GMC Systems mbH

Installation und Konfiguration von KIM für GMC PaDok

Datum: 08.12.2020

GMC Systems mbH
Albert-Einstein-Straße 3
98693 Ilmenau

Inhaltsverzeichnis

1 KIM 3

2 Voraussetzungen 3

2.1 TI-Zugang 3

2.2 KIM Anmeldung/ Registrierung und Installation des KIM-Client Modules 3

2.3 Kartenterminal und Kryptographiekarten 4

2.4 Systemvoraussetzungen 4

2.5 Installation der GMC Padok Version 4

3 Konfiguration eines KIM-Kontos im GMC PaDok 4

3.1 TI-Konfiguration 4

3.2 Konfiguration des KIM-Accounts 7

4 Kryptokartenverwaltung 9

4.1 Änderung der PIN einer Kryptokarte 11

4.2 Ersetzen der Transport-PIN einer transportgeschützten Kryptokarte 12

4.3 Entsperren einer gesperrten PIN mit Hilfe der PUK 14

1 KIM

Mit dem Kommunikationsdienst KIM (Kommunikation im Medizinwesen) ist es für Praxen möglich, medizinische Dokumente elektronisch und sicher über die Telematikinfrastruktur (TI) zu versenden und zu empfangen. KIM verbindet erstmalig Nutzer im Gesundheitswesen über Einrichtungs-, System- und Sektorengrenzen hinweg. Mit KIM können alle TI-Teilnehmer miteinander kommunizieren. Hierzu zählen beispielsweise Ärzte, Zahnärzte, Psychotherapeuten und Apotheker in medizinischen Einrichtungen wie Praxen, Versorgungszentren, Apotheken und Krankenhäuser. Aber auch die offiziellen Interessensvertretungen der benannten Berufsgruppen, wie KBV/KVen, KZBV/KZVen, GKV-SV/Kassen, ABDA und DKG.

Die Vorteile von KIM:

Vertraulichkeit der Nachrichten: Sensible Daten können immer nur von demjenigen gelesen werden, für den sie gedacht sind. Kartenbasierte Verschlüsselung macht ein unberechtigtes Mitlesen nachweislich unmöglich.
Fälschungssicher: Niemand kann KIM-Nachrichten unbemerkt verfälschen und manipulieren. Adressaten erkennen immer, ob sie die E-Mail so erhalten haben, wie sie der Absender auch verschickt hat.
Geprüfte Identität: Empfänger einer Nachricht können immer sicher sein: Wer als Absender draufsteht, ist auch der Absender der Nachricht. Denn die Identitäten der Kommunikationspartner werden vor der Anlage im Adressbuch zweifelsfrei geprüft.
Schnelle Auffindbarkeit: Alle KIM-Teilnehmer sind im zentralen Adressbuch auffindbar. Es entfällt ein umständliches Suchen von E-Mail-Adressen.
Abrechenbarkeit: KIM ist das sichere Übermittlungsverfahren nach § 291b Abs. 1e SGB V und dadurch die Basis für eine mögliche Vergütung.

2 Voraussetzungen

2.1 TI-Zugang

Grundlage für KIM ist ein Anschluss an die Telematikinfrastruktur mit dem sogenannten **E-Health-Konnektor.** Dieser unterstützt neben dem Versichertenstammdatenmanagement (VSDM) auch medizinische Anwendungen wie den elektronischen Medikationsplan (eMP) und das Notfalldatenmanagement (NFDM). Praxen, welche bereits an die TI angebunden sind, benötigen ein Konnektor-Update: damit wird ihr vorhandenes Gerät zum E-Health-Konnektor, welcher zusätzlich die qualifizierte elektronische Signatur unterstützt. Erste Hersteller haben ihre Updates Mitte 2020 zur Verfügung gestellt. Wenden Sie sich für weitere Informationen bitte an ihren PVS-Hersteller oder IT-Dienstleister.

2.2 KIM Anmeldung/ Registrierung und Installation des KIM-Clientmodules

Es wird ein Vertrag mit einem von der gematik zugelassenen KIM-Anbieter benötigt, welcher Ihnen das KIM-Clientmodul und ein KIM-Postfach zur Verfügung stellt. Nach erfolgter Anmeldung wird das KIM-Clientmodul in Ihrer Einrichtung installiert und konfiguriert und Sie erhalten eine spezielle E-Mail-Adresse für den Kommunikationsdienst KIM. Folgen Sie dazu bitte den Anweisungen Ihres KIM-Anbieters.

2.3 Kartenterminal und Kryptographiekarten

Damit KIM zum Einsatz kommen kann, benötigen medizinische Einrichtungen einen E-Health-Konnektor, ein Kartenterminal, einen Praxis-/Institutionsausweis (SMC-B) und gegebenenfalls einen Heilberufsausweis (HBA) mindestens der Generation 2.0 für die qualifizierte elektronische Signatur beim Versand etwa von eArztbriefen oder eAU´s. Liegt ein Heilberufsausweis noch nicht vor, sollte dieser schnellstmöglich bei der jeweiligen Standesorganisation beantragt werden.

