

Abschnitt 1: Einführung

- A. Lernziele

Abschnitt 2: Überprüfung und Vorbereitung

- A. Prozessüberblick
- B. Notwendige Ausstattung für die Installation
- C. Überprüfung der Komponenten beim Empfang der Lieferung
- D. Beschädigte Sicherheitssiegel des secunet-Konnektors erkennen
- E. Auspacken und Vorbereiten der Kartenterminals
- F. Beschädigte Paketsiegel der Kartenterminals erkennen
- G. Gerätesiegel der eHealth-Kartenterminals
- H. Überprüfen Sie Ihr Wissen
- I. Zusammenfassung

Abschnitt 3: Erstmalige Inbetriebnahme des Konnektors

- A. Vorbereitung der Erstanmeldung
- B. Fehleranzeigen des Konnektors
- C. Validierung des Konnektor-Zertifikats
- D. TLS-Zertifikat importieren
- E. Initialpasswort ändern
- F. Zusammenfassung

Abschnitt 4: Einführung in die Bedienungsoberfläche

- A. Der Home-Bildschirm
- B. In der Bedienoberfläche navigieren
- C. Die Prüfung von Eingaben
- D. Warnungen und Hinweise

Abschnitt 5: Schluss

- A. Mitwirkende
- B. Weiterführende Literatur
- C. Quellennachweise
- D. Fast geschafft
- E. Überprüfung
- F. Lernimpulse

Abschnitt 1: Einführung

Nachdem die Checklisten vollständig sind und Sie als DVO ein klares Verständnis von der Praxissituation bezüglich der TI-Anbindung haben, die Vorbereitung der Konfiguration abgeschlossen ist sowie alle Installationsvoraussetzungen und benötigten Teile vorhanden sind,

Erste Schritte der Installation

können Sie zum vereinbarten Termin, an den Sie die Praxis zuvor noch einmal erinnert haben, zur Installation der TI-Anbindung fahren.

Lernziele

Nachdem Sie diese Lerneinheit absolviert haben, sollten Sie folgende Fähigkeiten erworben haben:

1. Sie können die ersten Prozessschritte der Installation benennen.
2. Sie können den Konnektor erstmalig in Betrieb nehmen.
3. Sie kennen den grundlegenden Aufbau der Bedienungsoberfläche.

Abschnitt 2: Überprüfung und Vorbereitung

Prozessüberblick

Hier sehen Sie einen Überblick über die einzelnen Prozessschritte bei der Installation der TI-Anbindung der Praxis. In dieser Lerneinheit werden wir Ihnen die ersten beiden Prozessschritte genauer vorstellen. In den folgenden beiden Lerneinheiten vervollständigen Sie den Prozess.

Notwendige Ausstattung für die Installation

Zum Installationstermin sollten Sie Folgendes mitbringen:

- ein Laptop mit Netzwerkanschluss,
- die Software des Support-Clients zur Installation auf dem Praxis-PC,
- die Konfigurationsdatei mit den vorkonfigurierten Praxisdaten (dies erspart Ihnen u. U. Zeit vor Ort),
- Ersatzkomponenten zur Netzwerkverkabelung wie:
 - Switches
 - LAN-Kabel
- und Ersatzgeräte für den Fehlerfall, also
 - einen secunet-Konnektor und
 - ein zugelassenes E-Health-Kartenterminal.

Wussten Sie eigentlich, dass für den Transport der Konnektoren durch Sie (in der Rolle des DVO) in die Arztpraxis die Vorgaben zur sicheren Lagerung der Konnektoren gelten? Die Konnektoren müssen auch während des Transports durch den DVO zum Installationstermin entsprechend gegen Zugriffe bzw. Manipulation geschützt werden. Detaillierte Informationen über Maßnahmen, um dies zu gewährleisten, haben wir Ihnen unter dem Bereich Ressourcen hinterlegt. Grundsätzlich gilt: Es dürfen nicht mehr Geräte transportiert werden als Sie pro Tag installieren.

Überprüfung der Komponenten beim Empfang der Lieferung

Vor Beginn der Installation sollte nochmals überprüft werden, ob alle notwendigen Voraussetzungen für die Installation gegeben sind. Dazu gehören insbesondere folgende Punkte:

- Alle notwendigen Komponenten liegen vor (Konnektor, E-Health Kartenterminal, gSMC-KT).
- Alle benötigten SMC-B(s) mit PIN(s) liegen vor und sind beim Zertifikatsanbieter freigeschaltet.
- Alle benötigten Zugangsdaten liegen vor.

Erste Schritte der Installation

Zunächst müssen die gemäß der sicheren Lieferkette in die Praxis gelieferten Komponenten im Beisein des Praxispersonals auf ihre Vollständigkeit und Unversehrtheit überprüft werden. Die Prüfung des Modulare Konnektors erfolgt gemäß dem Sicherheitsbeiblatt „Empfang und Prüfung“ und umfasst folgende Schritte:

1. Siegelband der Transportverpackung prüfen

Bei einem Öffnungsversuch lösen sich die Schichten des Siegelbands, sodass ein Schriftzug erkennbar ist.

Normale Ansicht



Teilweise geöffnet



Wenn das Siegelband oder die Transportverpackung beschädigt sind, darf der Modulare Konnektor nicht verwendet werden.

2. Prüfung der Vollständigkeit der Lieferung

Der Lieferumfang des Modulare Konnektors umfasst folgendes Zubehör:

Ein externes Netzteil (AC Adapter mit 220V und Netzkabel mit Kaltgerätestecker), zwei Sicherheitsbeiblätter (Empfang und Prüfung sowie Aufstellung und Inbetriebnahme) und eine CD/DVD (Bedienhandbuch als PDF).

3. Beide Sicherheitssiegel des Modulare Konnektors prüfen

Die Größe der Sicherheitssiegel beträgt 30 mm x 10 mm.



Die Sicherheitssiegel besitzen folgende Sicherheitsmerkmale:

- Kreuzförmige Sicherheitsstanzungen
- Seriennummer
- Öffnungsbotschaft „GEOFFNET OPENED“ bei Beschädigung
- Thermoreaktive Linienzüge

Ab einer Temperatur von ca. 45 °C sind die roten Linien nicht mehr zu sehen.

Erste Schritte der Installation



Thermoreaktive Linienzüge

- UV-aktiver Schriftzug „SECURITY“

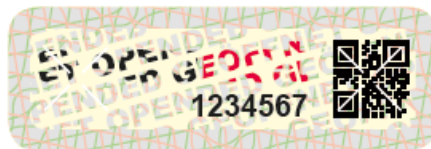
Der Schriftzug wird unter UV-Licht von ca. 365 nm sichtbar.



Sicherheitssiegel unter UV-Licht

Beschädigte Sicherheitssiegel des secunet-Konnektors erkennen

So erkennen Sie Beschädigungen der Sicherheitssiegel:



Beschädigtes Sicherheitssiegel



Rückstände eines abgezogenen Sicherheitssiegels

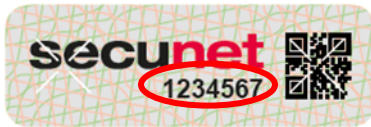
- Sind die Sicherheitsmerkmale beeinträchtigt?
- Sind die Sicherheitssiegel entlang der Gehäusekanten durchschnitten oder zerkratzt?
- Hat ein Sicherheitssiegel unzureichende Verbindung zum Gehäuse und lässt es sich leicht abheben?
- Ist eins der Sicherheitssiegel farblich verändert?
- Haften Klebereste auf einem der Sicherheitssiegel?

Sobald Sie eine Beschädigung an einem der Sicherheitssiegel erkennen, dürfen Sie das Gerät nicht in Betrieb nehmen.

