte das Pairing des Kartenterminals fehlschlagen, wird das Kartenterminal in der Kartenterminalübersicht nicht angezeigt.

Hinweis: Bei der ersten Inbetriebnahme des TIaaS Clients und nach dem ersten erfolgreichen Pairing eines Kartenterminals über den Client, konfigurieren Sie bitte Ihre gewünschte Arbeitsumgebung, die Sie für die Nutzung mit dem vKonnektor verwenden möchten. Nähere Informationen finden Sie dazu im Kapitel Abschnitt 7

Hinweis: Falls Sie ein Primärsystem (z.B. eine Praxisverwaltungssoftware) verwenden und dort ein eigenes TLS-Client-Zertifikat für die Kommunikation mit dem TIaaS RZ verwenden möchten, übermittelt Sie bitte dieses TLS-Client-Zertifikat an den TIaaS Anbieter.

Hinweis: Es ist wichtig, dass Sie sich das Einstellungspasswort Ihres Kartenterminals gut merken, da es für Operationen (wie z.B. Pairing und Firmware Update) verwendet wird.

5.3 Kartenterminal entfernen

Ein verbundenes Kartenterminal kann in der Kartenterminalübersicht durch die Auswahl von *Kartenterminal entfernen* wieder entfernt werden. Dafür muss die Auswahl der Aktion durch die Anzeige *Wollen Sie das Kartenterminal wirklich entfernen?* bestätigt werden.

Hinweis: Nur Kartenterminals, die durch den TIaaS Client mit dem vKonnektor verbunden wurden, können vom Benutzer entfernt werden.

5.4 SICCT Admin-Session PIN hinterlegen

Das Hinterlegen oder Aktualisieren der SICCT Admin-Session PIN[2] lässt sich durch die Auswahl von *Admin-Session PIN des Kartenterminals hinterlegen…* im Kontextmenü des Kartenterminals auslösen.

6 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.

6.1 Kartenübersicht

In der Kartenübersicht werden alle Ihre gesteckten Karten über alle Kartenterminals dargestellt (siehe Abbildung 9). Dabei werden der Kartentyp, das Kartenterminal mittels der ID und MAC-Adresse sowie das

[2] SICCT Admin-Session PIN: Die Kartenterminal-PIN für die SICCT Admin-Session, die vom Konnektor bei Kartenterminal-Firmware Updates aufgebaut wird.

Einsteckdatum und das Ablaufdatum des Zertifikates angezeigt. Zudem können die einzelnen angezeigten Karten über ein Kontextmenü verfügen, über das ausgewählte PIN-Operationen an den Karten in den verbundenen Kartenterminals durchgeführt werden können. Nach Abfrage über das Kontextmenü wird ein Status mit zusätzlichen Informationen dargestellt.

Abbildung 9: Kartenübersicht

6.2 Kartenaktionen

Nachdem die Karten aufgelistet wurden, stehen Ihnen für die Kartentypen SMC-B und HBA durch Auswahl des Kontextmenüs verschiedene Operationen zur Verfügung. Dabei handelt es sich jeweils um PIN-Operationen, die mit einer Erfolgsmeldung oder einer Fehlermeldung (siehe Abschnitt 12.4) abgeschlossen werden.

Folgende Aktionen stehen zur Verfügung:

- Für SMC-B Karten (siehe auch Abbildung 10):
  - PIN-Status abfragen
  - PIN verifizieren
  - PIN ändern
  - PIN entsperren