2.4 Systemvoraussetzungen

- Betriebssystem
  - Windows 7 SP1 oder höher (empfohlen Windows 10)
  - Windows Server 2008 R2 oder höher (empfohlen Windows Server 2016)
- Es werden folgende freigeschalteten Ports für die Kommunikation mit dem TI-Konnektor bzw. dem KIM-Clientmodul benötigt:
  - POP3: Port 995 (TLS)
  - SMTP: Port 465 (TLS)
  - LDAP: Port 636

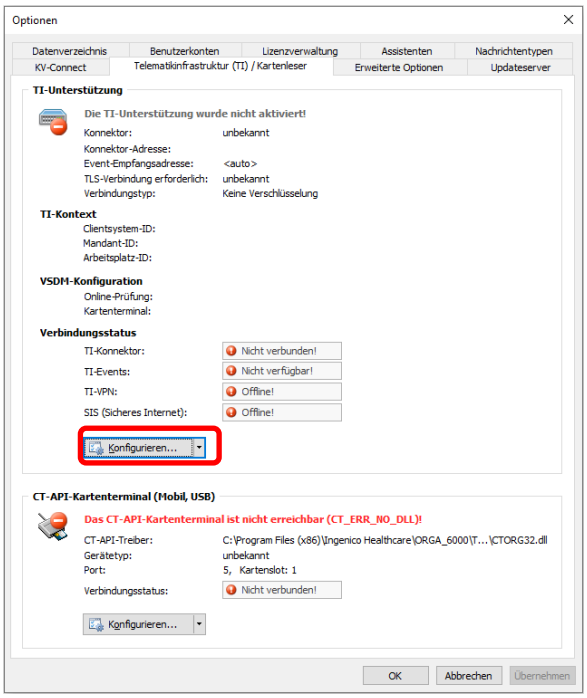
2.5 Installation der GMC PaDok Version

Die Funktionalität „Kommunikation über KIM“ wird Ihnen ab der GMC PaDok Version 4.4.6.0 zur Verfügung gestellt. Bitte installieren Sie diese oder eine höhere Programmversion bzw. spielen Sie das Update für ein vorhandenes GMC PaDok ein.

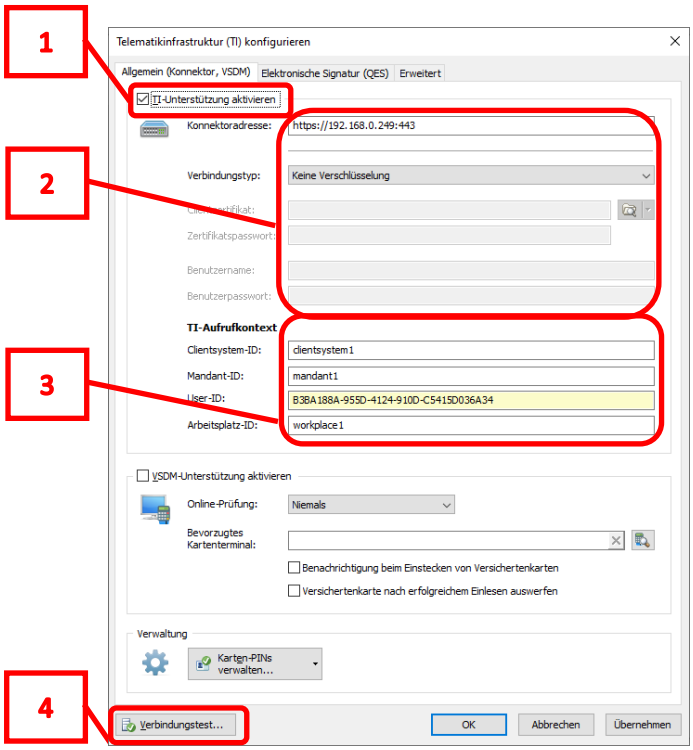
3 Konfiguration eines KIM-Kontos im GMC PaDok

3.1 TI-Konfiguration

Zur Kommunikation mit den Kryptokarten SMC-B (Einrichtungskarte) und/oder HBA (Heilberufsausweis) muss GMC PaDok den Konnektor und die Kartenterminals erreichen, in welchen die benötigten Karten stecken. Wenn Sie diesen TI-Aufrufkontext im GMC PaDok bisher noch nicht für das Einlesen von Versichertenkarten (VSDM) konfiguriert haben, so müssen Sie dies für die Nutzung der KIM-Funktionalität im GMC PaDok jetzt tun. Öffnen Sie dazu bitte den Konfigurationsdialog im Menü unter Extras/Optionen/Telematikinfrastruktur (TI) / Kartenleser.



Bei Neueinrichtung der TI-Funktionalität werden alle Pflichtfelder rot markiert. Gehen Sie auf „Konfigurieren“.