4. Seriennummern der Sicherheitssiegel notieren

Diese Seriennummern finden Sie hier:

Erste Schritte der Installation



5. Gehäuse auf Eindringversuche prüfen

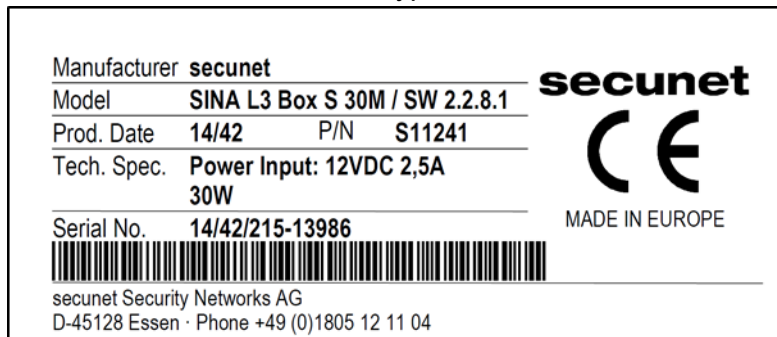
So erkennen Sie Eindringversuche:

- Gibt es Beschädigungen von Gehäuse und Lackierung?
- Gibt es Beschädigungen im Bereich der Verbindungen?
- Gibt es Öffnungen im Gehäuse?
- Sind die LEDs der Betriebsanzeigen beschädigt?
- Gibt es zusätzliche Aufkleber oder externe Bauteile, die Ihnen unbekannt sind?

Sobald Sie eine Beschädigung feststellen oder den Verdacht haben, dass das Gerät manipuliert wurde, dürfen Sie es nicht in Betrieb nehmen.

6. Seriennummer des Gerätes notieren

Diese befindet sich auf dem Typenschild:



7. Geheimnis festlegen

Für den Konnektor muss ein Geheimnis aus mindestens sechs Groß- oder Kleinbuchstaben für die Notfallwiederherstellung (alternativer Werksreset) dokumentiert werden.

8. Geheimnis dem DVO vor Ort mitteilen

9. Kontaktdaten des DVO dokumentieren

Auspacken und Vorbereiten der Kartenterminals

Die E-Health-Kartenterminals müssen ebenfalls ausgepackt und auf Auffälligkeiten überprüft werden. An dieser Stelle möchten wir Sie darauf hinweisen, dass Sie vor der Inbetriebnahme eines der vorgestellten Geräte zwingend die Bedienungsanleitung lesen und die Sicherheitshinweise beachten müssen.

Beschädigte Paketsiegel der Kartenterminals erkennen

Ingenico-Kartenterminals werden in Verpackungen versandt, die rundherum mit einem Siegelband verschlossen sind. In regelmäßigem Wechsel ist auf dem türkisgrünen Siegelband das ingenico-Healthcare-Logo und ein Barcode mit der Siegelbandnummer aufgebracht. Wenn das Siegelband beschädigt ist, müssen Sie die Annahme des Pakets verweigern.

Beschädigte Paketsiegel können Sie an folgenden Auffälligkeiten erkennen:

- das Siegelband umspannt die Verpackung nicht vollständig

Erste Schritte der Installation

- es ist eingerissen oder aufgeschlitzt
- es fehlt komplett
- der diagonale Text APERTO OPENED GEÖFFNET OVERT ist zu erkennen

Dieser Text ist im Normalfall nur auf dem grünen Untergrund des Siegels leicht zu erkennen. Unter den weißen Bereichen des Siegels ist er normalerweise nicht zu erkennen. Sobald das Siegelband von der Verpackung gelöst und anschließend wieder aufgeklebt wird, verliert der Klebestreifen an Haftkraft und der Schriftzug wird deutlicher zu sehen. Wenn das Siegelband komplett entfernt wurde, verbleibt nur noch der Schriftzug auf der Verpackung.

Gerätesiegel der eHealth-Kartenterminals

Auf dieser Abbildung sehen Sie die Positionen der verschiedenen Siegel des ingenico-Kartenterminals Orga 6141.

Die Kartenterminals haben verschiedene Gehäuse- und Slotsiegel. Geräte mit fehlenden oder beschädigten Siegeln dürfen nicht genutzt werden. Die Siegel- sowie Seriennummer des Kartenterminals muss dokumentiert werden.

Nun sollten die Karteneinschübe der E-Health-Kartenterminals mit den gSMC-KTs bestückt werden. Anschließend muss der Karteneinschub mit einem durch den Administrator unterschriebenen Slotsiegel versiegelt werden. Diese Slotsiegel werden mit dem Kartenterminal zusammen ausgeliefert. Ein beschädigtes Slotsiegel weist auf Manipulationsversuche hin. Geräte mit beschädigten oder fehlenden Slotsiegeln dürfen nicht mehr verwendet werden.

Überprüfen Sie Ihr Wissen

Welche dieser Siegel sind beschädigt?

1.



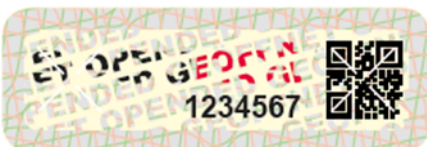
2.



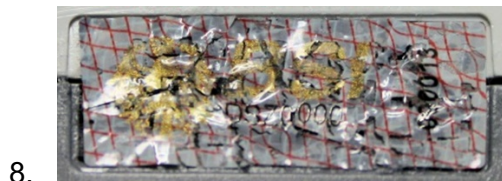
3.



4.



Erste Schritte der Installation



Feedback: Richtig! Sie haben alle beschädigten Siegel identifiziert.
Falsch! Versuchen Sie es erneut. Unter 2.3 und 2.5 können Sie sich die passenden Hinweise ansehen.

Zusammenfassung

Sie haben die ersten Schritte im Installationsprozess kennengelernt. Hier ein kurzer Überblick:

Leistung	Erwartetes Ergebnis
----------	---------------------

Erste Schritte der Installation

Überprüfung der Vollständigkeit und Unversehrtheit der Komponenten im Beisein des Praxispersonals.	Konnektor und Kartenterminals sind vollständig und unversehrt. Die Vorgaben der sicheren Lieferkette wurden eingehalten. Die notwendigen Informationen sind auf dem Sicherheitsbeiblatt dokumentiert.
Auspacken und Vorbereitung der Geräte	Konnektor und Kartenterminal sind ausgepackt und vorbereitet zum Anschluss. Die gSMC-KTs sind in die Kartenterminals eingebracht und die Slots gemäß den Vorgaben versiegelt.

Abschnitt 3: Erstmalige Inbetriebnahme des Konnektors

Der Modulare Konnektor wird über eine webbasierte Bedienoberfläche eingerichtet und bedient. Im Folgenden lernen Sie diese Oberfläche kennen und erfahren, wie Sie sich am Konnektor erstmalig anmelden.

Vorbereitung der Erstanmeldung

Der initiale Zugriff auf die webbasierte Bedienoberfläche ist nur über die lokale Administrationsschnittstelle in der Praxis möglich. Zuerst müssen Sie jedoch das Gerät verkabeln und einschalten. Hierzu können Sie wieder Schritt für Schritt vorgehen:

1. Verbinden Sie den Modulare Konnektor mit dem Netzteil und schließen Sie dieses an die Stromversorgung an.
2. Schalten Sie den Modulare Konnektor ein.
3. Die Betriebsanzeigen leuchten auf und das Gerät startet. Wenn die Anzeige SYSTEM dauerhaft leuchtet, ist der Modulare Konnektor betriebsbereit. Warten Sie nach dem erfolgreichen Start des Modularen Konnektors mindestens 60 Sekunden, damit die LAN-Schnittstelle automatisch die IP-Adresse 169.254.1.2 zugewiesen bekommt.
4. Stellen Sie sicher, dass die LAN-Schnittstelle des Clientsystems eine IP-Adresse aus dem Adressbereich des Modularen Konnektors verwendet (Empfehlung: 169.254.1.10).
5. Verbinden Sie den LAN-Anschluss direkt mit einem Clientsystem (= Laptop zur Installation).
6. Stellen Sie sicher, dass keine weiteren Netzwerkkomponenten angeschlossen sind. Entfernen Sie ggf. alle weiteren Verbindungen, wie zum Beispiel WAN-Anschlüsse.

