Für PEDs:
E-Health-Anbindung (TI) in charly

ab charly-Version 9.11.0

Stand 07.05.2019

Impressum / Copyright

solutio GmbH

Zahnärztliche Software und Praxismanagement

Max-Eyth-Straße 42

71088 Holzgerlingen

Fon 07031 4618-700

Fax 07031 4618-99700

info@solutio.de

www.solutio.de

Dokumentversion: 20190507.141700-ANL-Konnektor

Support

Technischer Support

Fon 07031 4618-900

Montag bis Freitag von 7:30 bis 18:00 Uhr

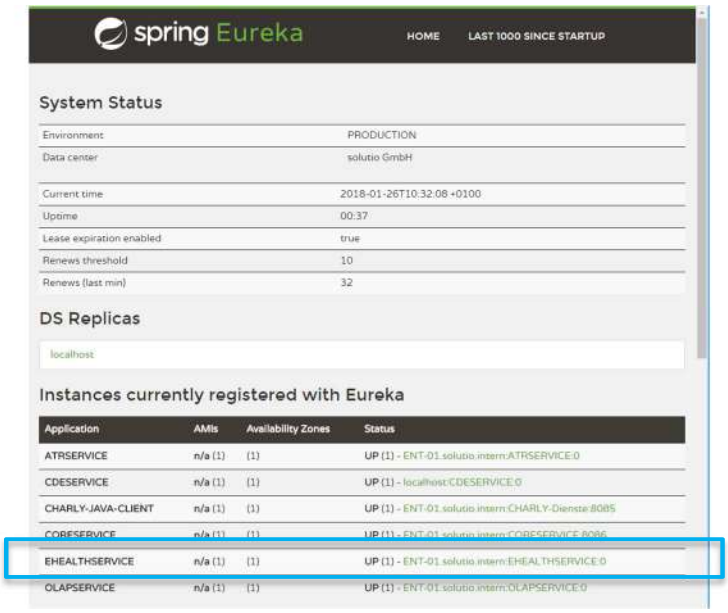
technik@solutio.de

Inhaltsverzeichnis

1 Allgemeine Voraussetzungen

- Sie haben eine kostenfreie Lizenz der solutio GmbH für die E-Health-Schnittstelle erworben.
- In der Menüleiste unter Hilfe > Zusätzliche Lizenzen ist die Checkbox E-Health (Anbindung Telematikinfrastruktur) aktiviert und die Lizenz der solutio GmbH eingetragen. charly wurde anschließend neu gestartet.
- In der Firewall ist der Port 8443 freigegeben, da die charly-Dienste SSL benutzen.
- Der E-Health-Service ist über den Client erreichbar.
  1. Öffnen Sie auf dem Client ein Browserfenster.
  2. Navigieren Sie zu `<IP-des-Servers>:8086`

  Bei korrekter Konfiguration öffnet sich das Eureka-Dashboard. Dort ist u.a. der **E-Health-Service** registriert und erreichbar.



2 Konnektor anlegen und konfigurieren

In charly haben Sie folgende Möglichkeiten, einen Konnektor anzubinden:

- Ohne TLS -> Kapitel 2.2
- TLS mit Zertifikatsprüfung -> Kapitel 2.3

Sobald ein Konnektor angelegt ist, können an dem Konnektor keine Änderungen mehr vorgenommen werden: Alle Felder sind „read-only".

2.1 Voraussetzungen

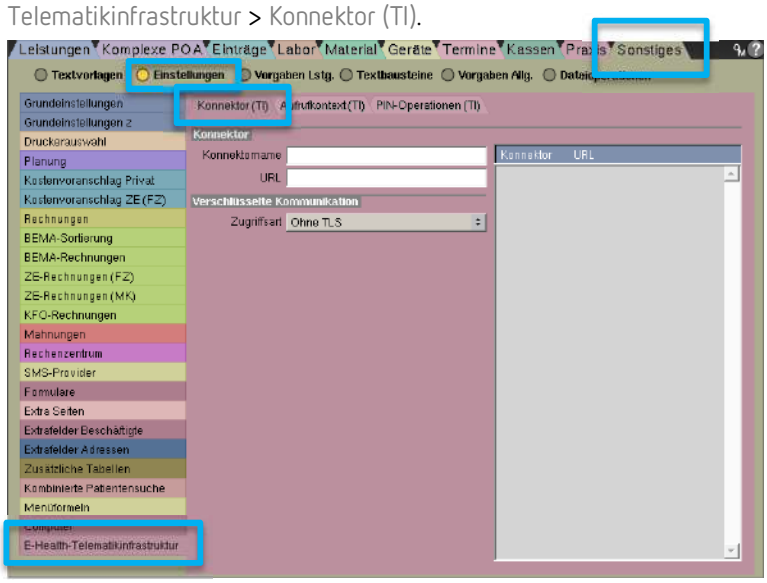
- Der Konnektor ist konfiguriert. Bitte beachten Sie hierzu die relevanten Einstellungen für die Anbindung ohne TLS und TLS mit Zertifikatsprüfung in den Kapiteln 8.1 bis 8.3.
- charly ist gestartet und der Mandant aufgerufen, für den der Konnektor eingerichtet wird.
- Um in den Stammdaten unter Sonstiges > Einstellungen > E-Health-Telematikinfrastruktur > Konnektor (TI) neue Konnektoren anlegen und konfigurieren zu können: Der angemeldete charly-Benutzer verfügt in der Maske „Stammdaten E-Health" über die Zugriffsberechtigungen „Lesen", „Ändern", „Löschen" und „Neu" (einzustellen in den Stammdaten unter Praxis > Gruppen).
- Sie kennen die URL des Konnektors.
- Für die Anbindung über TLS mit Zertifikatsprüfung: Laden Sie das entsprechende Zertifikat auf der Internetseite https://download.tsl.ti-dienste.de/ herunter:
  - Für KoCoBox: „`GEM.KOMP-CA1.der`"
  - Für T-Systems / RISE / secunet: „`GEM.KOMP-CA3.der`"

  > **Wichtig:** Die benötigten Zertifikate können sich je nach Firmware eines Konnektors unterscheiden. Bitte prüfen Sie selbständig, welches Zertifikat Ihr Konnektor tatsächlich benötigt. Weitere Informationen finden Sie hier: Welches Zertifikat benötigt der Konnektor?

2.2 Ohne TLS

1. Wählen Sie den Hauptbereich Stammdaten.

2. Gehen Sie in den Karteireiter Sonstiges > Einstellungen > E-Health-Telematikinfrastruktur > Konnektor (TI).



3. Klicken Sie auf den Button Leeren.
   - Die Felder leeren sich.

4. Geben Sie in das Feld Konnektorname den **frei wählbaren** Namen des Konnektors ein (Beispiel: „Konnektor01“).

   > **Wichtig:** Falls Sie denselben Konnektor bei weiteren Mandanten einrichten möchten, müssen sich die Namen des Konnektors in charly von Mandant zu Mandant unterscheiden.

5. Geben Sie in das Feld URL die IP-Adresse des Konnektors ein.
   Beispiel: `http://192.168.173.3/connector.sds`

6. Klicken Sie auf den Button Neu.
   - Die neu hinzugefügte Schnittstelle des Konnektors wird in die Liste aufgenommen. Der Eintrag erhält als Information den Konnektornamen sowie die IP-Adresse des Konnektors.

     Wenn Sie den Konnektor in der Liste markieren, werden im Bereich Konnektor der Konnektorname und die Konnektor-URL angezeigt. Diese sind grau hinterlegt und nicht mehr editierbar.