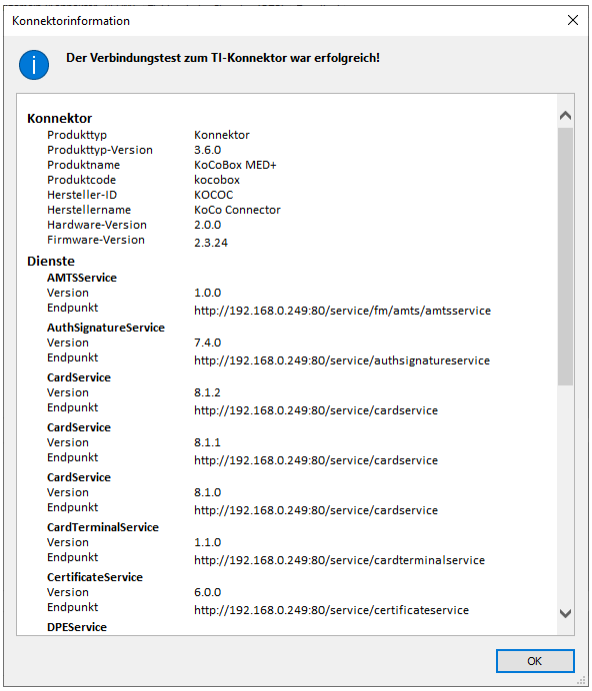


(1) Der folgende Eingabedialog öffnet sich, aktivieren Sie hier als erstes die TI-Unterstützung für GMC PaDok.

(2) Geben Sie dann bitte die IP-Adresse einschließlich Protokoll und Port unter der der TI-Konnektor im Netzwerk erreichbar ist und den Verbindungstyp der Verbindung zum TI-Konnektor Ihrer Praxis an.

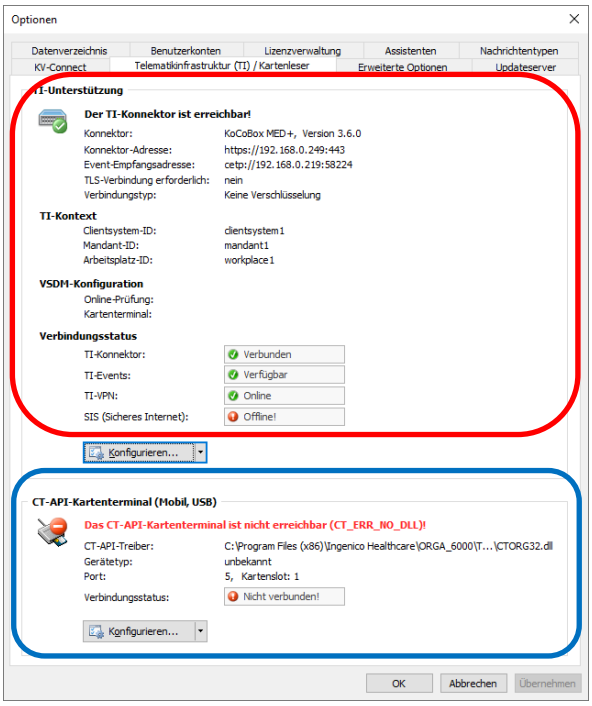
(3) Nun müssen Sie noch den TI-Aufrufkontext, welcher sich aus der Clientsystem-ID, der Mandant-ID und der Arbeitsplatz-ID zusammensetzt konfigurieren. Diese Daten entnehmen Sie bitte aus der TI-Konnektorkonfiguration oder der TI-Konfiguration Ihres Praxisverwaltungssystems.

(4) Um die Korrektheit der angegebenen Daten zu überprüfen, können Sie einen Verbindungstest zum TI-Konnektor durchführen.



Ist die TI-Konfiguration korrekt und der TI-Konnektor im Netzwerk erreichbar, so erhalten Sie eine Erfolgsmeldung.

Bestätigen Sie diese mit „OK“ und übernehmen Sie die Konfiguration.

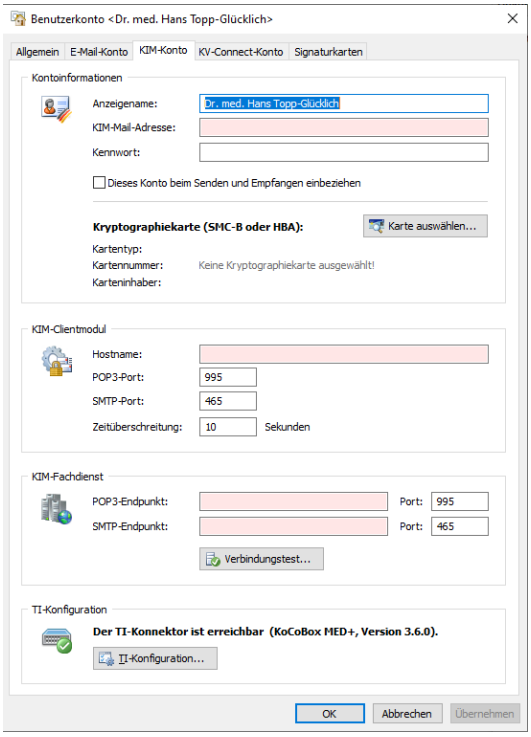


Auf der Optionsseite zur TI-Unterstützung wird Ihnen nun der Verbindungsstatus zum TI-Konnektor, der TI-Aufrufkontext und die verfügbaren TI-Dienste angezeigt.