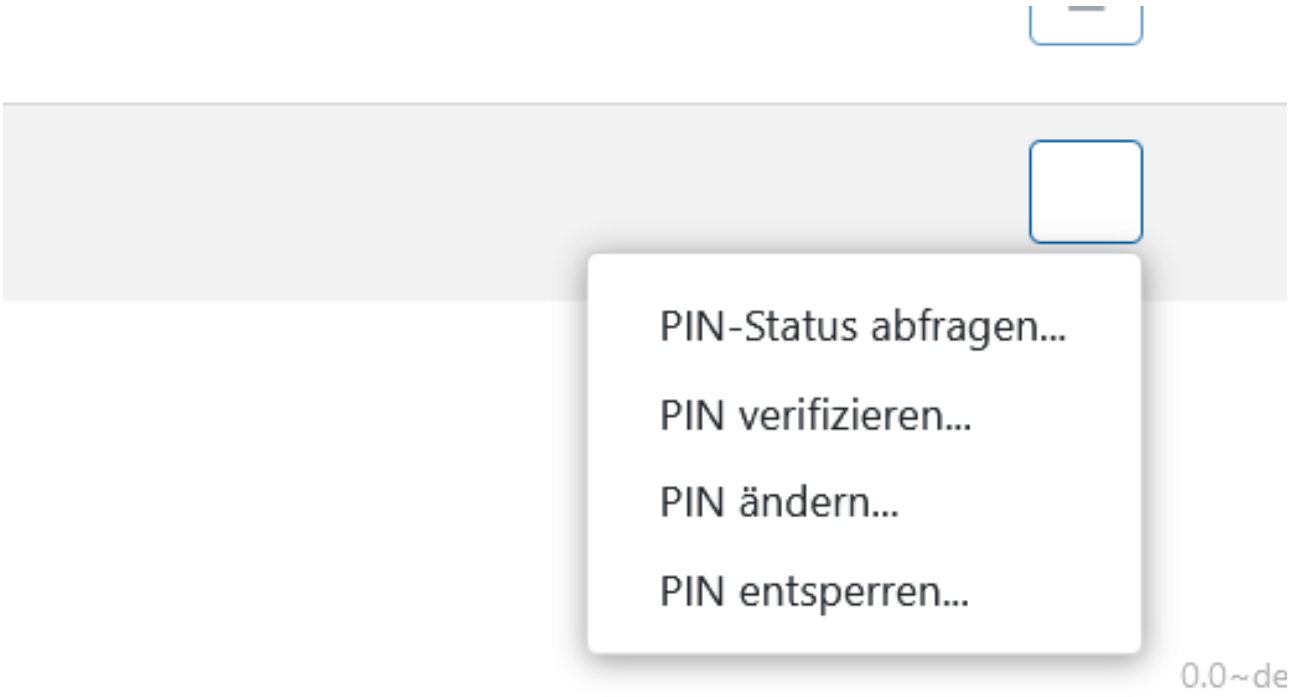

Abbildung 10: PIN-Operationen für SMC-B Karten

- Für HBA Karten (siehe auch Abbildung 11)
  - CH-PIN-Status abfragen
  - CH-PIN ändern
  - CH-PIN entsperren
  - QES-PIN-Status abfragen
  - QES-PIN ändern
  - QES-PIN entsperren

Hinweis: Nach der Auswahl einer Operation beachten Sie bitte die Anzeige an Ihrem Kartenterminal, in dem die betreffende Karte gesteckt ist.

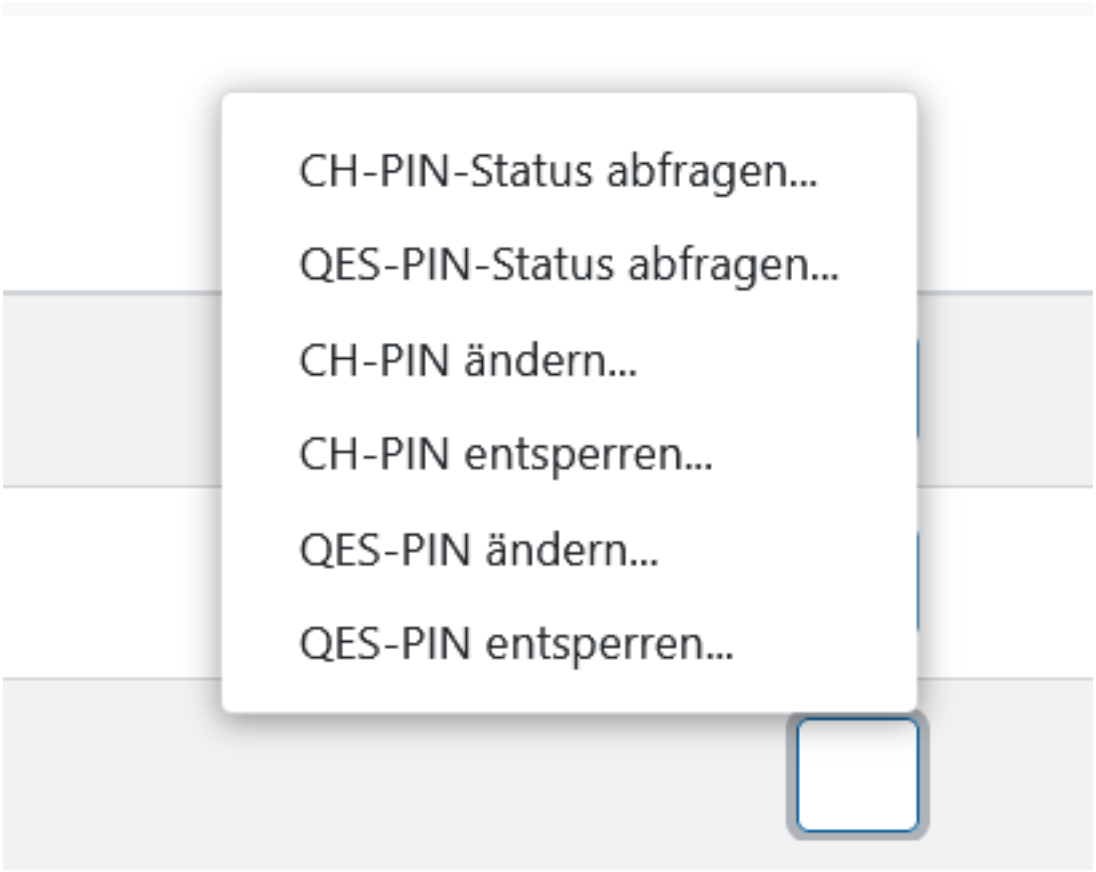

Abbildung 11: PIN-Operationen für HBA Karten

6.2.1 PIN-Status abfragen

Für transportgeschützte PINs wird die Art des Transportschutzes angegeben. Für PINs kann die Anzahl der noch verbleibenden Versuche für PIN-Verifikationen ermittelt werden oder ob die PIN bereits verifiziert wurde.

Neben der PIN für SMC-B Karten gibt es bei HBA Karten sowohl die QES-PIN für die qualifizierte elektronische Signatur und die CH-PIN für die Verschlüsselungs- und Authentifizierungsfunktionalität.

Hinweis: Wenn es für einen Kartentyp mehrere verschiedene PINs gibt, können die Operationen auf PIN-Ebene ausgewählt werden.

6.2.2 PIN verifizieren

Um eine SMC-B Karte freizuschalten, kann im TIaaS Client die Verifikation einer PIN ausgelöst werden. Bitte achten Sie auf die Meldung am Display des Kartenterminals und bestätigen Sie die Verifikation.