Die nächste Folie hilft Ihnen, die verschiedenen optischen Signale des Konnektors richtig zu deuten.

Fehleranzeigen des Konnektors

Hier eine Übersicht der Anzeigen beim Systemstart und möglicher Fehleranzeigen.

LED(s)	Signal	Erläuterung
Service, Update,	An	Boot-Prozess des BIOS startet

Erste Schritte der Installation

Remote		
Update, Remote	An	Boot-Prozess des BIOS wird fortgesetzt
Remote	An	Boot-Prozess des BIOS wurde erfolgreich abgeschlossen
Alle	An	Fehler beim Boot-Prozess des BIOS
Alle außer Power	Aus	Boot-Prozess des Betriebssystems startet
System	Blinkt	System startet
System	An	System ist betriebsbereit
System	An	Fehler mit hoher Priorität beim Systemstart
Service	Blinkt	

Validierung des Konnektor-Zertifikats

Die folgende Beschreibung setzt voraus, dass Sie Google Chrome als Browser und ein Windows-Betriebssystem verwenden. Das Handbuch des secunet-Konnektors empfiehlt Google Chrome ab Version 61. Bitte beachten Sie, dass es zu Abweichungen in der Bedienung kommen kann, wenn Sie einen anderen Browser oder ein anderes Betriebssystem verwenden.

Die Administrationsschnittstelle zum Modulare Konnektor wird über eine TLS-Verbindung abgesichert. Beim TLS-Verbindungsaufbau wird für die Authentisierung des Modulare Konnektors ein TLS-Zertifikat verwendet, das im Gerät hinterlegt ist. Um sicherzustellen, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird, muss dieses validiert werden, da sonst der Schutz von z. B. Zugangsdaten nicht sichergestellt werden kann.

Erst danach authentisiert sich der Administrator durch die Eingabe von Zugangsdaten an der Administrationsschnittstelle.

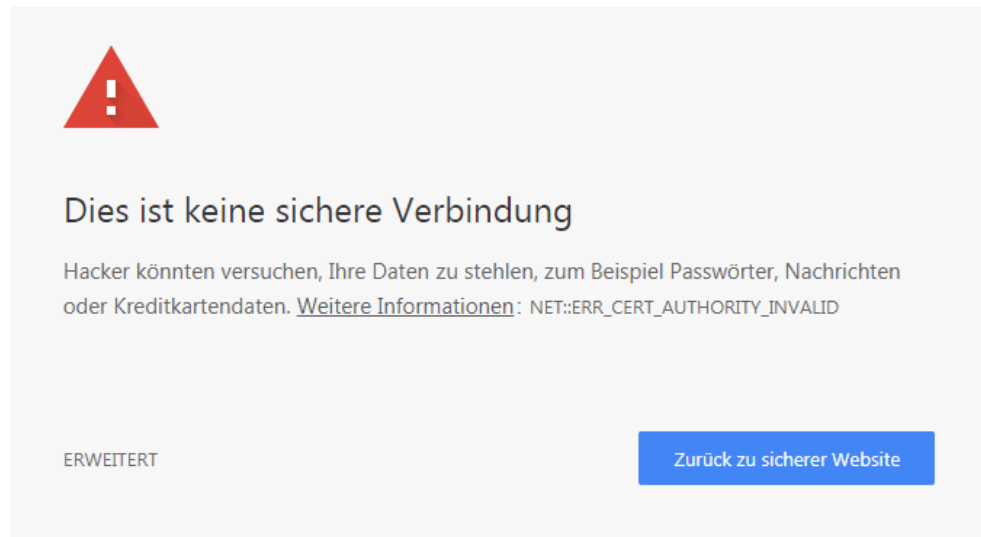
Validieren Sie das Zertifikat des Modulare Konnektors, indem Sie es exportieren und in den Browser importieren.

Gehen Sie für die Exportierung wie folgt vor:

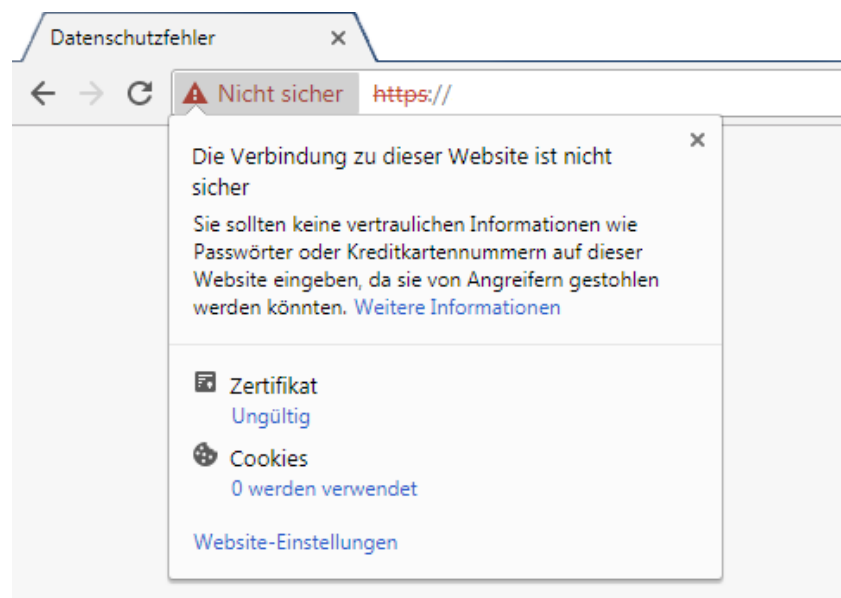
1. Falls nicht bereits geschehen, verbinden Sie sich mit dem Modulare Konnektor und rufen Sie die Bedienoberfläche auf, indem Sie in die Adresszeile des Browsers die vom Handbuch des Konnektors vorgegebene Zieladresse eingeben (<http://169.254.1.2:8500/management>).

Es sollte diese Fehlermeldung im Browser angezeigt werden:

Erste Schritte der Installation

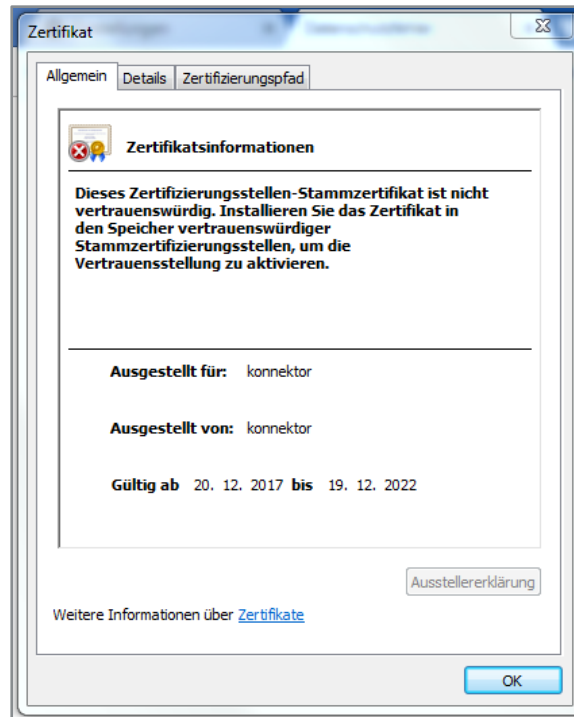


2. Neben der Adresszeile wird ein Warnsymbol mit dem Text **Nicht sicher** angezeigt. Klicken Sie darauf, um Verbindungsinformationen einzublenden.