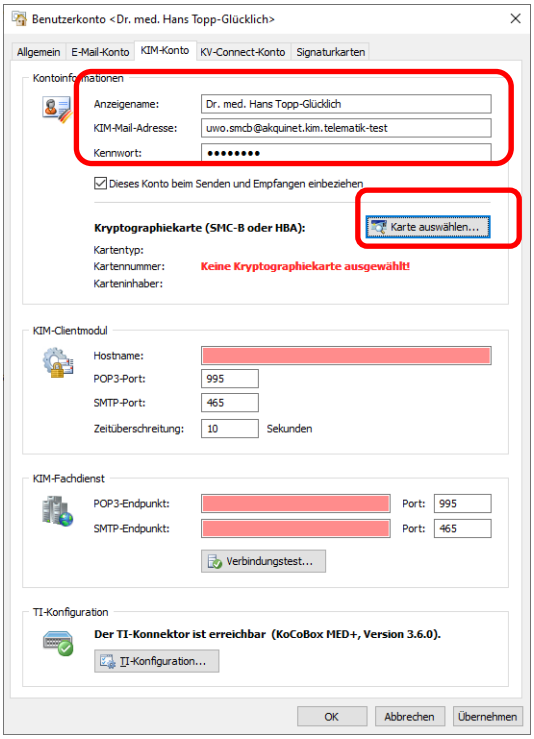
Der blau markierte Bereich ist für KIM nicht relevant. Hier können Sie ein evtl. noch in der Praxis vorhandenes per USB angeschlossenes CT-API Kartenterminal bzw. ein mobiles TI-Kartenterminal konfigurieren.

3.2 Konfiguration des KIM-Accounts

Die von Ihnen bei Ihrem KIM-Anbieter registrierte KIM-Mail-Adresse für Ihr KIM-Postfach müssen Sie nun mit einem GMC-PaDok Benutzerkonto verknüpfen, um KIM-Nachrichten bzw. eArztbriefe mit GMC PaDok versenden bzw. empfangen zu können. Falls Sie eine KIM-Mailadresse für die Praxis und weitere persönliche Arzt-Mailadressen registriert haben, so ordnen Sie die KIM-Mailadresse für die Praxis dem Praxiskonto in GMC PaDok zu und die Arzt-Mailadressen den entsprechenden Arztkonten.

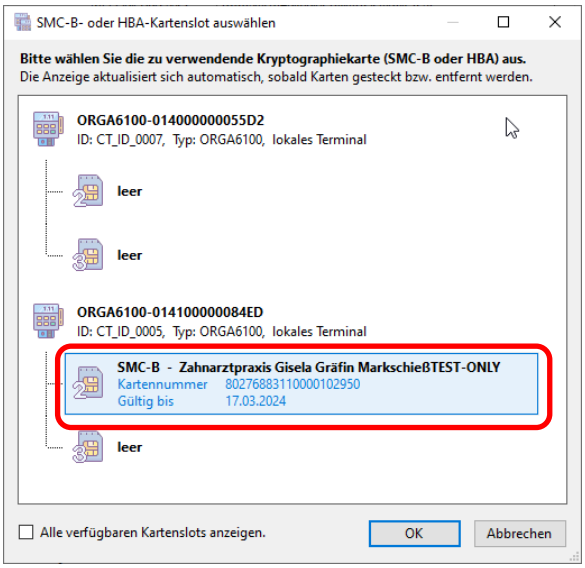


Melden Sie sich dazu mit dem entsprechenden Benutzerkonto am GMC PaDok an und gehen im Menü Extras/Nutzereinstellungen auf den Reiter „KIM-Konto“. Es öffnet sich dieser Eingabedialog.

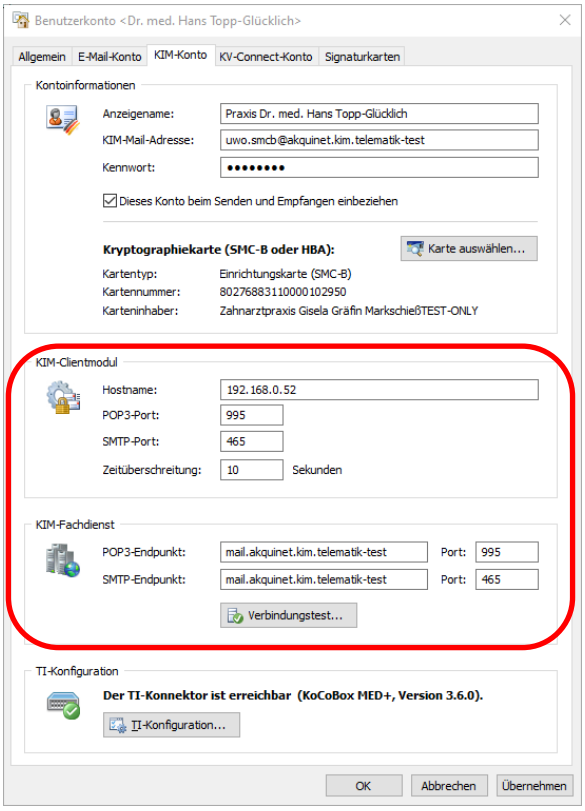


Der Anzeigename für das KIM-Konto wird aus den Nutzereinstellungen schon vorbelegt, kann aber von Ihnen geändert werden. Geben Sie hier bitte Ihre KIM-Mailadresse und Ihr Kennwort ein.