Bei erfolgreicher Verifikation wird der PIN-Status dargestellt, ansonsten erscheint eine Fehlermeldung entsprechend Abschnitt 12.4.

6.2.3 PIN ändern

Über die entsprechende Auswahl im Kontextmenü kann eine PIN geändert werden. Wird diese Operation ausgewählt, ist am Kartenterminal sowohl die alte als auch die neue PIN einzugeben.

Bei erfolgreicher Änderung wird eine Erfolgsmeldung angezeigt, ansonsten erscheint eine Fehlermeldung entsprechend Abschnitt 12.4.

6.2.4 PIN entsperren

Wenn eine PIN blockiert wurde, kann eine Freischaltung durch die entsprechende Auswahl im Kontextmenü der Karte ausgelöst werden. Dabei muss zunächst am PIN-Pad des Kartenterminals ein PUK eingegeben werden. Anschließend kann ebenso am Kartenterminal eine neue PIN gesetzt werden. Abschließend wird der Zähler für PIN-Eingabeversuche auf den Anfangswert zurückgesetzt.

7 Arbeitsumgebung

Unter dem Menüpunkt *Arbeitsumgebung* können Sie Mandanten, Arbeitsplätze und Clientsysteme dem vKonnektor zuweisen und weiters die Zuordnungen von Mandanten, SMC-B Karten, Arbeitsplätzen und Clientsystemen vornehmen.

Hinweis: Aufgrund von Konnektorbeschränkungen sind die Namen von Entitäten der Arbeitsumgebung auf maximal 31 Zeichen beschränkt. Es dürfen nur Groß- und Kleinbuchstaben, Zahlen und Bindestriche sowie Unterstriche verwendet werden. Andere Sonderzeichen und Umlaute sind nicht zulässig.

Das Menü der Arbeitsumgebung ist in zwei Bereiche eingeteilt, die ähnlich funktionieren.

7.1 Entitäten

Der obere Teil der Ansicht der Arbeitsumgebung dient der Verwaltung der Entitäten der Arbeitsumgebung und ist in Abbildung 12 dargestellt. Die Assoziationen dieser Entitäten miteinander und mit Kartenterminals sowie SMC-B Karten bilden die Arbeitsumgebung, die dem vKonnektor hinzugefügt werden kann.

Hinweis: Alle hinzugefügten und gelöschten Entitäten bleiben nur temporär gespeichert bis diese durch Auswahl von *Einstellungen speichern* an den vKonnektor übertragen werden. Beim Verlassen oder Aktualisieren dieser Seite ohne vorheriger Übertragung an den vKonnektor werden alle Änderungen verworfen.

1. **Entitäteneingabe:** Hier fügen Sie einen Namen für eine neue Entität ein.
   - Bei Erstellung eines neuen Mandanten erscheint dieser in der Übersicht der Arbeitsumgebung.
   - Arbeitsplätze lassen sich in der Übersicht der Arbeitsumgebung Mandanten zuweisen.
   - Clientsysteme lassen sich in der Übersicht der Arbeitsumgebung Mandanten zuweisen.

2. **Hinzufügen der Entität:** Nach der Eingabe des Namens erstellen Sie die Entität durch Auswahl von *Hinzufügen*.
3. **Löschen einer Entität:** Durch die Auswahl des Löschen-Symbols wird die Entität aus der Liste der vorhandenen Entitäten gelöscht.

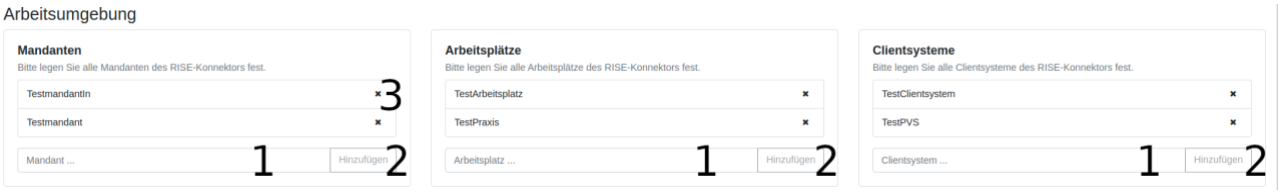

Abbildung 12: Entities

7.2 Mandantenansicht

Der untere Teil der Seite bildet die Arbeitsumgebung des vKonnektors ab wie in Abbildung 13 dargestellt.

- Die angelegten Mandanten erhalten jeweils einen eigenen Eintrag im Akkordeon-Menü.
- Nach Auswahl eines Mandanten können weitere Einstellungen verändert werden.
- Alle Entitäten lassen sich über die vorhandenen Dropdown-Menüs zuweisen. Bei SMC-B Karten und Clientsystemen ist das möglich ohne den Mandanten aufzuklappen.
- Bei Clientsystemen und Arbeitsplätzen ist es möglich, mehrere Zuweisungen pro Mandant durchzuführen.
- Per Auswahl auf das *X*-Symbol lassen sich Zuweisungen der Entitäten aufheben.

Hinweis: Alle getätigten Einstellungen bleiben nur temporär gespeichert bis diese durch Auswahl von *Einstellungen speichern* an den vKonnektor übertragen werden. Beim Verlassen oder Aktualisieren dieser Seite ohne vorheriger Übertragung an den vKonnektor werden alle Änderungen verworfen.