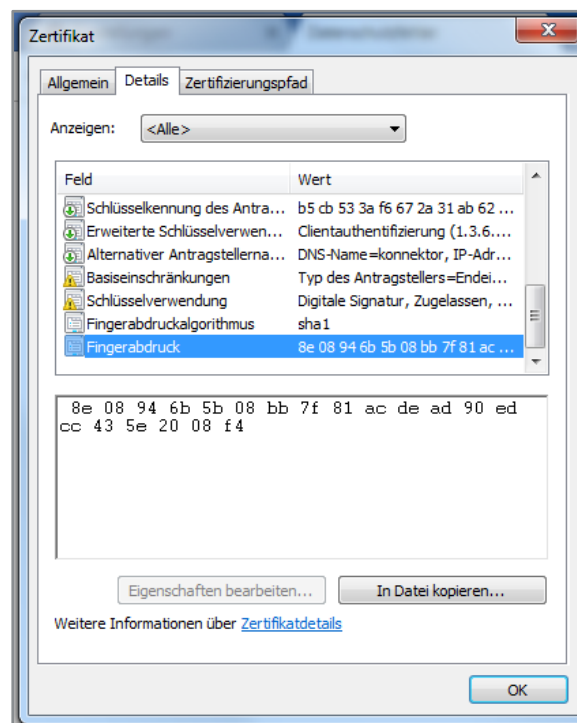


3. Klicken Sie unter Zertifikat auf Ungültig, um weitere Informationen anzuzeigen.

Erste Schritte der Installation



4. Öffnen Sie den Reiter **Details**, um weitere Informationen über das Zertifikat wie beispielsweise den Fingerprint anzuzeigen.

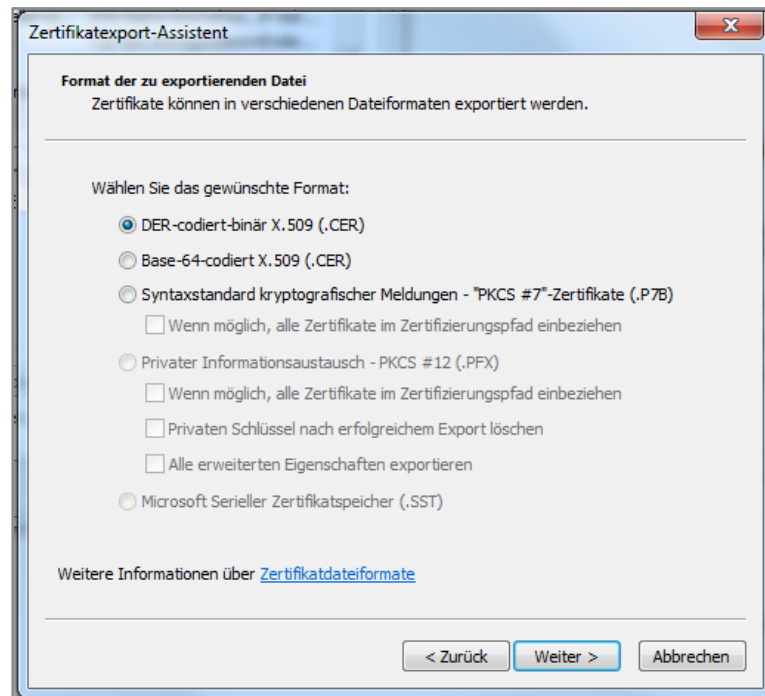


5. Klicken Sie auf **In Datei kopieren ...**, um das Zertifikat zu exportieren. Der Zertifikatexport-Assistent öffnet sich.

Erste Schritte der Installation



6. Wählen Sie das Format DER-codiert-binär X.509 (.CER).



7. Folgen Sie den Anweisungen des Zertifikatexport-Assistenten, um das Zertifikat in einer Datei abzuspeichern.

TLS-Zertifikat importieren

Das gespeicherte Zertifikat des Modularen Konnektors muss nun in den Browser des Clientsystems importiert werden.

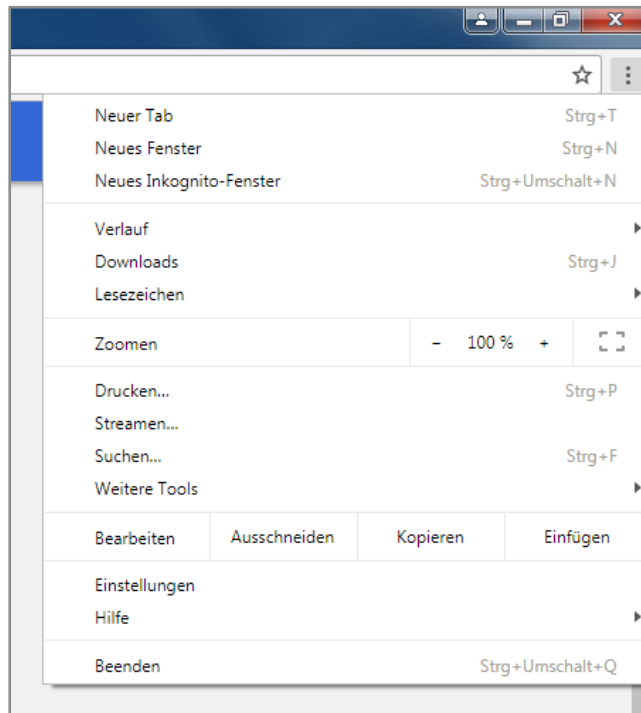
Gehen Sie wie folgt vor, um das Zertifikat in den Browser zu importieren:

1. Klicken Sie auf das Menü-Symbol  rechts neben der Adressleiste, um weitere

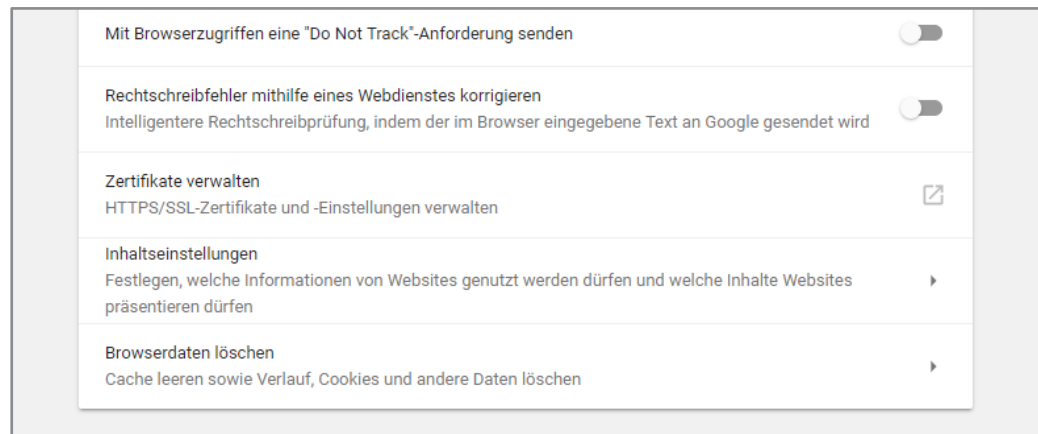
Erste Schritte der Installation

Optionen anzuzeigen.

2. Klicken Sie auf **Einstellungen**.

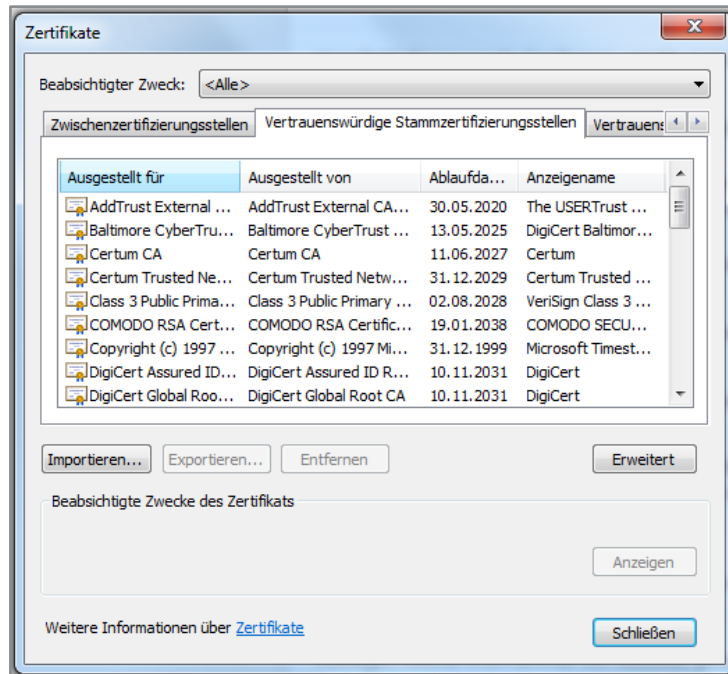


3. Klicken Sie am unteren Bildschirmrand auf **Erweitert**, um alle Einstellungen einzublenden.
4. Klicken Sie auf **Zertifikate verwalten**. Es werden nun alle bereits importierten Zertifikate angezeigt.