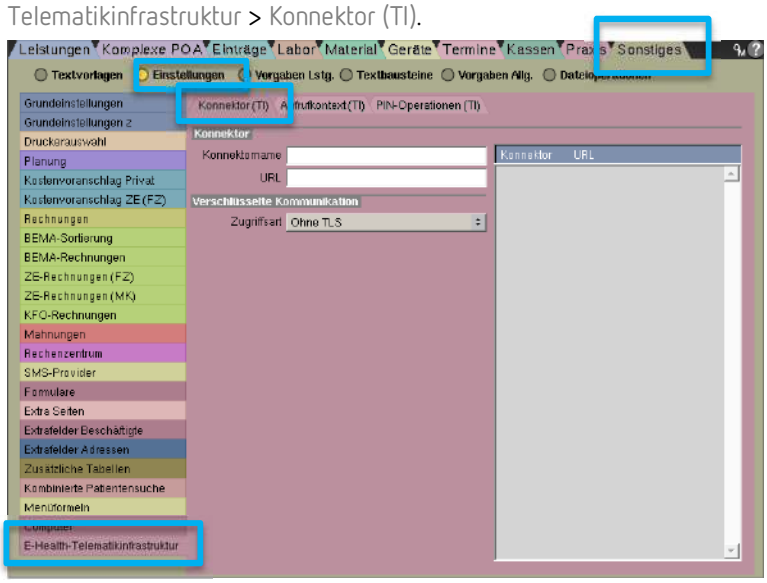
7. Wenn Sie weitere Konnektoren anlegen und konfigurieren möchten, wiederholen Sie die Schritte 3 bis 6.

2.3 TLS mit Zertifikatsprüfung

Die Konfiguration der Zugriffsart und die zugehörigen Zertifikatsfelder sind nur sichtbar, während ein neuer Konnektor angelegt wird.

1. Wählen Sie den Hauptbereich Stammdaten.

2. Gehen Sie in den Karteireiter Sonstiges > Einstellungen > E-Health-Telematikinfrastruktur > Konnektor (TI).



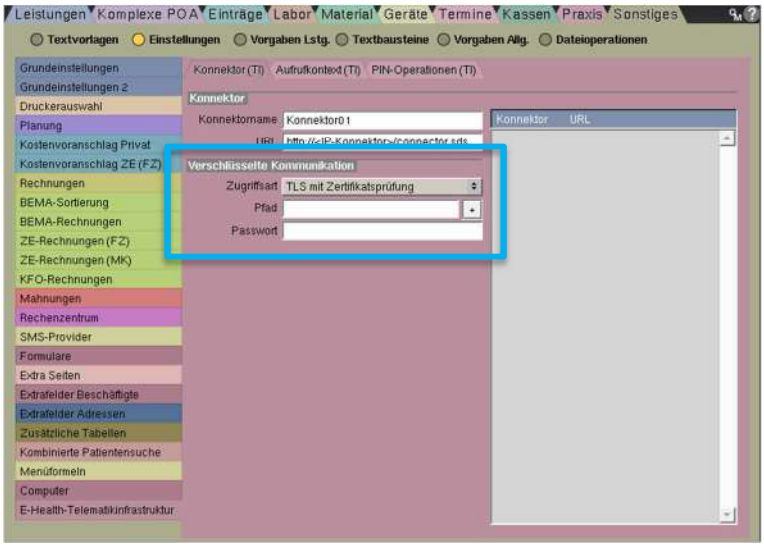
3. Klicken Sie auf den Button Leeren.
   - Die Felder leeren sich.

4. Geben Sie in das Feld Konnektorname den **frei wählbaren** Namen des Konnektors ein (Beispiel: „Konnektor01").

> **Wichtig:** Falls Sie denselben Konnektor bei weiteren Mandanten einrichten möchten, müssen sich die Namen des Konnektors in charly von Mandant zu Mandant unterscheiden.

5. Geben Sie in das Feld URL die IP-Adresse des Konnektors ein.
   Beispiel: `https://192.168.173.3/connector.sds`

6. Wählen Sie im Bereich Verschlüsselte Kommunikation aus der Dropdownliste die Option TLS mit Zertifikatsprüfung.



7. Klicken Sie rechts neben dem Feld Pfad auf den [+]-Button.
   - Der Explorer öffnet sich.
8. Navigieren Sie zu dem Pfad des Zertifikats.
9. Klicken Sie auf den Button Öffnen.
   - Der Pfad zu dem Zertifikat ist in das Feld Pfad übernommen.
10. Geben Sie in das Feld Passwort ein **beliebiges** Passwort für das Zertifikat ein.
11. Klicken Sie auf den Button Neu.
    - Die neu hinzugefügte Schnittstelle des Konnektors wird in die Liste aufgenommen. Der Eintrag erhält als Information den Konnektornamen sowie die IP-Adresse des Konnektors.

      Wenn Sie den Konnektor in der Liste markieren, werden im Bereich Konnektor der Konnektorname und die Konnektor-URL angezeigt. Diese sind grau hinterlegt und nicht mehr editierbar. Der Bereich Verschlüsselte Kommunikation ist ausgeblendet.
12. Wenn Sie weitere Konnektoren mit TLS-Serverzertifikat anlegen und konfigurieren möchten, wiederholen Sie die Schritte 3 bis 11.

3 Aufrufkontext anlegen und konfigurieren

Nachdem Sie einen Konnektor angelegt haben, können Sie für diesen Konnektor einen oder mehrere Aufrufkontexte konfigurieren.

Für die Client-Authentifizierung haben Sie in charly folgende Möglichkeiten:

- Ohne TLS -> Kapitel 0
- TLS mit Zertifikatsprüfung -> Kapitel 3.3
- TLS mit Basic Authentifizierung -> Kapitel 3.4

Sobald ein Aufrufkontext angelegt ist, können an dem Aufrufkontext keine Änderungen mehr vorgenommen werden: Alle Felder sind „read-only". Einzige Ausnahme: Sie können dem Aufrufkontext einen oder mehrere Computer zuweisen.

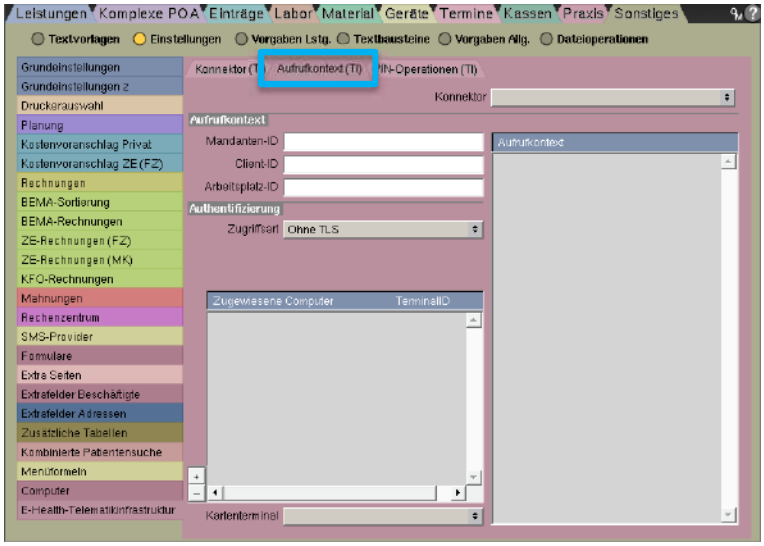
3.1 Voraussetzungen

- Der Konnektor, für den Sie einen Aufrufkontext anlegen und konfigurieren möchten, ist in den Stammdaten unter Sonstiges > Einstellungen > E-Health-Telematikinfrastruktur > Konnektor (TI) angelegt.
- In dem Konnektor haben Sie mindestens einen Aufrufkontext angelegt. Die Parameter für die Mandanten-ID, Client-ID und Arbeitsplatz-ID dieses Aufrufkontextes liegen Ihnen vor.
- Für die Anbindung über **TLS mit Zertifikatsprüfung**:
  - KoCoBox / RISE / secunet
    Sie haben das Clientzertifikat (Datei mit Endung `*.p12`) aus dem Konnektor exportiert und das Passwort für das Clientzertifikat notiert.
  - T-Systems
    Sie haben das Clientzertifikat (Datei mit Endung `*.pfx`) aus dem Konnektor exportiert. Ein Passwort gibt es nicht.