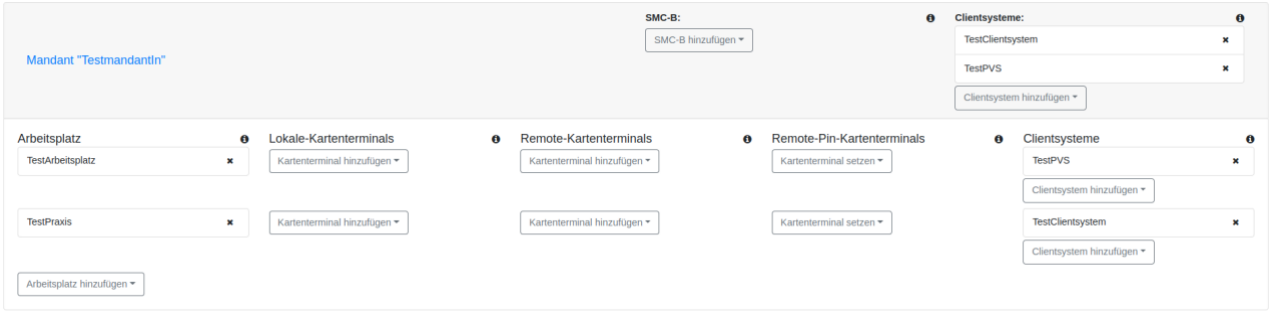

Abbildung 13: Mandantenansicht

8 Konfiguration

In diesem Abschnitt werden die Konfigurationsmöglichkeiten des TIaaS Clients beschrieben.

Wurden die für den TIaaS Client benötigten Zertifikate bei der Installation nicht eingespielt, müssen grundlegende Einstellungen in der grafischen Benutzeroberfläche vorgenommen werden bevor der TIaaS Client verwendet werden kann. Dazu müssen vor der Inbetriebnahme auch entsprechende

Zertifikate und Schlüsselmaterial lokal vorhanden sein, die für den Betrieb notwendig sind. Diese befinden sich innerhalb des bereitgestellten Konfigurationsarchivs (*.zip*-Datei) Der Nutzer muss sicherstellen, dass nur vertrauenswürdige Zertifikate und Schlüssel eingebracht werden.

Die entsprechenden Zertifikate und das Schlüsselmaterial müssen vom TIaaS Anbieter über einen sicheren Kanal unter Wahrung der Vertraulichkeit und Integrität zur Verfügung gestellt werden. Dies gilt sowohl initial für die Ersteinrichtung als auch periodisch vor Ablauf des jeweils aktuell verwendeten Zertifikats.

In der grafischen Benutzeroberfläche unter dem Menüpunkt *Konfiguration* können Sie Zertifikate für die Verbindung zum TIaaS RZ importieren und speichern (siehe Abschnitt 8.1). Weitere Konfigurationsmöglichkeiten sind direkt über die TIaaS Client-Konfigurationsdatei möglich (siehe Abschnitt 8.2), die bereits im Rahmen der Installation eingespielt wurde.

8.1 Konfiguration der TLS-Kommunikation

Unter dem Menüpunkt *Konfiguration* ist es möglich die Zertifikate und das Schlüsselmaterial für die TLS-Kommunikation zum TIaaS RZ in den lokalen KeyStore und TrustStore zu importieren und zu speichern (siehe Abbildung 14).

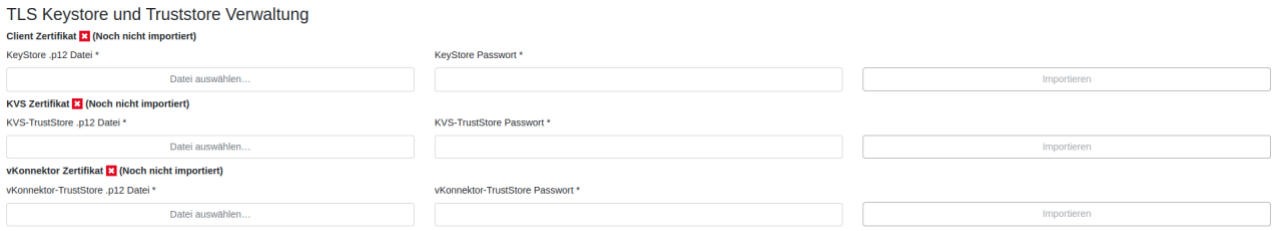

Abbildung 14: Konfiguration der TLS-Zertifikate

Für den erfolgreichen TLS-Verbindungsaufbau und die verschlüsselte Kommunikation zum vKonnektor sind folgende Zertifikate und Schlüsselmaterial notwendig:

1. **Client Zertifikat**:
   Auswahl einer lokal verfügbaren passwortgeschützten **.p12*-Datei mit dem TLS-Client-Zertifikat und privaten Schlüssel für die zertifikats-basierte Client-Authentifizierung mit dem TIaaS RZ sowie Eingabe des Passworts.

2. **KVS Zertifikat:**
   Auswahl einer lokal verfügbaren passwortgeschützten **.p12*-Datei mit dem TLS-Server-Zertifikat für die Authentifizierung der KVS im TIaaS RZ sowie Eingabe des Passworts.

3. **vKonnektor Zertifikat:**
   Auswahl einer lokal verfügbaren passwortgeschützten **.p12*-Datei mit dem TLS-Server-Zertifikat für die Authentifizierung des vKonnektors im TIaaS RZ sowie Eingabe des Passworts.

Für jedes nötige Zertifikat wurde Ihnen in Ihrem Installationspaket eine **.p12*-Datei zur Verfügung gestellt. Um jedes dieser Zertifikate importieren zu können, wählen Sie im ersten Schritt *Datei auswählen…* und wählen Sie das entsprechende Verzeichnis mit der Datei aus.