Gehen Sie dann auf „Karte auswählen“.

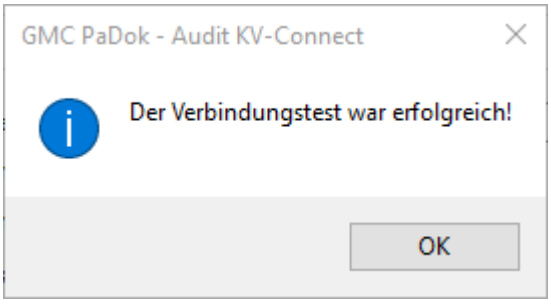


Wählen Sie im sich daraufhin öffnenden Kartenauswahldialog die TI-Kryptokarte aus, auf welche Sie die KIM-Mailadresse bei Ihrem KIM-Anbieter registriert haben. Dies kann eine SMC-B (Einrichtungskarte) oder ein HBA (Heilberufsausweis) sein. Diese Kryptokarte wird insbesondere zur Entschlüsselung von empfangenen KIM-Nachrichten benötigt. Bestätigen Sie Ihre Auswahl mit „OK“.



Als letztes müssen Sie noch angeben, unter welchem Hostnamen bzw. unter welcher IP-Adresse das KIM-Clientmodul sowie unter welchem Hostnamen der KIM-Fachdienst in Ihrem Netzwerk erreichbar ist. Fragen Sie dazu ggf. Ihren KIM-Anbieter.

Zum Test Ihrer Eingaben gehen Sie bitte auf „Verbindungstest“.



Ist die Verbindung zum KIM-Clientmodul und zum Fachdienst möglich, so erhalten Sie eine Erfolgsmeldung.

Sie können Ihr KIM-Mailkonto nun zum Versenden und Empfangen von KIM-Nachrichten nutzen!

4 Kryptokartenverwaltung

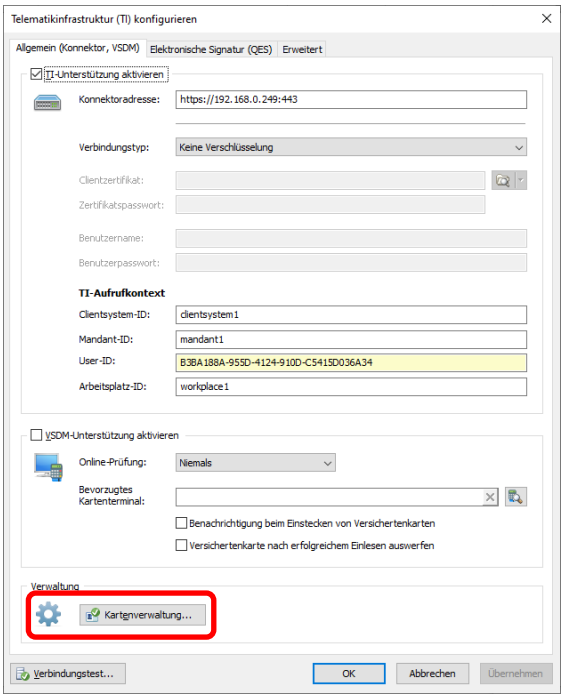
Zur Verwaltung der TI-Kryptokarten (eGK, SMC-B bzw. HBA) gibt es in GMC PaDok eine Kartenverwaltung, mit deren Hilfe Sie:

- den aktuellen PIN-Status der Karten-PINs abfragen können
- Transport-PINs durch individuelle Karten-PINs ersetzen können
- gesperrte PINs mit Hilfe der zugehörigen PUK entsperren können

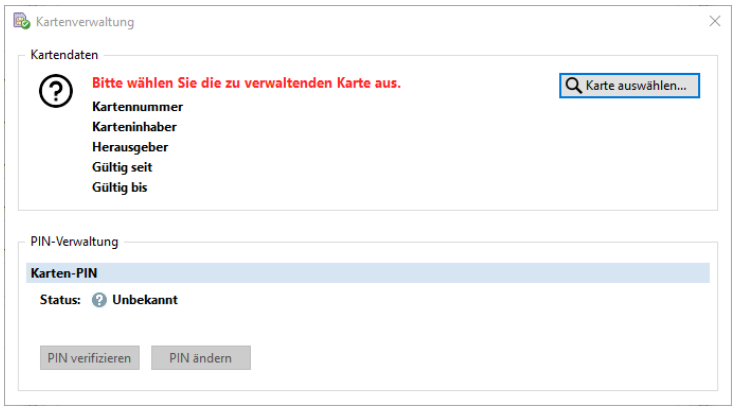
sowie

- bestehende Karten-PINs durch neue PINs ersetzen können.