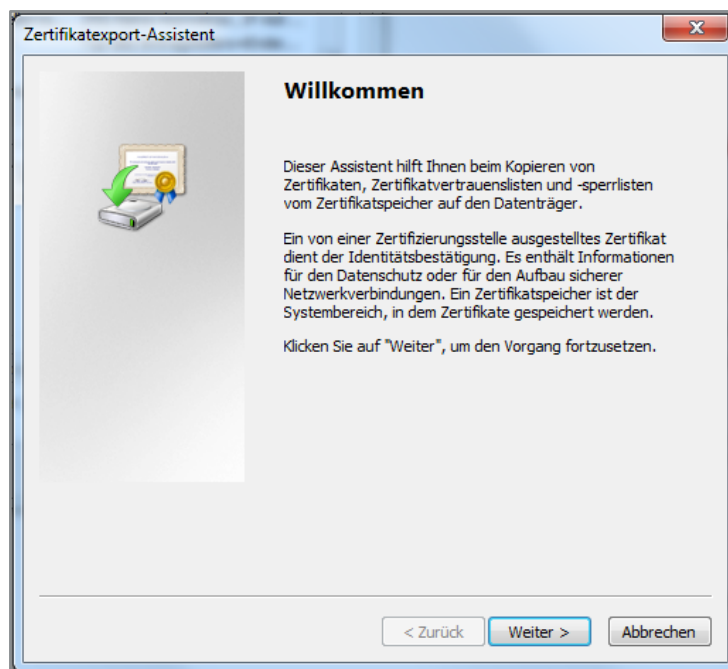


5. Öffnen Sie den Reiter **Vertrauenswürdige Stammzertifizierungsstellen** und klicken Sie auf **Importieren**.

Erste Schritte der Installation

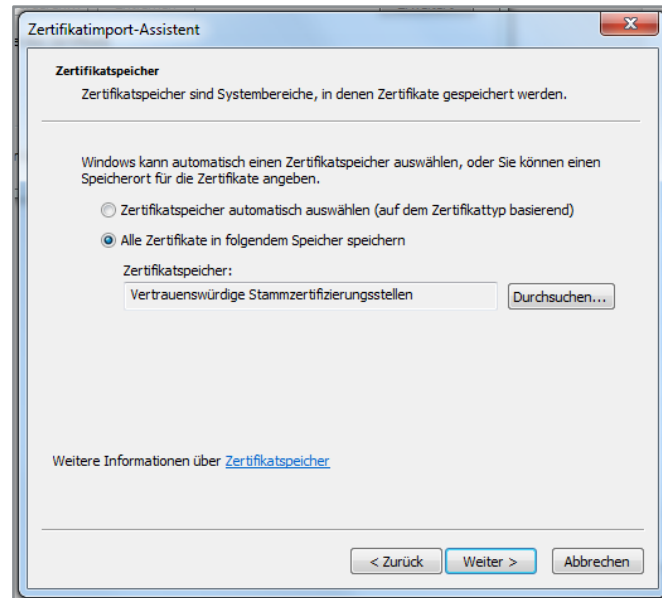


Der Zertifikatsexport-Assistent öffnet sich.

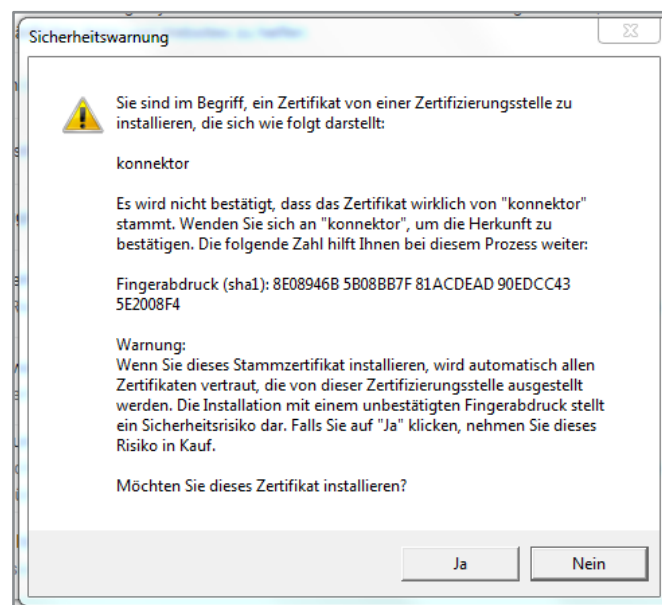


6. Folgen Sie den Anweisungen des Zertifikatsexport-Assistenten und wählen Sie die abgespeicherte Datei mit dem Zertifikat des Modulareren Konnektors aus.
7. Wählen Sie als Zertifikatsspeicher **Vertrauenswürdige Stammzertifizierungsstellen** aus und schließen Sie den Import ab.

Erste Schritte der Installation

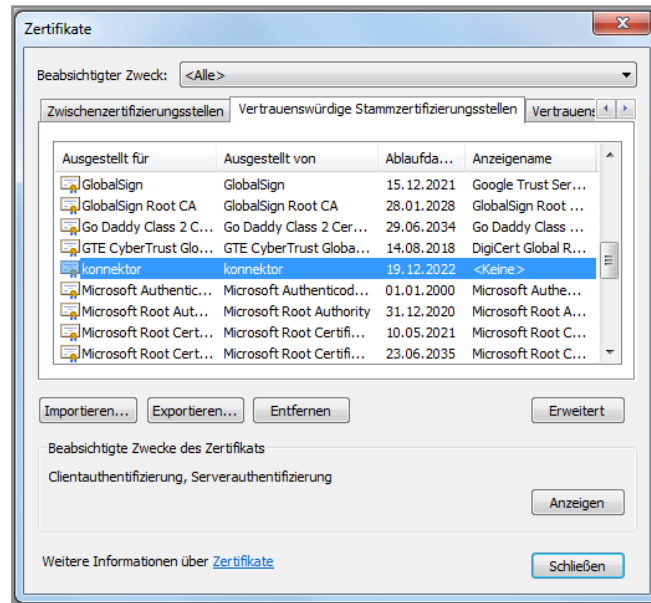


8. Es wird nun eine Sicherheitswarnung angezeigt. Bestätigen Sie, dass Sie dieses Zertifikat installieren möchten.



9. In den Browser-Einstellungen können Sie unter **Zertifikate verwalten** im Reiter **Vertrauenswürdige Stammzertifizierungsstellen** nun das Zertifikat des Konnektors einsehen.
10. Wählen Sie das Zertifikat aus und klicken Sie auf **Anzeigen**, um weitere Informationen zu sehen. Hier können Sie im Reiter **Details** zum Abgleich auch den Fingerprint anzeigen (siehe nachfolgend).

Erste Schritte der Installation



11. Starten Sie den Browser neu.

Das Zertifikat ist nun validiert und Sie können sich auf der Bedienoberfläche des Modularen Konnektors anmelden.

Zertifikatsvalidierungen für weitere Clientsysteme

Sobald Sie einmal das Zertifikat in einem Clientsystem importiert haben, können Sie die Zertifikatsvalidierung für weitere Clientsysteme im lokalen Netzwerk **anhand des exportierten Zertifikats** durchführen, ohne eine direkte Verbindung zwischen Clientsystem und Modularem Konnektor aufzubauen. In diesem Fall müssen Sie sicherstellen, dass das importierte Zertifikat jeweils mit dem bereits validierten Zertifikat übereinstimmt, z. B. über einen Vergleich des Fingerprints der Zertifikate.