Im nächsten Schritt geben Sie das erforderliche Passwort zur ausgewählten Zertifikats-Datei ein, das Ihnen über einen sicheren Kommunikationskanal bereitgestellt wurde. Dies ist von der Übermittlung des Installationspakets unabhängig. Ohne korrektes Passwort schlägt der Import der Zertifikats-Datei fehl.

Um den Import des Zertifikats abzuschließen, wählen Sie *Importieren* (bei bereits bestehendem Zertifikat: Auswahl von *Aktualisieren*). Nach erfolgreichem Import wird ein neben dem erfolgreich hochgeladenen Zertifikat ein grünes Symbol angezeigt (siehe Abbildung 15).

Abbildung 15: Erfolgreich hochgeladenes Zertifikat

Alle Zertifikate müssen korrekt hinterlegt werden, um den ordnungsgemäßen und sicheren Betrieb des TIaaS Clients zu gewährleisten.

8.2 Konfiguration der Anwendung

Eine initiale Konfiguration des TIaaS Clients wird Ihnen vom TIaaS Anbieter im Rahmen des Installationspakets in Form einer Konfigurationsdatei *TIC_Configuration_<Name>.yml* zur Verfügung gestellt. Diese Konfiguration muss während der Installation eingespielt werden (siehe Abschnitt 2), sodass sie beim erstmaligen Start der Anwendung bereits vorliegt.

Nach der Installation kann die Konfiguration nur geändert werden, indem die Konfigurationsdatei über einen Editor geöffnet und editiert wird.

Hinweis: Führen Sie Änderungen in der Konfigurationsdatei nur im Zuge der Problembehandlung gemeinsam mit dem TIaaS Anbieter durch. Eine falsche Konfiguration kann den ordnungsgemäßen und sicheren Betrieb des TIaaS Clients stören.

In der Konfigurationsdatei des TIaaS Clients können über bereitgestellte Konfigurationsmöglichkeiten Einstellungen vorgenommen werden. Die Konfigurationsdatei befindet sich im Konfigurationsverzeichnis des TIaaS Clients *riseTic* im Home-Verzeichnis des Benutzers. Unter Windows ist die Datei unter *C:\Users\<Username>\.config\riseTic\application.yml* zu finden.

In Tabelle 1 sind die Konfigurationsmöglichkeiten mit Name in der Konfigurationsdatei, Beschreibung und Datentyp aufgelistet. Der Inhalt der Konfigurationsdatei ist von der jeweiligen Umgebung abhängig und ist entsprechend befüllt. Ist in der Konfigurationsdatei eine Einstellung nicht vorhanden, so wird vom TIaaS Client ein Default-Wert angenommen. Wenn ein anderer Wert als der Default-Wert verwendet werden soll, muss die Konfigurationseinstellung, falls noch nicht vorhanden, hinzugefügt und entsprechend gesetzt werden. Dabei muss beachtet werden, dass URLs mit einem “/” escaped werden.

Tabelle 1: Konfigurationsmöglichkeiten

Name in der Konfigurationsdatei	Beschreibung	Datentyp
tiaas.client.kvs.tic-id-header	Identifier des TIaaS Clients	String
tiaas.client.kvs.url	IP-Adresse des TIaaS KVS im RZ	IP-Adresse
tiaas.client.wireguard.ip	IP-Adresse des VPN	IP-Adresse
tiaas.client.konnektor.url	IP-Adresse des vKonnektors	IP-Adresse

8.3 Kartenterminal-Konfiguration

Weiters befindet sich die Datei *application-card-terminal.yml* im Konfigurationsverzeichnis des TIaaS Clients. Unter Windows ist die Datei unter *C:\Users\<Username>\.config\riseTic\application-card-terminal.yml* zu finden. Diese enthält die Pairing-Informationen des Kartenterminals und wird nach dem ersten Pairing-Versuch eines Kartenterminals angelegt.

Diese Konfiguration kann nur geändert werden, indem die Konfigurationsdatei über einen Editor geöffnet und editiert wird, und sollte nur im Zuge der Problembehandlung (siehe Abschnitt 12.3) in Abstimmung mit dem TIaaS Anbieter verändert werden. Die Kartenterminalport-Informationen lassen sich von Netzwerkadministratoren aus dieser Datei auslesen.

9 Logging

Der TIaaS Client schreibt Logdateien, die eine Analyse und ein Nachvollziehen der technischen Vorgänge ermöglichen. Die Logdateien befinden sich im Unterordner *log* des Applikationsverzeichnisses des TIaaS Clients *riseTic* im Home-Verzeichnis des Benutzers. Unter Windows ist das Verzeichnis unter *C:\Users\<Username>\riseTic\log* zu finden.

Bei jedem Start des TIaaS Clients wird eine neue Logdatei angelegt. Die Logdateien enthalten keine sensiblen Daten.

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

10 Updates

10.1 TIaaS Client

Es werden regelmäßig Updates des TIaaS Clients zur Verfügung gestellt. Die Abfrage nach neuen Updates erfolgt automatisch während der TIaaS Client ausgeführt wird. Bei Verfügbarkeit eines neuen Updates

wird dieses im Hintergrund heruntergeladen und beim nächsten Start des TIaaS Clients wird das Installationspaket installiert.

Updates, die wesentliche Änderungen an der Betriebssystem-Konfiguration vornehmen, müssen gegebenenfalls manuell Administratorberechtigungen erteilt werden, um die erfolgreiche Funktionalität des TIaaS Clients zu gewährleisten.