- Für die Anbindung über **TLS mit Basic Authentifizierung**:
  - Sie haben im Konnektor einen Benutzernamen sowie ein Passwort definiert. Diesen Benutzernamen und dieses Passwort benötigen Sie für die Konfiguration über TLS mit Basic Authentifizierung in charly.
- Um in den Stammdaten unter Sonstiges > Einstellungen > E-Health-Telematikinfrastruktur > Aufrufkontext (TI) neue Aufrufkontexte anlegen und konfigurieren zu können: Der angemeldete charly-Benutzer verfügt in der Maske „Stammdaten E-Health" über die Zugriffsberechtigungen „Lesen", „Ändern", „Löschen" und „Neu" (einzustellen in den Stammdaten unter Praxis > Gruppen).

3.2 Ohne TLS

1. Wechseln Sie im Karteireiter E-Health-Telematikinfrastruktur in den Reiter Aufrufkontext (TI).



2. Klicken Sie auf den Button Leeren.
   - Die Felder leeren sich.
3. Wählen Sie aus der Dropdownliste Konnektor den Konnektor, für den Sie einen Aufrufkontext konfigurieren wollen.

   Beispiel: „Konnektor01"
4. Geben Sie in die folgenden Felder die Parameter ein, die Sie im Konnektor definiert haben:

- Mandanten-ID
- Client-ID
- Arbeitsplatz-ID

Beispiel: „001" für den ersten Mandanten, „CHARLY" für den Client und „Rezeption" für die Arbeitsplatz-ID.

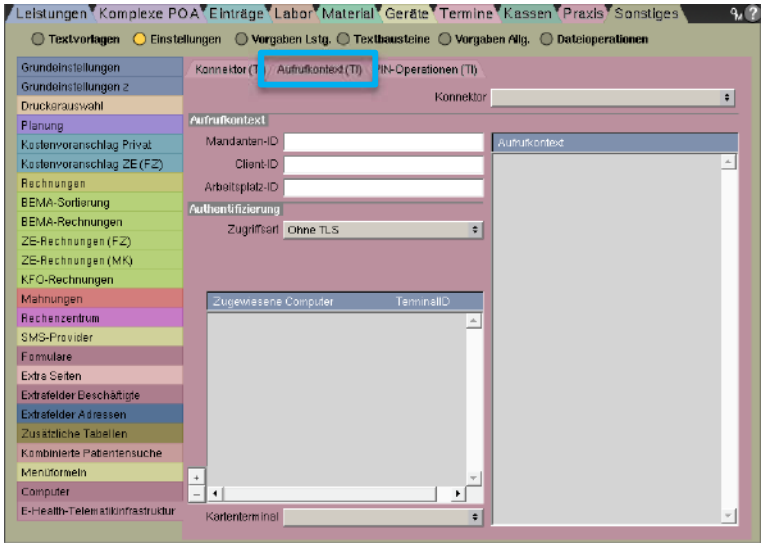
5. Klicken Sie auf den Button Neu.
   - Der neu hinzugefügte Aufrufkontext des Konnektors wird in die Liste aufgenommen. Der Eintrag erhält als Information die Mandanten-ID, Client-ID und Arbeitsplatz-ID.

     Wenn Sie in der Liste den erstellten Aufrufkontext (Beispiel: „001/CHARLY/Rezeption") markieren, werden im Bereich Aufrufkontext die Mandanten-ID, die Client-ID und die Arbeitsplatz-ID) angezeigt. Diese sind grau hinterlegt und nicht mehr editierbar.
6. Wenn Sie weitere Aufrufkontexte mit dem Konnektor verbinden möchten, wiederholen Sie die Schritte 3 bis 5.

3.3 TLS mit Zertifikatsprüfung

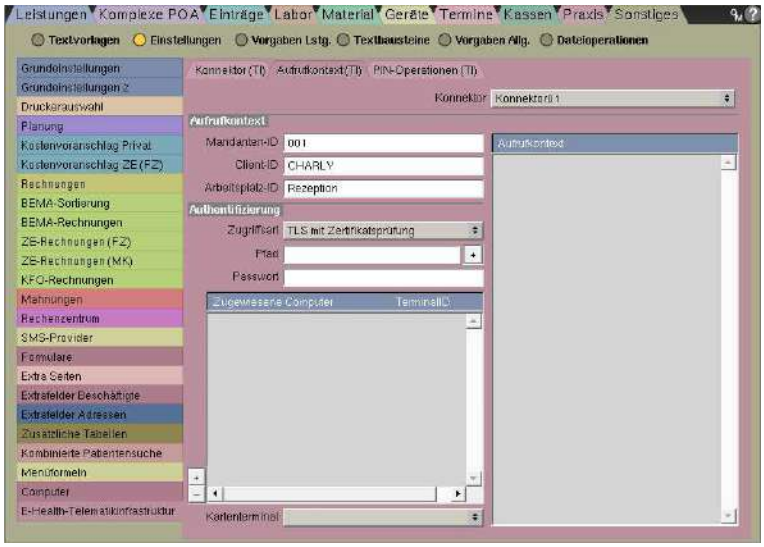
Die Konfiguration der Zugriffsart und die zugehörigen Zertifikatsfelder sind nur sichtbar, während ein neuer Aufrufkontext angelegt wird.

1. Wechseln Sie im Karteireiter E-Health-Telematikinfrastruktur in den Reiter Aufrufkontext (TI).



2. Klicken Sie auf den Button Leeren.
   › Die Felder leeren sich.
3. Wählen Sie aus der Dropdownliste Konnektor den Konnektor, für den Sie einen Aufrufkontext konfigurieren wollen.
   Beispiel: „Konnektor01"
4. Geben Sie in die folgenden Felder die Parameter ein, die Sie im Konnektor definiert haben:
   - Mandanten-ID
   - Client-ID
   - Arbeitsplatz-ID

   Beispiel: „001" für den ersten Mandanten, „CHARLY" für den Client und „Rezeption" für die Arbeitsplatz-ID.



5. Wählen Sie im Bereich Authentifizierung aus der Dropdownliste die Option TLS mit Zertifikatsprüfung.
6. Klicken Sie rechts neben dem Feld mit der Beschreibung Pfad auf den [+]-Button.
   › Der Explorer öffnet sich.
7. Navigieren Sie zu dem Pfad des Clientzertifikats.
   - KoCoBox / RISE / secunet: Datei mit Endung `*.p12`
   - T-Systems: Datei mit Endung `*.pfx`
8. Klicken Sie auf den Button Öffnen.
   › Der Pfad zu dem Zertifikat ist in das Feld Pfad übernommen.

9. KoCoBox / RISE / secunet: Geben Sie in das Feld Passwort das Passwort des Clientzertifikats ein.

   T-Systems: Lassen Sie das Feld Passwort leer.