Remote Management

Falls Sie Remote Management zulassen wollen, muss das Zertifikat des Modularen Konnektors in das Clientsystem des Remote Administrators importiert werden. Führen Sie dazu die oben beschriebenen Schritte im Browser des Remote-Management-Systems durch und melden Sie sich dabei mit der Adresse für Remote Management an.

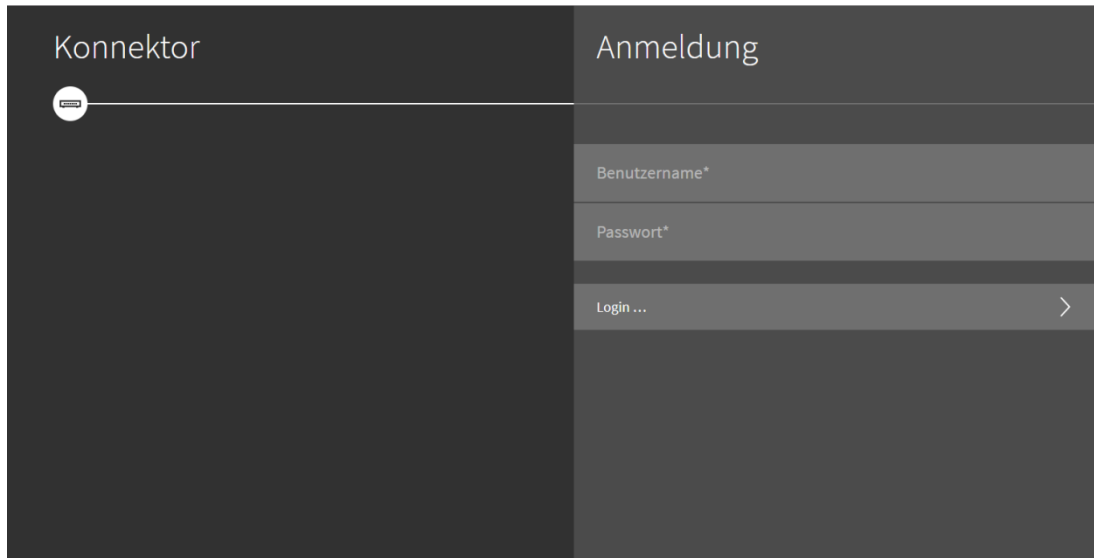
Nach dem Import des Zertifikats des Modularen Konnektors muss der Fingerprint mit dem eines bereits validierten Zertifikats abgeglichen werden. Dies kann zum Beispiel telefonisch erfolgen. Erst danach darf die Remote-Schnittstelle benutzt werden.

Initialpasswort ändern

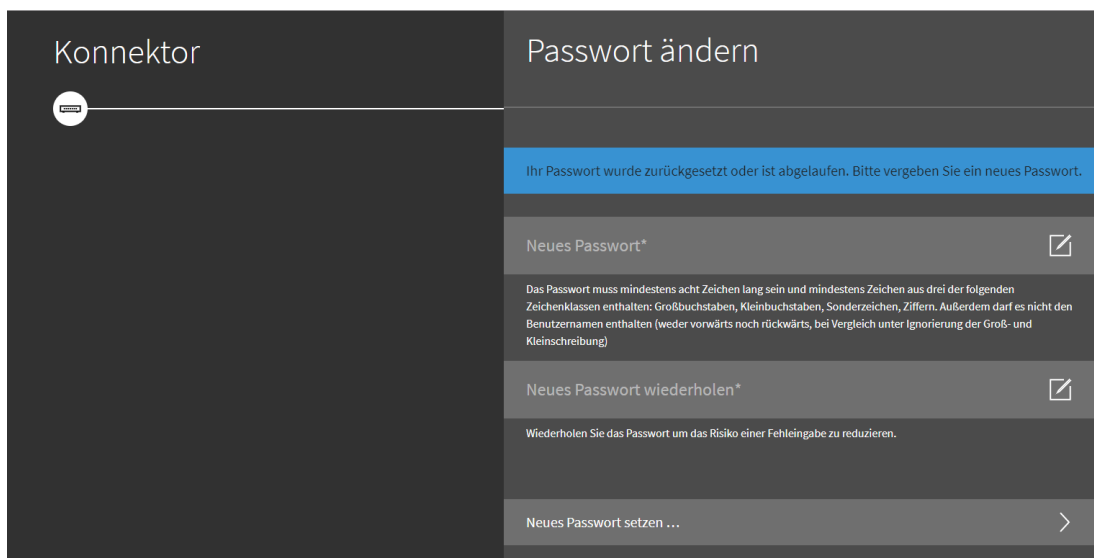
Nachdem Sie das Zertifikat validiert haben, können Sie die WAN- und LAN-Anschlüsse entsprechend des geplanten Einsatzszenarios verbinden und die nächsten Schritte durchführen, um das Initialpasswort zu ändern.

1. Rufen Sie die Bedienoberfläche erneut auf. Sie gelangen diesmal direkt zur Anmeldung.

Erste Schritte der Installation



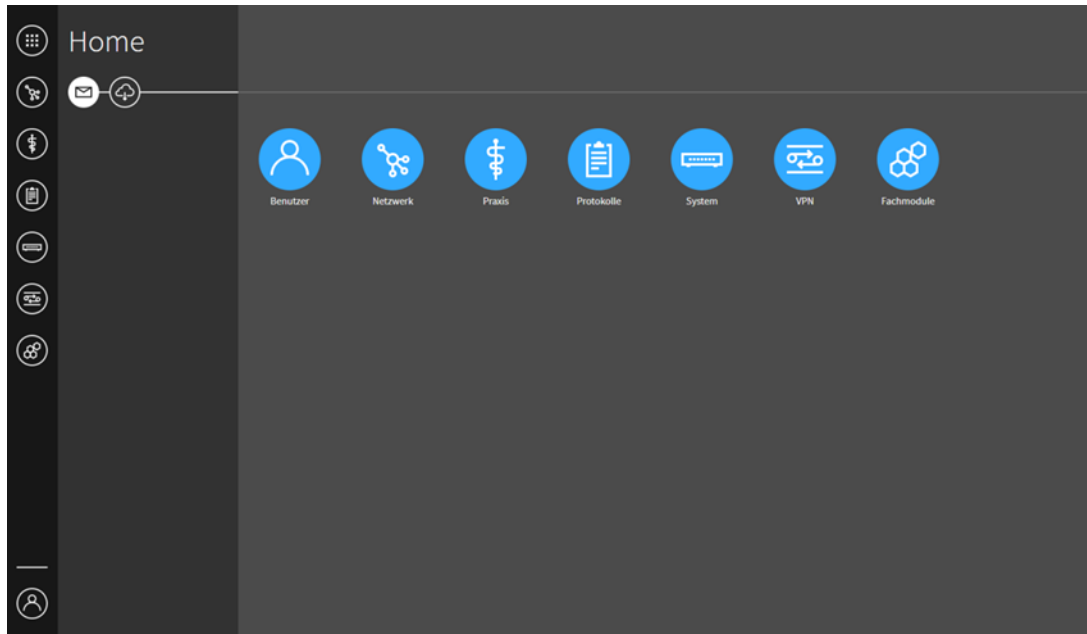
2. Melden Sie sich mit den Initialzugangsdaten aus dem Handbuch des Konnektors an.
Diese lauten:
Benutzername: super
Passwort: konnektor
3. Sie werden aufgefordert, ein neues Passwort einzugeben.
Falls Sie bei der ersten Anmeldung nicht zum Passwortwechsel aufgefordert werden, darf der Modulare Konnektor nicht in Betrieb genommen werden. Es besteht die Gefahr einer möglichen Kompromittierung!
4. Geben Sie ein neues Passwort ein und wiederholen Sie dieses.