Hinweis: Falls Sie den TIaaS Client nicht in das Standard-Installationsverzeichnis installiert haben, kann es notwendig sein, dem Update-Installations-Assistenten Administratorberechtigungen zu erteilen (siehe Abschnitt 2).

10.2 WireGuard

Neben der TIaaS Client Anwendung wird bei der Installation auch der WireGuard VPN Client auf Ihrem Betriebssystem installiert. Für WireGuard werden ebenso in regelmäßigen Abständen neue Updates der Software geprüft. Diese Prüfung erfolgt wie das Update selbst automatisch im Hintergrund.

11 Deinstallation

11.1 Windows

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

1. Beenden Sie zunächst die Anwendung des TIaaS Clients.
2. Öffnen Sie die Windows *Einstellungen* (*Windows Startmenü* > *Einstellungen* oder Windows-Taste + I).
3. Wählen Sie den Menüpunkt *Apps* aus.
4. Suchen Sie in der Liste nach der Applikation *RISE TI as a Service Client* und wählen Sie den Eintrag aus.
5. Wählen Sie *Deinstallieren* und bestätigen Sie.
6. Erteilen Sie Administratorberechtigung.
7. Der Deinstallationsprozess des TIaaS Clients startet.
8. Wählen Sie aus, welche Dateien, die im Zuge der Installation und des Betriebes des TIaaS Clients erstellt wurden, nach der Deinstallation weiterhin verfügbar sein sollen (siehe Abbildung 16).
    - **Konfigurationsordner entfernen**: Diese Auswahl entfernt das Installationsverzeichnis mit der TIaaS Konfiguration, in das der TIaaS Client installiert wurde.
    - **Logdateien entfernen**: Diese Auswahl löscht alle Logdateien, die im Zuge des Betriebes erstellt wurden, von der Festplatte.
    - **VPN-Tunnel entfernen**: Diese Auswahl entfernt die WireGuard-Konfiguration für den TIaaS Client, die für dessen Betrieb nötig ist.

- **WireGuard deinstallieren**: Entfernt den WireGuard-Service, der für die korrekte Funktionalität des TIaaS Clients nötig ist.
  Achtung: Wählen Sie diese Option nur aus, wenn Sie WireGuard für *keine* andere Anwendung nutzen, da deren Betrieb sonst eventuell gestört werden kann.

9. Folgen Sie den Anweisungen des Assistenten um die Deinstallation abzuschließen.

11.2 MacOS

Zur Deinstallation gehen Sie bitte in folgender Reihenfolge vor:

1. Beenden Sie zunächst die Anwendung des TIaaS Clients.
2. Öffnen Sie den Ordner der Applikation *RISE TI as a Service Client* in Ihrem Programme-Verzeichnis im Finder.
3. Starten Sie das *RISE TI as a Service Client Deinstallationsprogramm*.
4. Erteilen Sie Administratorberechtigung.
5. Der Deinstallationsprozess des TIaaS Clients startet.
6. Wählen Sie aus, welche Dateien, die im Zuge der Installation und des Betriebes des TIaaS Clients erstellt wurden, nach der Deinstallation weiterhin verfügbar sein sollen (siehe Abbildung 16).
   - **Konfigurationsordner entfernen**: Diese Auswahl entfernt das Installationsverzeichnis mit der TIaaS Konfiguration, in das der TIaaS Client installiert wurde.
   - **Logdateien entfernen**: Diese Auswahl löscht alle Logdateien, die im Zuge des Betriebes erstellt wurden, von der Festplatte.
   - **VPN-Tunnel entfernen**: Diese Auswahl entfernt die WireGuard-Konfiguration für den TIaaS Client, die für dessen Betrieb nötig ist.
   - **WireGuard deinstallieren**: Entfernt den WireGuard-Service, der für die korrekte Funktionalität des TIaaS Clients nötig ist.
     Achtung: Wählen Sie diese Option nur aus, wenn Sie WireGuard für *keine* andere Anwendung nutzen, da deren Betrieb sonst eventuell gestört werden kann.
7. Folgen Sie den Anweisungen des Assistenten um die Deinstallation abzuschließen.