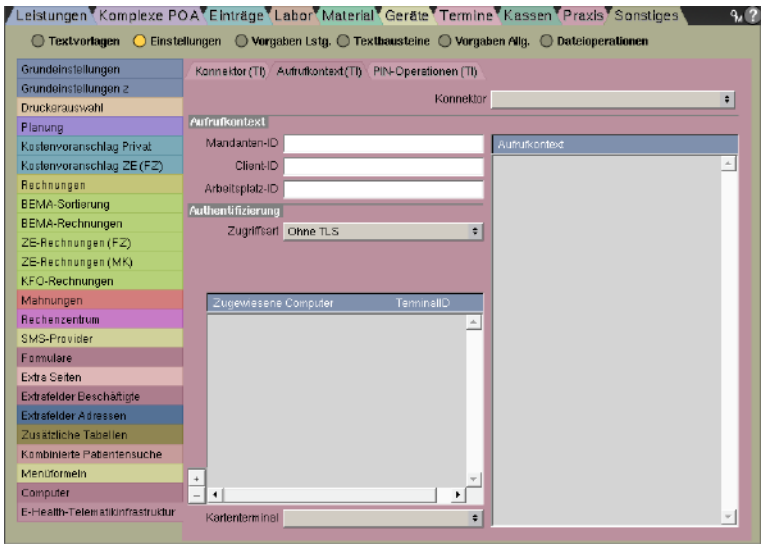
10. Klicken Sie auf den Button Neu.
    - Der neu hinzugefügte Aufrufkontext des Konnektors wird in die Liste aufgenommen. Der Eintrag erhält als Information die Mandanten-ID, Client-ID und Arbeitsplatz-ID.

      Wenn Sie in der Liste den erstellten Aufrufkontext (Beispiel: „001/CHARLY/Rezeption") markieren, werden im Bereich Aufrufkontext die Mandanten-ID, die Client-ID und die Arbeitsplatz-ID) angezeigt. Diese sind grau hinterlegt und nicht mehr editierbar. Der Bereich Authentifizierung ist ausgeblendet.

11. Wenn Sie weitere Aufrufkontexte mit dem Konnektor verbinden möchten, wiederholen Sie die Schritte 3 bis 10.

3.4 TLS mit Basic Authentifizierung

1. Wechseln Sie im Karteireiter E-Health-Telematikinfrastruktur in den Reiter Aufrufkontext (TI).

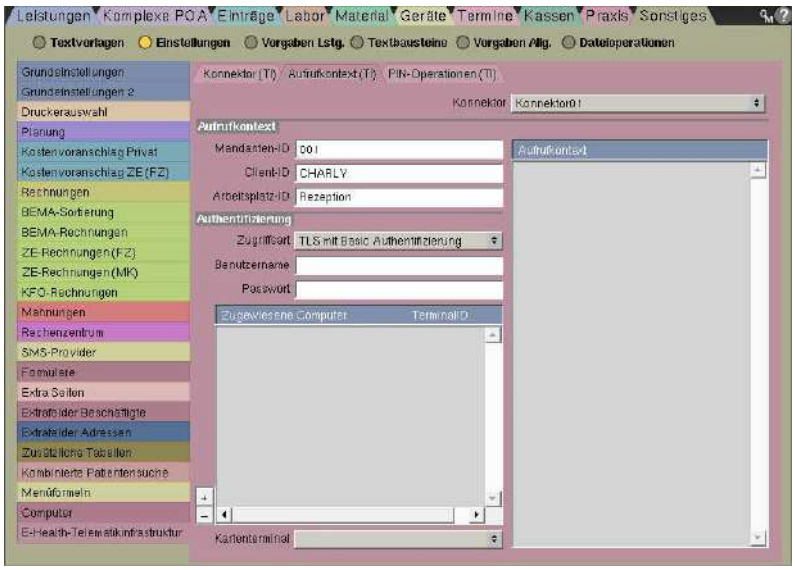


2. Klicken Sie auf den Button Leeren.
   - Die Felder leeren sich.

3. Wählen Sie aus der Dropdownliste Konnektor den Konnektor, für den Sie einen Aufrufkontext konfigurieren wollen.
   Beispiel: „Konnektor01"

4. Geben Sie in die folgenden Felder die Parameter ein, die Sie im Konnektor definiert haben:
   - Mandanten-ID
   - Client-ID
   - Arbeitsplatz-ID

   Beispiel: „001" für den ersten Mandanten, „CHARLY" für den Client und „Rezeption" für die Arbeitsplatz-ID.



5. Wählen Sie im Bereich Authentifizierung aus der Dropdownliste die Option TLS mit Basic Authentifizierung.

6. Geben Sie in das Feld Benutzername den Benutzernamen ein, den Sie im Konnektor für die Basic Authentifizierung definiert haben.

7. Geben Sie in das Feld Passwort das Passwort ein, das Sie im Konnektor für die Basic Authentifizierung definiert haben.

8. Klicken Sie auf den Button Neu.
   - Der neu hinzugefügte Aufrufkontext des Konnektors wird in die Liste aufgenommen. Der Eintrag erhält als Information die Mandanten-ID, Client-ID und Arbeitsplatz-ID.

Wenn Sie in der Liste den erstellten Aufrufkontext (Beispiel: „001/CHARLY/Rezeption") markieren, werden im Bereich Aufrufkontext die Mandanten-ID, die Client-ID und die Arbeitsplatz-ID) angezeigt. Diese sind grau hinterlegt und nicht mehr editierbar. Der Bereich Authentifizierung ist ausgeblendet.

9. Wenn Sie weitere Aufrufkontexte mit dem Konnektor verbinden möchten, wiederholen Sie die Schritte 3 bis 9.

4 Computer zuweisen

Nachdem Sie einen Aufrufkontext angelegt haben, können Sie diesem Aufrufkontext einen oder mehrere Computer zuweisen. Ein Computer darf dabei immer nur einem Aufrufkontext zugewiesen sein!

Jedem Computer können Sie wiederum ein festes Kartenterminal zuweisen und auf diese Weise die Anzahl der verfügbaren eGK bei einer eGK-Lesung einschränken.

1. Wählen Sie im Karteireiter E-Health-Telematikinfrastruktur im Reiter Aufrufkontext (TI) in der Dropdownliste Konnektor den Konnektor, dessen Aufrufkontext Sie einen Computer zuweisen möchten (z. B. "Konnektor01").
2. Markieren Sie in der Liste rechts den Aufrufkontext, dem Sie einen Computer zuweisen möchten.
3. Klicken Sie bei der Liste Zugewiesene Computer auf den [+]-Button.
   - Der folgende Dialog öffnet sich.

4. Wählen Sie den Computer aus der Dropdownliste dem der Aufrufkontext zugewiesen wird und klicken Sie auf den Button OK.
   - Der neu hinzugefügte Computer ist in die Liste Zugewiesene Computer aufgenommen.

5. Markieren Sie den Computer in der Liste und wählen Sie unterhalb der Liste aus der Dropdownliste Kartenterminal das Kartenterminal.
   › Bei dem Computer ist in der Spalte "TerminalID" das Kartenterminal eingetragen.
6. Wenn Sie dem markierten Aufrufkontext weitere Computer zuweisen möchten, wiederholen Sie die Schritte 3 bis 5.

5 Konnektorstatus testen

Prüfen Sie Ihre Konnektor- und Aufrufkontext-Konfiguration in charly, indem Sie den Konnektorstatus testen. Der Status wird aufgeschlüsselt nach:

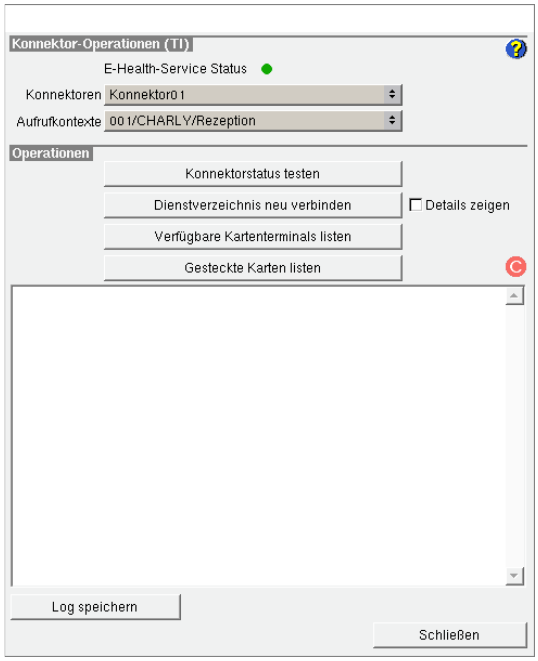
- TI-Status Der TI-Status zeigt, ob der Konnektor über den VPN-Zugangsdienst (VPN = Virtual Private Network) eine sichere Verbindung zu der zentralen Telematik-infrastruktur aufbauen kann. Der Weg in die TI wird dabei "getunnelt".
- SI-Status Der SI-Status zeigt an, ob der optionale Dienst "Sicherer Internet Service" (SIS) für den geschützten Zugriff auf das Internet verfügbar ist. Ein Zugriff auf das Praxisnetzwerk über eingehende Verbindungen ist hierbei technologisch ausgeschlossen.