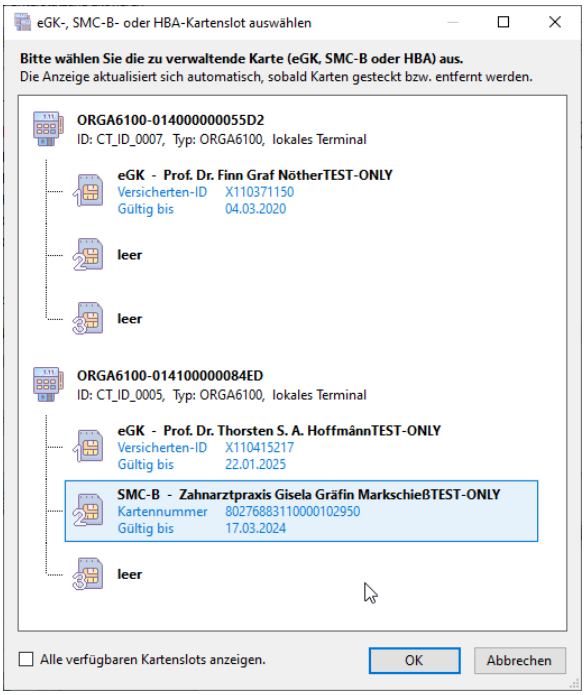
Die Funktion „Transport-PINs durch individuelle Karten-PINs ersetzen“ müssen Sie z.B. durchführen, wenn Sie ihren neuen HBA vom Kartenanbieter erhalten haben, bevor Sie diesen verwenden können.



Um zur Kryptokartenverwaltung zu gelangen, öffnen Sie bitte die TI-Konfiguration im Menü unter Extras/Optionen/Telematikinfrastruktur (TI) / Kartenleser. Gehen Sie dort bitte auf „Konfigurieren“ und im sich öffnenden Konfigurationsdialog klicken Sie bitte auf den Button „Kartenverwaltung“.

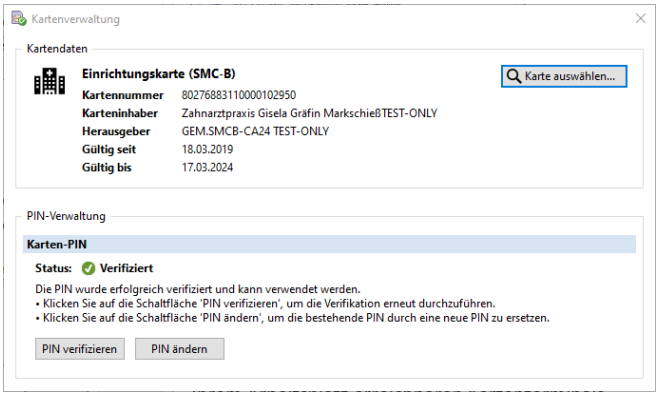


Sie werden aufgefordert, die zu verwaltenden TI-Kryptokarte auszuwählen.



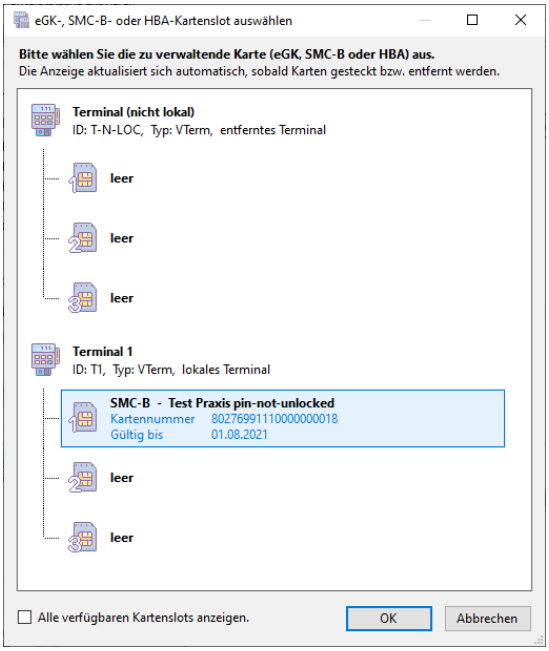
Es öffnet sich der Kartenauswahldialog, welcher alle verfügbaren Kryptokarten, welche in den von Ihrem Arbeitsplatz erreichbaren Kartenterminals stecken, anzeigt.

Wählen Sie nun die entsprechende Kryptokarte aus.