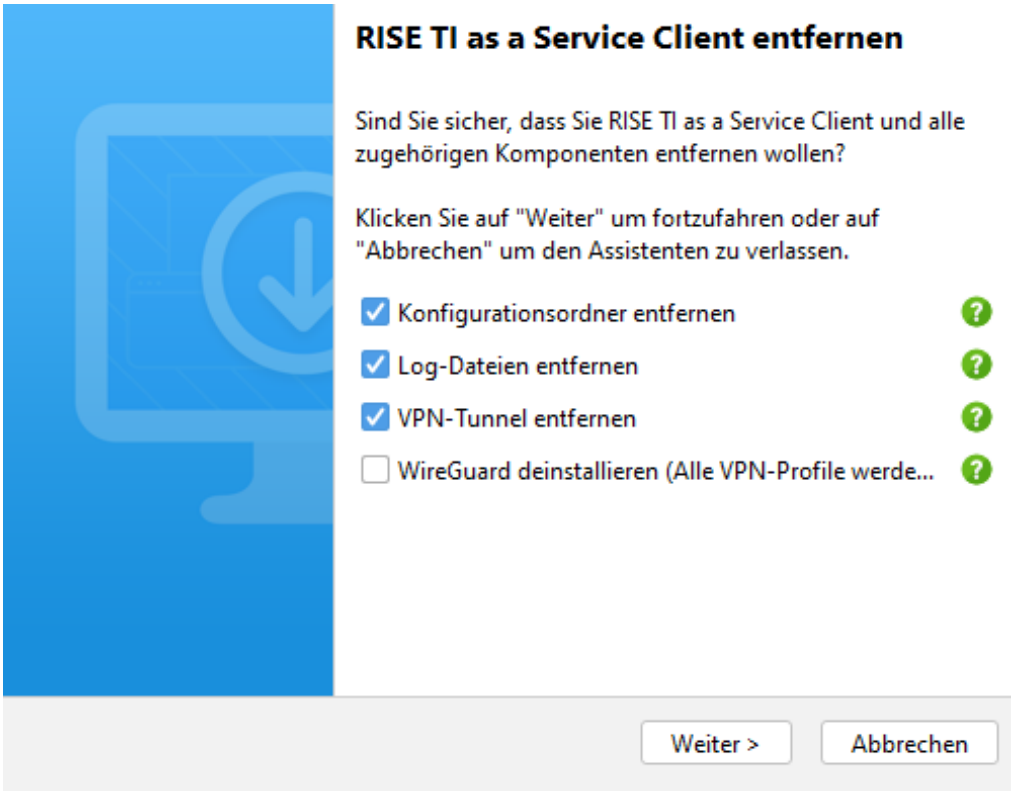

Abbildung 16: Deinstallation des TIaaS Clients

12 Fehlerbehebung

Im Folgenden werden mögliche Fehler aufgelistet, die während des Betriebs des TIaaS Clients auftreten können, sowie mögliche Ursachen und Lösungsvorschläge. Leer gelassene Zellen entsprechen inhaltlich der darüber stehenden Zelle.

Hinweis: Sollten Fehler mit den angegebenen Lösungsvorschlägen nach mehrmaligen Versuchen bzw. nach erneuter Installation des TIaaS Clients nicht behebbar sein, kontaktieren Sie bitte den TIaaS Anbieter-Support.

12.1 vKonnektor

Tabelle 2: Mögliche Fehlerursachen betreffend vKonnektor

Problem	Mögliche Ursache	Lösungsvorschlag
vKonnektor-Statussymbol ist rot	Keine/schlechte Verbindung mit dem Internet	Überprüfen Sie, ob Sie eine bestehende Internetverbindung haben.
	TIaaS Client-Konfiguration inkorrekt	Kontrollieren Sie die vKonnektor IP-Adresse in der Konfigurationsdatei (siehe Abschnitt 8.2). Stimmt diese nicht mit der, in der ausgelieferten Konfigurationsdatei hinterlegten vKonnektor IP-Adresse überein, passen Sie die

Problem	Mögliche Ursache	Lösungsvorschlag
		vKonnektor IP-Adresse in der bestehende TIaaS-Client Konfigurationsdatei an.
	vKonnektor Zertifikat inkorrekt/ungültig	Importieren Sie das im Installationspaket übermittelte vKonnektor Zertifikat erneut (siehe Abschnitt 8.1).
	Ungültige VPN-Verbindung	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
	vKonnektor offline	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf, wenn das Problem länger als 5 Minuten besteht.

12.2 Zertifikate

Tabelle 3: Mögliche Fehlerursachen betreffend Zertifikaten

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Der angeführte KeyStore konnte nicht importiert werden. Bitte überprüfen Sie die Eingabe.	Falsches Passwort beim Import des Zertifikats	Kontrollieren Sie die Korrektheit des eingegebenen Passworts und geben es erneut ein.
Automatische Aktualisierung des Schlüsselmaterials fehlgeschlagen. Bitte starten Sie die Applikation neu.	Interner Zertifikatsfehler des TIaaS Clients	Starten Sie die Applikation des TIaaS Clients neu.
Ein Validierungsfehler ist aufgetreten. Bitte überprüfen Sie die Eingabe	Ungültiges Dateiformat des hochzuladenden Zertifikats (sollte verhindert werden).	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.

12.3 Kartenterminal

Tabelle 4: Mögliche Fehlerursachen betreffend Kartenterminal

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Service Announcement konnte nicht empfangen werden.	Das Kartenterminal befindet sich nicht im selben Netzwerk.	Stellen Sie sicher, dass das Kartenterminal über seinen Ethernet-Port mit dem selben lokalen Netzwerk verbunden ist wie Ihr PC auf dem der TIaaS Client läuft.

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
	Es wurde ein falsches Netzwerkinterface ausgewählt.	Wählen Sie das korrekte Netzwerkinterface aus der angebotenen Liste aus (siehe Abschnitt 5.2).
	Es wurde eine falsche Kartenterminal IP-Adresse angegeben.	Kontrollieren Sie, ob die IP-Adresse des Kartenterminals korrekt eingegeben wurde. Vergewissern Sie sich bei Ihrem Netzwerkadministrator, dass Sie die korrekte IP-Adresse verwenden.
	Das Kartenterminal ist bereits mit einem Konnektor verbunden.	Heben Sie die Kartenterminal-Zuweisung zu diesem Kartenterminal bei allen lokalen Konnektoren auf. Besitzen Sie keine lokalen Konnektoren, nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Kartenterminal konnte nicht im KVS hinzugefügt werden.	Keine/schlechte Internetverbindung	Überprüfen Sie Ihre Internetverbindung.
	Ungültige VPN-Verbindung	Kontrollieren Sie, ob der vKonnektor erreichbar ist (siehe Abschnitt 4).
	Das KVS Zertifikat ist inkorrekt/ungültig.	Importieren Sie das im Installationspaket übermittelte KVS Zertifikat erneut (siehe Abschnitt 8.1). Bei bestehendem Problem, nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Pairing-Information konnte nicht gefunden werden.	Unzureichende Pairing-Daten wurden bei der Weitergabe der Kartenterminal-Informationen bereitgestellt.	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Die aktualisierte Konfiguration konnte nicht geschrieben werden.	Der TIaaS Client kann die bestehende Kartenterminal-Konfigurationsdatei nicht anpassen.	Stellen Sie sicher, dass die Kartenterminal-Konfigurationsdatei *application-card-terminal.yml* (siehe Abschnitt 8.3) nicht in einem anderen Programm geöffnet ist. Der TIaaS Client muss über Schreibrechte an der Datei verfügen.
Kartenterminal bereits verbunden.	Das Kartenterminal ist bereits mit dem TIaaS Clients verbunden.	Entfernen Sie das Kartenterminal per Auswahl in der Kartenterminalübersicht (siehe Abschnitt 5.3). Erscheint das betroffene