Der TI-Status und der SI-Status kennen jeweils die folgenden Zustände:

- Offline Im Offline-Modus des Konnektors kann keine Verbindung zum VPN-Zugangsdienst aufgebaut werden (z. B. weil die WAN- Schnittstelle nicht angeschlossen oder die Verbindung gestört ist).
- Online Im Online-Modus des Konnektors besteht eine VPN-Verbindung zur zentralen Telematikinfrastruktur oder es wird davon ausgegangen, dass diese Verbindung jederzeit aufgebaut werden kann.

5.1 Vorgehensweise

1. Wählen Sie in der Menüleiste unter Hilfe die Option Konnektor-Operationen (TI).
   - Der folgende Dialog öffnet sich.



2. Wählen Sie aus der Dropdownliste Konnektoren den Konnektor, für den Sie den Test durchführen möchten.
3. Wählen Sie aus der Dropdownliste Aufrufkontexte den Aufrufkontext, für den Sie den Test durchführen möchten.
4. Klicken Sie auf den Button Konnektorstatus testen.
   - Der Status wird im Log-Bereich ausgegeben.

Weitere mögliche Operationen in diesem Dialog sind:

- **Dienstverzeichnis neu verbinden**

  Über den Button Dienstverzeichnis neu verbinden werden die Fachdienste, die auf dem Konnektor laufen, neu geladen und anschließend mit den Fachdienst-Namen und den Versionen im Log-Bereich gelistet.

  Wenn Sie die Checkbox Details zeigen aktivieren, werden neben den Fachdienst-Namen und den Versionen der Fachdienste zusätzliche Informationen angezeigt.

- **Verfügbare Kartenterminals listen**

  Über den Button Verfügbare Kartenterminals listen werden die verfügbaren Kartenterminals mit zusätzlichen Informationen im Log-Bereich gelistet.

- **Gesteckte Karten listen**

  Über den Button Gesteckte Karten listen werden sämtliche Karten mit zusätzlichen Informationen gelistet, die in den Kartenterminals gesteckt sind.

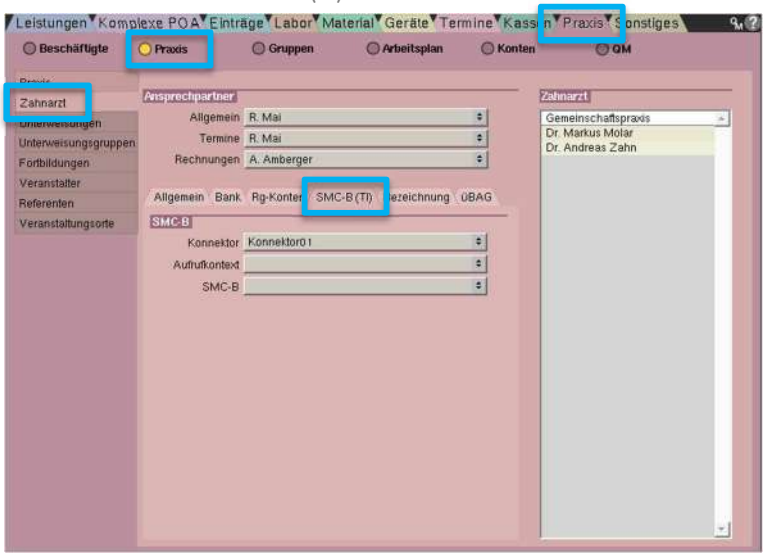
6 SMC-B mit Abrechnungsnummer verknüpfen

Für eine korrekte Zuweisung der Karteneinlesungen in charly, muss die SMC-B mit der Abrechnungsnummer des Zahnarztes bzw. der Gemeinschaftspraxis verknüpft werden.

6.1 Vorgehensweise

1. Wählen Sie den Hauptbereich Stammdaten.

2. Gehen Sie in den Karteireiter Praxis > Praxis > Zahnarzt und wählen Sie dort den Unterkarteireiter SMC-B (TI).



3. Abhängig von Ihrer Praxisform: Markieren Sie in der Liste Zahnarzt die Gemeinschaftspraxis **oder** den Zahnarzt, dem Sie die SMC-B zuweisen möchten.
4. Wählen Sie aus der Dropdownliste Konnektor den Konnektor.
5. Wählen Sie aus der Dropdownliste Aufrufkontext den Aufrufkontext.
6. Wählen Sie aus der Dropdownliste SMC-B die SMC-B, die der Gemeinschaftspraxis bzw. dem markierten Zahnarzt zugeordnet werden soll.
7. Klicken Sie auf den Button OK.
   › Die SMC-B ist mit der Abrechnungsnummer der Gemeinschaftspraxis bzw. des markierten Zahnarztes verknüpft.

   Bei einer Gemeinschaftspraxis ist die zugewiesene SMC-B automatisch auf alle Zahnärzte in der Liste Zahnarzt übertragen.
8. Wenn Sie weitere SMC-Bs zuweisen möchten, wiederholen Sie die Schritte 3 bis 7.

7 Backup-Strategie mit Systemadministrator besprechen

Um einen fehlerfreien Betrieb des Konnektors und charly gewährleisten zu können, besprechen Sie bitte nach der erfolgreichen Konfiguration des Konnektors mit dem Systemadministrator der Praxis die Backup-Strategie.

Falls der Systemadministrator im Rahmen des Backups auch die Datenbank sichert und dafür den Datenbank-Server anhält, muss er sein Backup-Skript wie folgt erweitern:

- Vor der Datenbanksicherung die charly-Dienste stoppen
- Nach der Datenbanksicherung die charly-Dienste starten

Die charly-Dienste befinden sich auf dem charly-Server im Verzeichnis `Solutio\Server\ncjs`

charly-Dienste stoppen

Mit dem folgenden Befehl werden alle charly-Dienste gestoppt:

- Windows `acd stopall`
- Mac `./acd.sh stopall`

charly-Dienste starten	Mit dem folgenden Befehl werden alle charly-Dienste gestartet: • Windows `acd startall` • Mac `./acd.sh startall`

8 FAQ

8.1 Einstellungen im KoCoBox-Konnektor

Die Einstellungen für die Konfiguration ohne TLS oder mit TLS finden Sie in der Konnektor-Oberfläche unter Verwaltung > Clientsysteme.