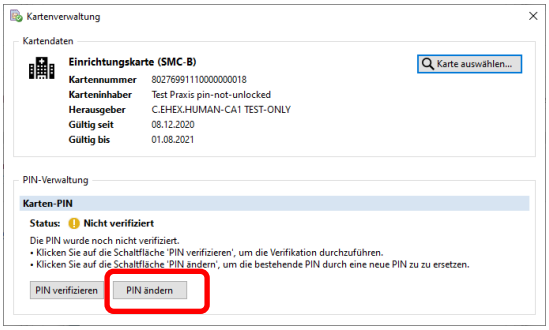


Es werden Ihnen im oberen Bereich die Informationen wie Kartennummer (ICCSN), Karteninhaber, Kartenherausgeber sowie Gültigkeitsdaten angezeigt. Im unteren Bereich werden Ihnen die PIN-Statusinformationen der Karte angezeigt und die vom PIN-Status abhängigen Funktionen zur Verfügung gestellt.
Ist wie hier im Beispiel der PIN-Status der Karten-PIN der SMC-B verifiziert, so können Sie die PIN erneut verifizieren oder die Karten-PIN ändern.

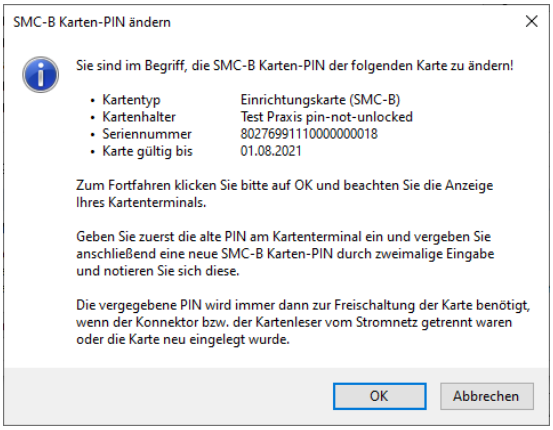
4.1 Änderung der PIN einer Kryptokarte



Öffnen Sie bitte die Kartenverwaltung wie oben beschrieben und wählen Sie die Karte aus, deren PIN Sie ändern wollen.

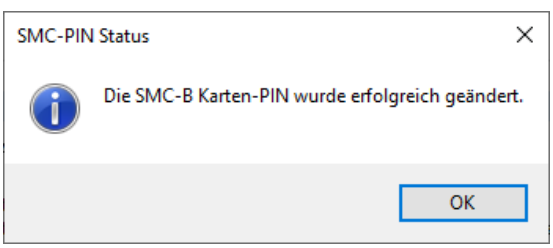


Es werden Ihnen im sich öffnenden Dialog im oberen Bereich die Informationen wie Kartennummer (ICCSN), Karteninhaber, Kartenherausgeber sowie Gültigkeitsdaten angezeigt. Im unteren Bereich werden Ihnen die PIN-Statusinformationen der Karte angezeigt und die vom PIN-Status abhängigen Funktionen zur Verfügung gestellt.
Klicken Sie hier auf „PIN ändern“.



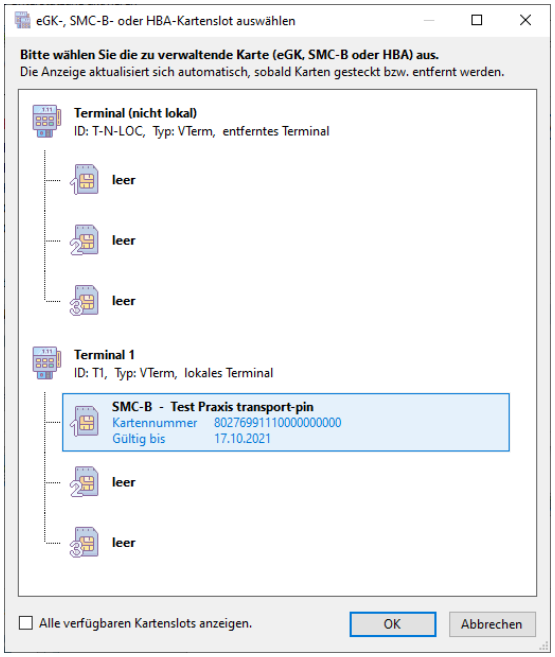
Es wird Ihnen ein Hinweis zum weiteren Ablauf angezeigt. Im Folgenden müssen Sie die Anzeige Ihres Kartenterminals beachten. Sie werden dazu aufgefordert zuerst Ihre alte PIN einzugeben und danach eine neue PIN durch zweimalige Eingabe zu vergeben.

Bitte notieren Sie die neu vergebene PIN und verwahren Sie diese sicher.

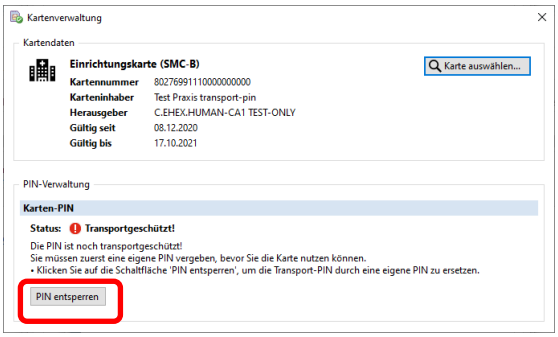


Sie erhalten eine Erfolgsmeldung, wenn die PIN erfolgreich geändert wurde.