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
		Kartenterminal nicht in der Liste, entfernen Sie es direkt aus der Kartenterminal-Konfigurationsdatei *application-card-terminal.yml* (siehe Abschnitt 8.3). Verbinden Sie das Kartenterminal neu über den TIaaS Client.
Das Kartenterminal konnte im KVS nicht entfernt werden.	Das Entfernen des Kartenterminals am vKonnektor ist fehlgeschlagen.	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Kartenterminal-Proxy konnte nicht gestartet werden.	Notwendige Ports für die Kommunikation zwischen vKonnektor und dem Kartenterminal sind bereits belegt.	Stellen Sie sicher, dass die vom Kartenterminal verwendeten Ports nicht durch andere Services auf Ihrem PC belegt werden.
Service Announcement konnte nicht gelesen werden.	Der TIaaS Client hat ungültige Kartenterminal-Informationen vom Kartenterminal erhalten.	Versuchen Sie, das Kartenterminal erneut hinzuzufügen (siehe Abschnitt 5.2). Bei bestehendem Problem nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Service Discovery fehlgeschlagen.	Es ist ein Problem beim Abruf der Kartenterminal-Informationen vom Kartenterminal aufgetreten.	Versuchen Sie, das Kartenterminal erneut hinzuzufügen (siehe Abschnitt 5.2). Bei bestehendem Problem nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Socket konnte nicht geöffnet werden.	Die Schnittstelle zum Abruf der Kartenterminal-Informationen konnte nicht geöffnet werden.	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
System-Informationen konnten nicht abgefragt werden.	Die Netzwerkinterfaces konnten nicht abgerufen werden.	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
Die Pairingblöcke des Kartenterminals sind voll. Bitte die Pairingblöcke am Kartenterminal freigeben, um das Hinzufügen des	Die Pairingblöcke des Kartenterminals sind voll.	Geben Sie die Pairingblöcke auf ihrem Kartenterminal gemäß dessen Handbuch frei.

Fehlermeldung	Mögliche Ursache	Lösungsvorschlag
Kartenterminals zu ermöglichen.		

12.4 Karten

Tabelle 5: Mögliche Fehlerursachen betreffend Karten

Problem	Mögliche Ursache	Lösungsvorschlag
Fehler beim Laden der Karten, Fehler bei der PIN Verifizierung, Fehler bei der PIN Änderung, Fehler bei der PIN Entsperrung	Keine/schlechte Internetverbindung	Überprüfen Sie, ob Sie eine bestehende Internetverbindung haben.
	Kartenterminal nicht verbunden	Verbinden Sie ein Kartenterminal, um die Kartenübersicht anzuzeigen zu können.
	TIaaS Client-Konfiguration inkorrekt	Kontrollieren Sie die KVS IP-Adresse in der Konfigurationsdatei (siehe Abschnitt 8.2). Stimmt diese nicht mit der, in der ausgelieferten Konfigurationsdatei hinterlegten KVS IP-Adresse überein, passen Sie die KVS IP-Adresse in der bestehende TIaaS-Client Konfigurationsdatei an.
	KVS Zertifikat inkorrekt/ungültig	Importieren Sie das im Installationspaket übermittelte KVS Zertifikat erneut (siehe Abschnitt 8.1). Bei bestehendem Problem, nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf.
	Ungültige VPN-Verbindung	Überprüfen Sie, ob der vKonnektor erreichbar ist (siehe Abschnitt 4).
	vKonnektor offline	Nehmen Sie Kontakt mit Ihrem TIaaS Anbieter auf, wenn das Problem länger als 5 Minuten besteht.
Fehler bei der PIN Verifizierung, Fehler bei der PIN Änderung, Fehler bei der PIN Entsperrung	Bestätigung der PIN am Kartenterminal verpasst	Kartenoperation erneut durchführen und rechtzeitig am Kartenterminal bestätigen.

13 Kontakt

Bei Fragen und Problemen zum TIaaS Client, welche nicht von Ihrem Vertragshändler bzw. Infrastrukturdienstleister beantwortet werden können, wenden Sie sich bitte per E-Mail oder telefonisch an den TIaaS 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 TIaaS Anbieter aufzunehmen. Auf der RISE TIaaS-Webseite befinden sich sämtliche Kontaktinformationen. Der RISE TIaaS Client Identifier (ID) ist bei zielgerichteten Fragen anzugeben. Sie finden diese ID in Ihrer TIaaS Client-Konfigurationsdatei (siehe Abschnitt 8.2).