Abbildung 1 ▶
Menü in der Konnektor-Oberfläche

Unter Clientsysteme > Anbindung Clientsysteme konfigurieren Sie die Verbindung. Im Folgenden sehen Sie jeweils einen Screenshot der relevanten Einstellungen für die Verbindung

- ohne TLS
- mit TLS
- mit TLS und Basic Authentifizierung

Abbildung 2 ▶
Einstellungen für Verbindung **ohne** TLS

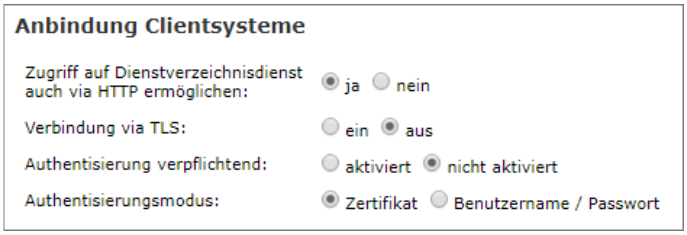


Abbildung 3 ▶
Einstellungen für Verbindung **mit** TLS

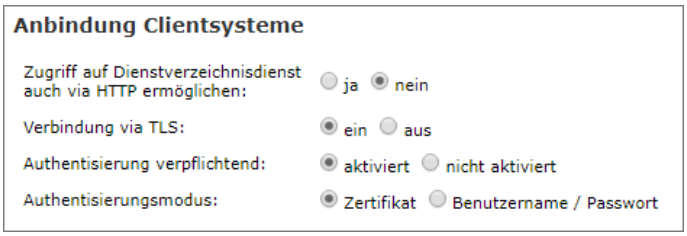
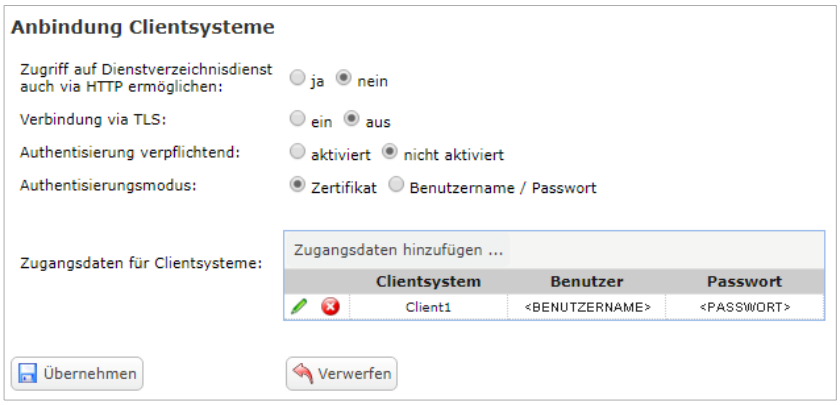


Abbildung 4 ▶
Einstellungen für Verbindung **mit** TLS **und** Basic Authentifizierung

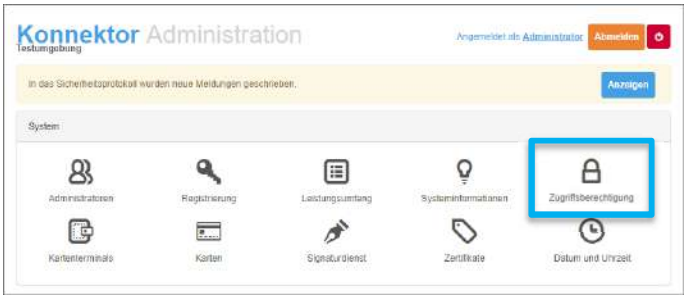


Klicken Sie im Bereich Zugangsdaten für Clientsysteme auf das grüne Stift-Symbol, um Ihre Zugangsdaten hinzuzufügen. Wählen Sie einen Benutzernamen (<BENUTZERNAME>) und ein Passwort (<PASSWORT>). Bestätigen Sie Ihre Eingabe über den Button „Übernehmen".

8.2 Einstellungen im T-Systems-Konnektor

Die Einstellungen für die Konfiguration ohne TLS, mit TLS oder mit TLS und Basic Authentifizierung finden Sie in der Konnektor-Oberfläche unter Zugriffsberechtigung.

Abbildung 5 ▶
Hauptmenü der Konnektor-Oberfläche



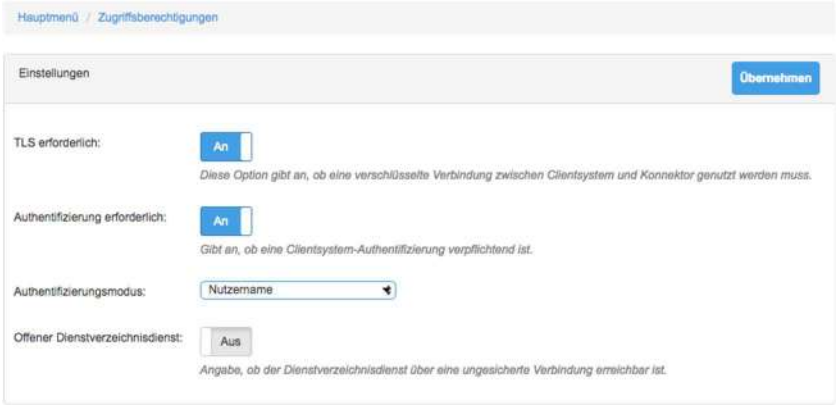
Im Bereich Einstellungen konfigurieren Sie die Verbindung. Im Folgenden sehen Sie jeweils einen Screenshot der relevanten Einstellungen für die Verbindung

- ohne TLS
- mit TLS
- mit TLS und Basic Authentifizierung

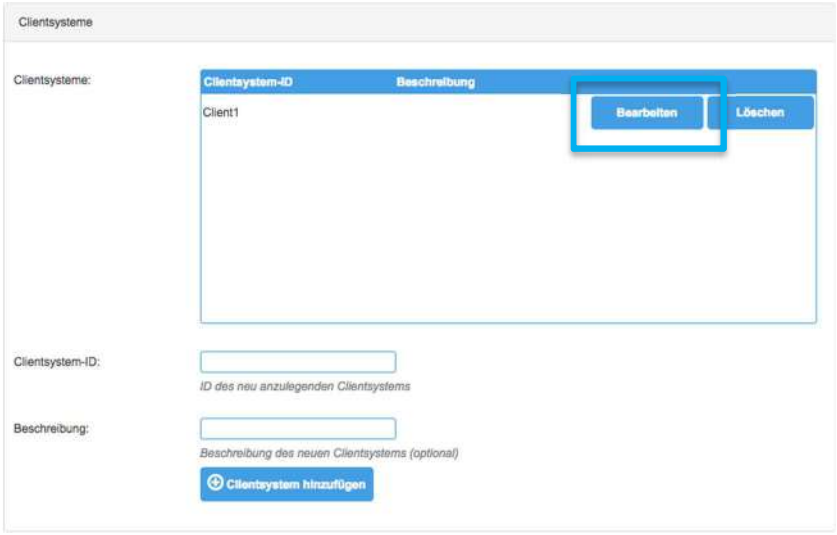
Abbildung 6 ▶
Einstellungen für Verbindung **ohne** TLS

Abbildung 7 ▶
Einstellungen für Verbindung **mit** TLS

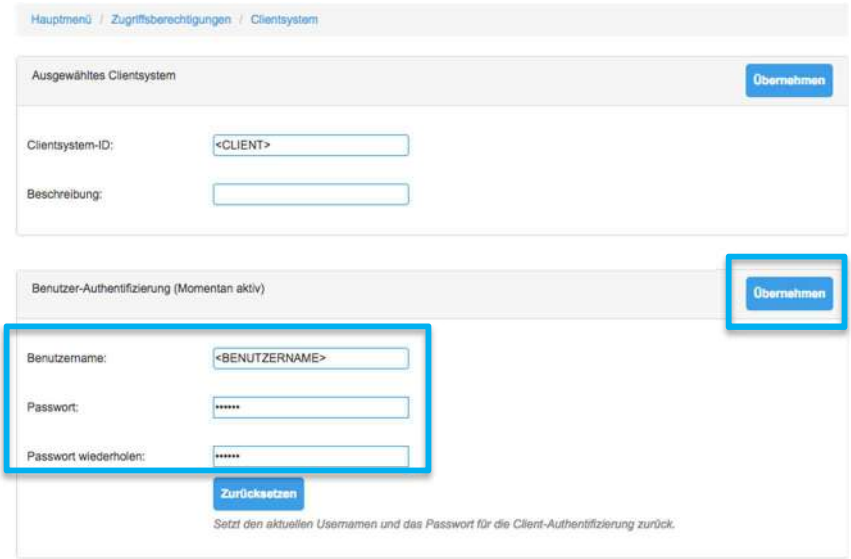
Abbildung 8 ▶
Einstellungen für Verbindung **mit** TLS **und** Basic Authentifizierung



Für die Basic Authentifizierung müssen Sie zusätzlich einen Benutzernamen und ein Passwort festlegen. Klicken Sie dazu im Bereich Clientsysteme neben dem Clientsystem auf den Button „Bearbeiten". Dadurch öffnet sich eine neue Seite.