5. Klicken Sie auf **Neues Passwort setzen ...**

Das neue Passwort wird dadurch gültig und die Ansicht **Home** wird angezeigt.
Das initiale Benutzerkonto besitzt die Benutzerrolle *Super-Admin*. Sie haben damit Zugriff auf alle Konfigurationsdaten und Benutzerkonten.

Erste Schritte der Installation

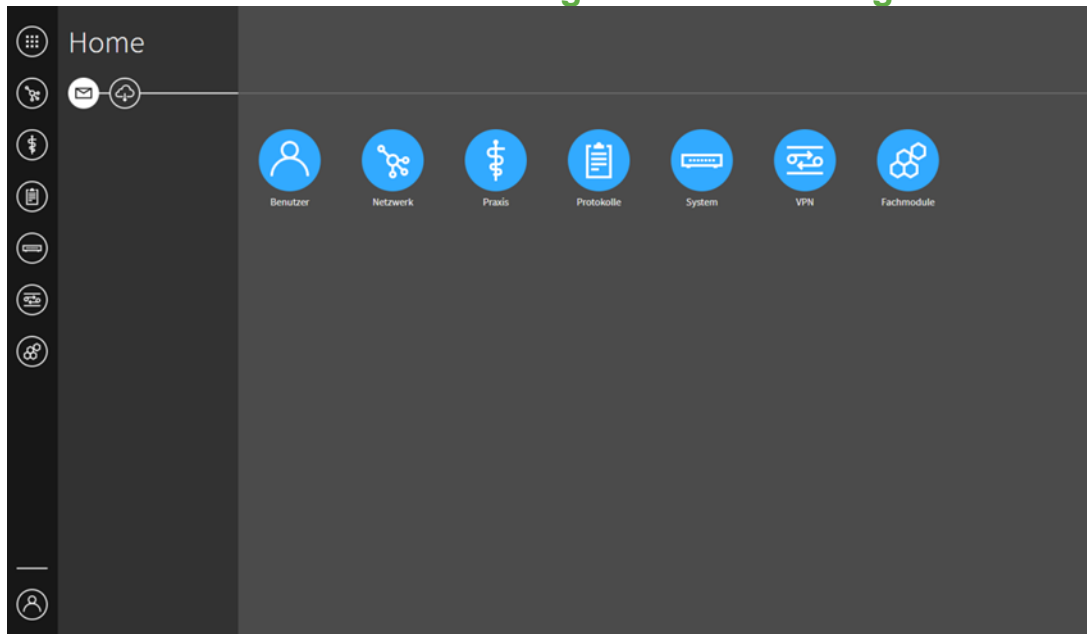


Zusammenfassung

Bevor Sie das Netzwerk und den Konnektor konfigurieren können, müssen Sie

1. die Transportverpackung auf Unversehrtheit überprüfen und die Komponenten auspacken,
2. Die Gehäuse-Sicherheitssiegel prüfen,
3. die gSMC-KT-Karten in die Kartenterminals stecken und die Slots versiegeln,
4. den Konnektor mit dem Clientsystem verbinden,
5. das Konnektor-Zertifikat validieren,
6. das Initialpasswort des Konnektors ändern.

Abschnitt 4: Einführung in die Bedienungsoberfläche



Der Home-Bildschirm

Hier sehen Sie den Home-Bildschirm der Bedienungsoberfläche des Konnektors. An dieser Stelle werden wir Ihnen die einzelnen Symbole, die Sie von hier aus anwählen können, vorstellen, bevor wir Ihnen in der nächsten Lerneinheit die einzelnen Konfigurationsmöglichkeiten zeigen. Direkt unter dem Schriftzug „Home“ sehen Sie ein weiteres Symbol.



Unterhalb dieses Symbols werden Ihnen der Status VPN-TI und SIS-TI sowie Sicherheitskritische Fehlermeldungen angezeigt. Schauen Sie zur Interpretation etwaiger Fehlermeldungen in das Handbuch.

Auf der linken Seite sehen Sie eine Reihe von Symbolen, die von jeder Seite der Bedienoberfläche aus anwählbar sind. Dies sind Shortcuts zu den verschiedenen Hauptmenüs, die Sie auch auf dem Home-Bildschirm sehen. Klicken Sie auf jedes Symbol, um Erläuterungen dazu zu erhalten.

Benutzer

Durch einen Klick auf diese Schaltfläche gelangen Sie zur Benutzerverwaltung. Hier können Sie Benutzerprofile anlegen und das Passwort ändern.

Netzwerk

Im Menü **Netzwerk** werden die LAN- und WAN-Schnittstellen und die Einstellung zur Netzwerk-Funktionalität konfiguriert, um den Modulare Konnektor in die Netzwerkumgebung einzubinden.

Praxis

Über den Bereich **Praxis** gelangen Sie zu den Einstellungen für Kartenterminals und können sich die gesteckten Karten anzeigen lassen. Außerdem gelangen Sie hier in den Bereich, in

Erste Schritte der Installation

dem Clientsysteme angelegt, verwaltet und die Verbindungseinstellungen konfiguriert werden können. Arbeitsplätze, Mandanten und Aufrufkontexte werden ebenfalls hier angelegt und konfiguriert.

Diagnose

Im Bereich **Diagnose** werden aktuelle Statusmeldungen und Betriebsinformationen angezeigt und vergangene Protokolleinträge können durchsucht sowie gelöscht werden.

System

Hierüber können verschiedene Systemeinstellungen erreicht werden. Der Konnektornamen kann definiert werden und Remote-Management sowie Standalone-Szenario können konfiguriert werden. Über das System-Menü kann auch ein Neustart mit oder ohne Werksreset des Konnektors durchgeführt werden.

TSL-Zertifikate können verwaltet, die Systemzeit des Konnektors eingestellt und Einstellungen zu Aktualisierungen des Konnektors getätigt werden. Außerdem können Sie sich im System-Menü die Version des Produkts anzeigen lassen und ein Backup der Einstellungen erstellen und auch einspielen.

VPN

Im Bereich VPN-Zugangsdienst kann der Modulare Konnektor mit Freischaltung für einen Mandanten am VPN-Zugangsdienst der TI freigeschaltet werden.

Fachmodule

Dieser Button ermöglicht den Zugriff auf die Konfiguration des Fachmoduls VSDM.

In der Bedienoberfläche navigieren

In den Dialogfenstern der Bedienoberfläche navigieren Sie mit folgenden Symbolen:



Dieser Pfeil bringt Sie zurück zum vorigen Bereich.



Hiermit löschen Sie Eingaben.



Das Kreuz verwirft Ihre Eingabe in dem entsprechenden Feld.



Mit dem Haken bestätigen Sie Ihre Eingabe.



Mit dem Pluszeichen fügen Sie neue Elemente hinzu.



Mit diesem Feld beginnen Sie eine neue Eingabe.



Die Punkte führen zu weiteren Einstellungen.

Erste Schritte der Installation



Durch einen Klick auf dieses Symbol können sie eine Auswahlliste ausklappen.

Sie können einen der angezeigten Werte wählen, wobei der aktuell gewählte Wert hervorgehoben ist (Beispiel).



Lade-/Warteanzeigen:



Dieses Symbol zeigt an, dass die Seite lädt.

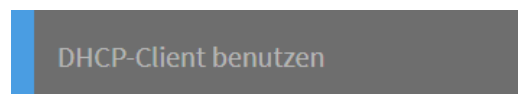


Dieses Symbol zeigt an, dass Ihre gewünschte Aktion durchgeführt wird.

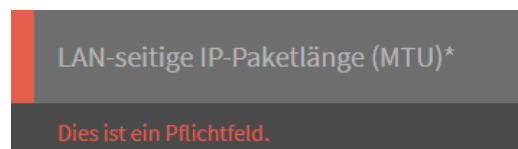
Die Prüfung von Eingaben

Wenn in einem Dialogfenster eine konfigurierte Einstellung verändert wird, wird die Validität automatisch geprüft und über Farbbalken vor dem Eingabefeld angezeigt:

Blau bedeutet, dass die Eingabe gültig ist.