Geben Sie dort für das gewählte Clientsystem einen Benutzernamen (<BENUTZERNAME>) und ein Passwort (<PASSWORT>) ein. Bestätigen Sie Ihre Eingabe über den Button „Übernehmen".



8.3 Einstellungen im RISE-Konnektor

Die Einstellungen für die Konfiguration ohne TLS oder mit TLS finden Sie in der Konnektor-Oberfläche unter Dienste > Clientsysteme.

Abbildung 9 ▶
Menü in der Konnektor-Oberfläche

Unter Clientsysteme > Anbindung Clientsysteme > Konfiguration konfigurieren Sie die Verbindung. Im Folgenden sehen Sie jeweils einen Screenshot der relevanten Einstellungen für die Verbindung

- ohne TLS
- mit TLS
- mit TLS und Basic Authentifizierung

Abbildung 10 ▶
Einstellungen für Verbindung **ohne** TLS

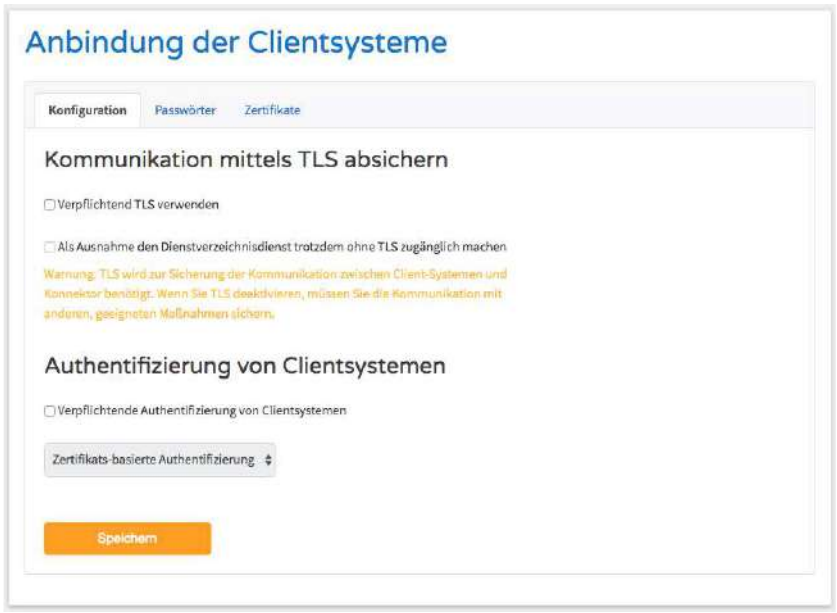


Abbildung 11 ▶
Einstellungen für Verbindung **mit** TLS

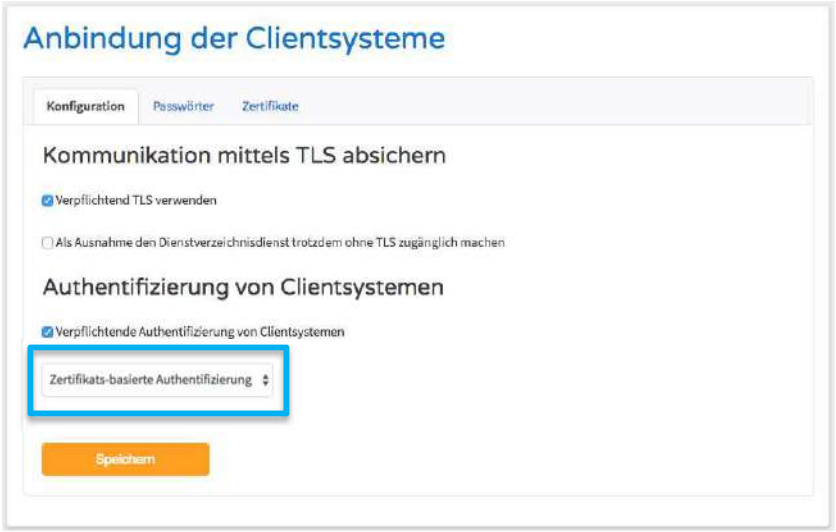
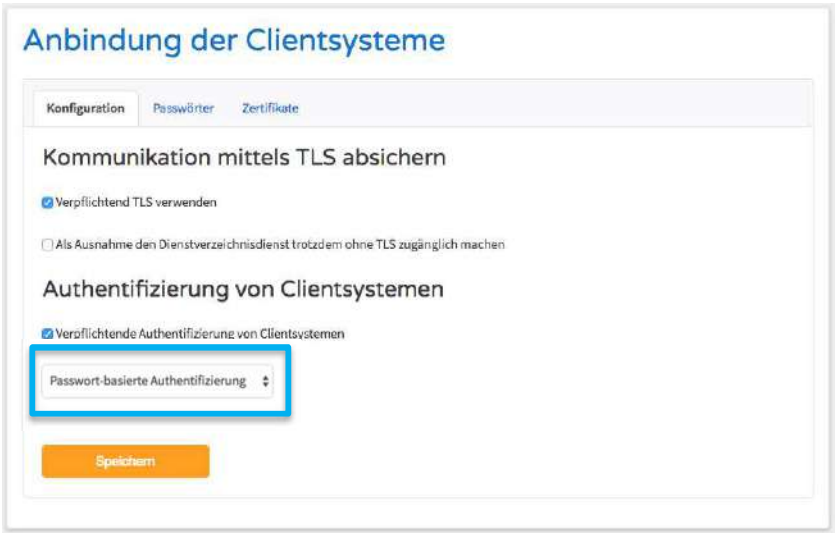
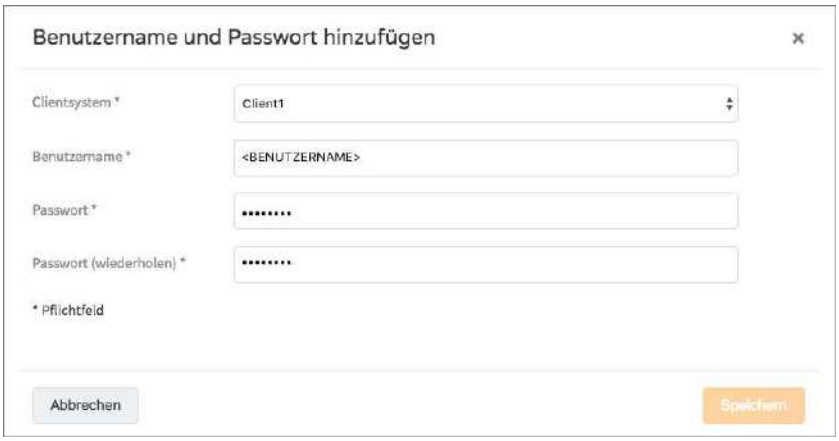


Abbildung 12 ▶
Einstellungen für Verbindung **mit** TLS **und** Basic Authentifizierung



Für die Basic Authentifizierung müssen Sie zusätzlich einen Benutzernamen und ein Passwort festlegen. Wechseln Sie dazu in den Bereich Passwörter. Klicken Sie neben dem Clientsystem in der Spalte Aktionen auf den Button mit dem Stiftsymbol. Dadurch öffnet sich eine neue Seite.

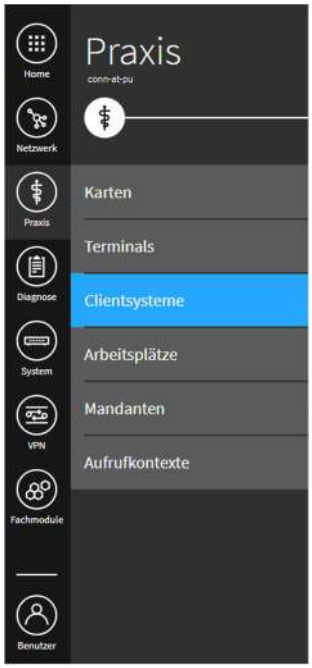
Geben Sie dort für das gewählte Clientsystem einen Benutzernamen (<BENUTZERNAME>) und ein Passwort (<PASSWORT>) ein. Bestätigen Sie Ihre Eingabe über den Button „Speichern".



8.4 Einstellungen im secunet-Konnektor

Die Einstellungen für die Konfiguration ohne TLS oder mit TLS finden Sie in der Konnektor-Oberfläche unter Praxis > Clientsysteme.

Abbildung 13 ▶
Menü in der Konnektor-Oberfläche



Unter Clientsysteme > Clientsystem-Einstellungen konfigurieren Sie die Verbindung. Im Folgenden sehen Sie jeweils einen Screenshot der relevanten Einstellungen für die Verbindung

- ohne TLS
- mit TLS
- mit TLS und Basic Authentifizierung

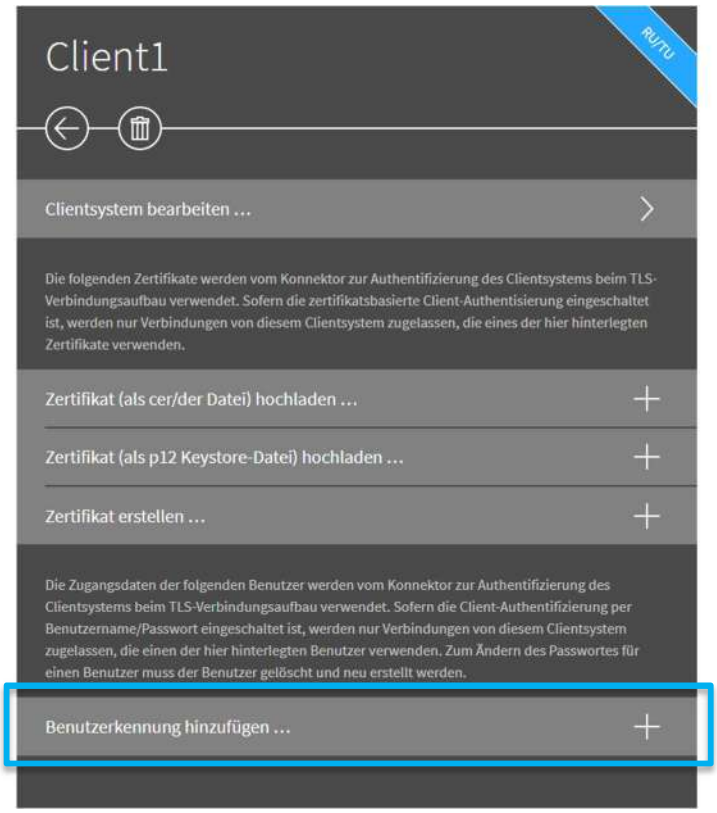
Abbildung 14 ▶
Einstellungen für Verbindung **ohne** TLS

Abbildung 15 ▶
Einstellungen für Verbindung **mit** TLS

Abbildung 16 ▶
Einstellungen für Verbindung **mit** TLS **und** Basic Authentifizierung

Für die Basic Authentifizierung müssen Sie zusätzlich einen Benutzernamen und ein Passwort festlegen. Verlassen Sie dazu nach dem Speichern die Client-Einstellungen.

Wählen Sie stattdessen im Bereich Clientsysteme das Clientsystem, für das Sie Benutzername und Passwort definieren möchten. Klicken Sie in den Einstellungen für das Clientsystem auf Benutzerkennung hinzufügen.



Geben Sie dort für das gewählte Clientsystem einen Benutzernamen (<BENUTZERNAME>) und ein Passwort (<PASSWORT>) ein. Bestätigen Sie Ihre Eingabe über den Button mit dem Haken.

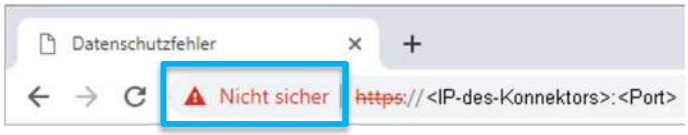
8.5 Welches Zertifikat benötigt der Konnektor?

Für die Anbindung über TLS mit Zertifikatsprüfung benötigen die Konnektoren ein Zertifikat. Das entsprechende Zertifikat laden Sie auf folgender Internetseite herunter: https://download.tsl.ti-dienste.de/

So finden Sie heraus, welches Zertifikat der jeweilige Konnektor benötigt (am Beispiel des **Browsers Chrome** – bei anderen Browsern ist die Vorgehensweise ggf. abweichend):

1. Öffnen Sie den Browser und geben Sie die URL für den administrativen Zugang des Konnektors ein.
   - Falls noch kein Zertifikat hinterlegt ist, zeigt der Browser, dass die Verbindung unsicher ist.

Abbildung 17 ▶
Beispiel: Browser Chrome ohne Zertifikat

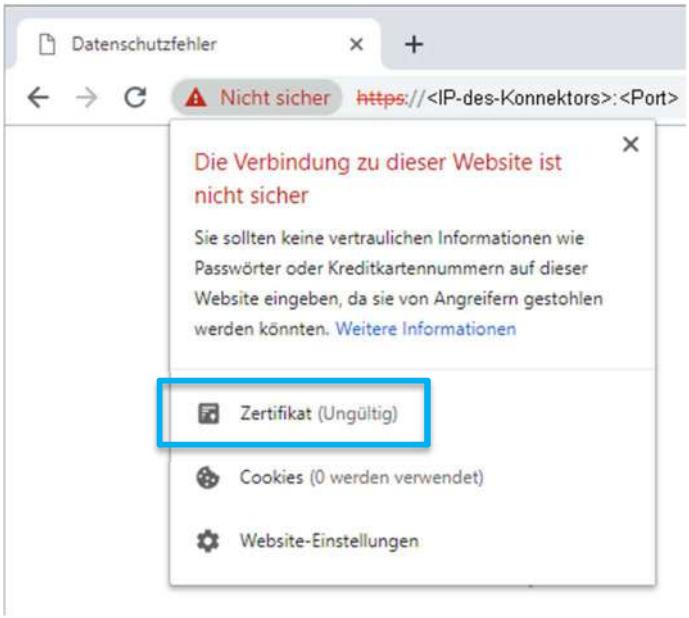


   - Falls bereits ein Zertifikat hinterlegt ist, zeigt der Browser in der Adressleiste ein Schloss-Symbol.

Abbildung 18 ▶
Beispiel: Browser Chrome mit gültigem Zertifikat

2. Klicken Sie auf das Warndreieck- bzw. das Schloss-Symbol.
3. Klicken Sie auf „Zertifikat".

Abbildung 19 ▶
Beispiel: Browser Chrome mit Verbindungsinformationen



4. Wählen Sie den Reiter „Details".
   › Unter „Aussteller" sehen Sie das benötigte Zertifikat.

Abbildung 20 ▶
Beispiel: Browser Chrome mit Details zum Zertifikat