Rot bedeutet, dass die Eingabe nicht gültig ist. Zusätzlich wird ein Fehlertext angezeigt.



Erste Schritte der Installation

Warnungen und Hinweise

Wenn Einstellungen vorgenommen werden, die Auswirkungen auf den Betrieb haben (z. B. Neustart oder Werksreset) oder wenn Elemente gelöscht werden (z. B. Mandanten oder Benutzer), wird ein Warnhinweis angezeigt. Bestätigen Sie diesen, um die Aktion durchzuführen.

Wichtige Informationen zum Status und zu aktuellen Vorgängen (z. B. eine fehlende Verbindung zur TI oder zum Herunterfahren des Modularen Konnektors) werden in einem farbigen Hinweis am oberen Bildschirmrand angezeigt.

Abschnitt 5: Schluss

Haben Sie die Lernziele erreicht?

1. Sie können die ersten Prozessschritte der Installation benennen.
2. Sie können den Konnektor erstmalig in Betrieb nehmen.
3. Sie kennen den grundlegenden Aufbau der Bedienungsoberfläche

Mitwirkende

Dr. Christian Ummerle

Arzt und Medizininformatiker. Ist seit mehr als 25 Jahren in verschiedenen leitenden Positionen im Bereich der IT im Gesundheitswesen tätig. Seit 2007 beschäftigt er sich schwerpunktmäßig mit Themen der Telematikinfrastruktur. Von 2010 bis 2017 war er Projektleiter für den GKV-Spitzenverband für das Versichertenstammdatenmanagement (VSDM) bei der gematik, das mit der erfolgreichen Erprobung des VSDM abgeschlossen wurde. Er ist Mitgründer und Prokurist der eHealth Experts GmbH. eHealthExperts ist eines der führenden Unternehmen in Deutschland für die Entwicklung und Testung von Informationssystemen in der Telematikinfrastruktur.

Gorden Bittner

hat Verwaltungswissenschaften studiert und leitete vor seiner Tätigkeit bei der secunet Security Networks AG den Fachbereich HealthCare bei TÜV Rheinland Consulting. Zuvor war er ca. 10 Jahre als Berater und Projektleiter im Gesundheitswesen tätig – vorrangig in leitender Funktion in Projekten rund um das Thema Telematik und Telemedizin. Herr Bittner hat unter anderem die Einführung der eGK für die AOK Gemeinschaft seit 2011 maßgeblich mitgestaltet und in diversen eHealth-Projekten seit 2006 mitgewirkt.

Robert Rath

war als examinierter Gesundheits- und Krankenpfleger über sieben Jahre in der stationären Pflege an der Berliner Charité beschäftigt. Dort arbeitete er im Fachbereich Hämatologie und Onkologie und war spezialisiert auf die Versorgung von chronischen Wunden und die praktische Anleitung von Auszubildenden und Praktikanten. Zusätzlich hat Herr Rath drei Jahre lang Gesundheitswissenschaften an der Charité studiert und den akademischen Grad Bachelor of Science erworben. Zurzeit ist er Fachautor bei Relias Learning und arbeitet gelegentlich als freier Dozent für das Thema Wundversorgung im Studiengang Bachelor of Nursing der Evangelischen Hochschule Berlin.

Weiterführende Literatur

Webseite der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik)
<https://www.gematik.de/>

Checkliste für Dienstleister vor Ort der gematik:

Erste Schritte der Installation

https://fachportal.gematik.de/fileadmin/user_upload/gematik/files/OPB-Infomaterialien/gem_2017-12-CL-DVO_checkliste_dienstleister_online.pdf

Glossar der Telematikinfrastruktur der gematik:

https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Spezifikationen/Methodische_Festlegungen/gemGlossar_V400.pdf

Quellennachweise

Secunet Security Networks AG (2018): Modularer Konnektor Version 2.0.0 – Bedienhandbuch für Administratoren und Benutzer, Version 1.0

Ingenico Healthcare e-ID (2017): Endnutzer-Checkliste „Sichere Lieferkette“, Version 7.11.1

Fast geschafft

Schließen Sie dieses Fenster, um zur Relias-Plattform zurückzukehren.

Überprüfung

1. Benennen Sie den nächsten Schritt, nachdem Sie die gSMC-KT in den Karteneinschub eines Kartenterminals gesteckt haben.

Sie versiegeln den Karteneinschub mit einem unterschriebenen Slot-Siegel.

Sie trennen das Kartenterminal vom Strom.

Sie dokumentieren, dass Sie die gSMC-KT in den Karteneinschub gesteckt haben.

Sie ändern das Passwort des Konnektors.

2. Sie wollen die Erstanmeldung am Konnektor durchführen. Was müssen Sie vorher sicherstellen?

Außer dem LAN-Anschluss zum Clientsystem sollten keine weiteren Netzwerkkomponenten angeschlossen sein.

Vor der Erstanmeldung müssen Sie zwingend das Initialpasswort ersetzen.

Sämtliche Sicherheitssiegel müssen dokumentiert und entfernt werden.

Die Zertifikatsvalidierung muss abgeschlossen sein.

3. Sie finden eine Komponente, deren Sicherheitssiegel beschädigt ist. Wie reagieren Sie?

Sie inspizieren die Komponente eingehend und wenn Sie keine Mängel feststellen können, erneuern Sie das Siegel.

Sie inspizieren die Komponente eingehend und wenn Sie keine Mängel feststellen können, machen Sie einen Vermerk in den Unterlagen und fahren mit der Installation fort.

Sie nehmen das Gerät nicht in Betrieb, sondern nutzen ein Ersatzgerät.

Sie brechen die Installation ab.

4. Woran erkennen Sie, dass der Konnektor betriebsbereit ist?

Die LED der Betriebsanzeige System leuchtet durchgehend.

Erste Schritte der Installation

Die LED der Betriebsanzeige System blinkt.

Die LED der Betriebsanzeige Power blinkt.

Die LEDs aller Betriebsanzeigen außer Update und Remote leuchten durchgehend.

5. Benennen Sie den Zweck der Validierung des Konnektor-Zertifikats.

Es gewährleistet, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird und somit der Schutz von Daten sichergestellt ist.

Es dient der Sicherstellung der korrekten Verbindung des Konnektors an die Telematikinfrastruktur.

Es gewährleistet, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird und somit der schnellstmögliche Datentransfer sichergestellt werden kann.

Es gewährleistet, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird und ermöglicht die Nutzung von weiteren Komponenten wie Kartenterminals.

Lernimpulse

LZ	FNr.	Frage / Antwortmöglichkeiten
1	1	Sie finden eine Komponente, deren Sicherheitssiegel beschädigt ist. Wie reagieren Sie?
		Sie inspizieren die Komponente eingehend und wenn Sie keine Mängel feststellen können, erneuern Sie das Siegel.
		Sie inspizieren die Komponente eingehend und wenn Sie keine Mängel feststellen können, machen Sie einen Vermerk in den Unterlagen und fahren mit der Installation fort.
		Sie nehmen das Gerät nicht in Betrieb, sondern nutzen ein Ersatzgerät.
		Sie brechen die Installation ab.
1	2	Benennen Sie den Zweck der Validierung des Konnektor-Zertifikats.
		Es gewährleistet, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird und somit der Schutz von Daten sichergestellt ist.
		Es dient der Sicherstellung der korrekten Verbindung des Konnektors an die Telematikinfrastruktur.
		Es gewährleistet, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird und somit der schnellstmögliche Datentransfer sichergestellt werden kann.
		Es gewährleistet, dass bei Verbindungsanfragen zum Modulare Konnektor das korrekte Zertifikat verwendet wird und ermöglicht die Nutzung von weiteren Komponenten wie Kartenterminals.