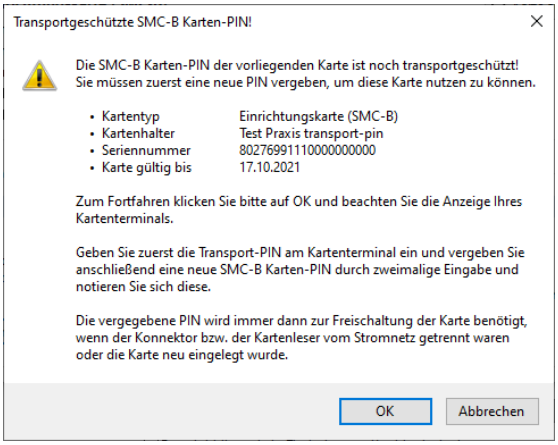
4.2 Ersetzen der Transport-PIN einer transportgeschützten Kryptokarte



Öffnen Sie bitte die Kartenverwaltung wie oben beschrieben und wählen Sie die Karte aus, deren Transport-PIN Sie durch die richtige PIN ersetzen wollen.

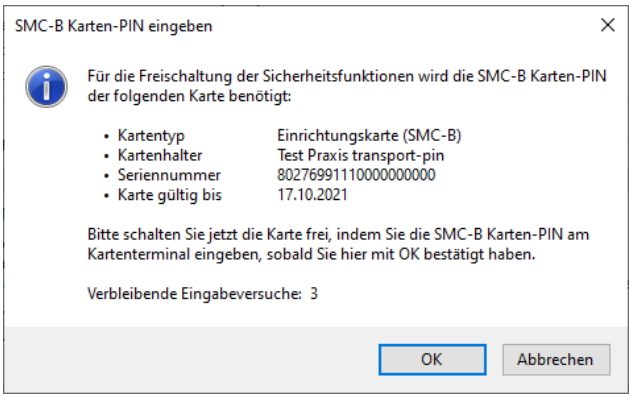


Es werden Ihnen im sich öffnenden Dialog im oberen Bereich die Informationen wie Kartennummer (ICCSN), Karteninhaber, Kartenherausgeber sowie Gültigkeitsdaten angezeigt. Im unteren Bereich werden Ihnen die PIN-Statusinformationen der Karte angezeigt und die vom PIN-Status abhängigen Funktionen zur Verfügung gestellt.
Im Fall einer transportgeschützten Karte haben Sie nur die Möglichkeit, durch „PIN entsperren“ die Transport-PIN durch eine selbst vergebene PIN zu ersetzen.

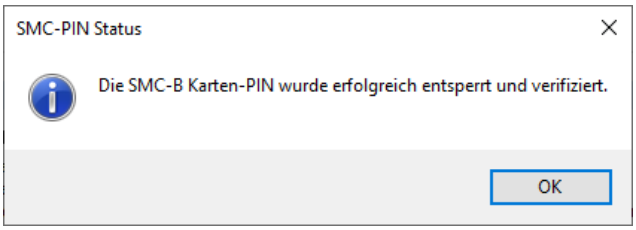


Es wird Ihnen ein Hinweis zum weiteren Ablauf angezeigt. Im Folgenden müssen Sie die Anzeige Ihres Kartenterminals beachten. Sie werden dazu aufgefordert zuerst die Transport-PIN einzugeben und danach eine neue PIN durch zweimalige Eingabe zu vergeben.

Bitte notieren Sie die neu vergebene PIN und verwahren Sie diese sicher.

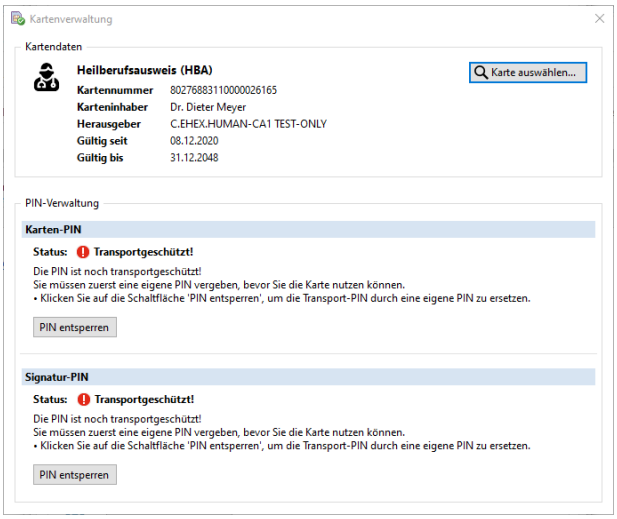


Danach werden Sie ggf. nochmals aufgefordert, Ihre PIN zur Freischaltung der Sicherheitsfunktionen der Karte am Kartenterminal einzugeben.



Sie erhalten eine Erfolgsmeldung, wenn die PIN erfolgreich geändert wurde.

Bei einem transportgeschützten HBA müssen Sie die Transport-PIN sowohl für die Karten-PIN als auch für die Signatur-PIN durch jeweils eine eigene PIN ersetzen.

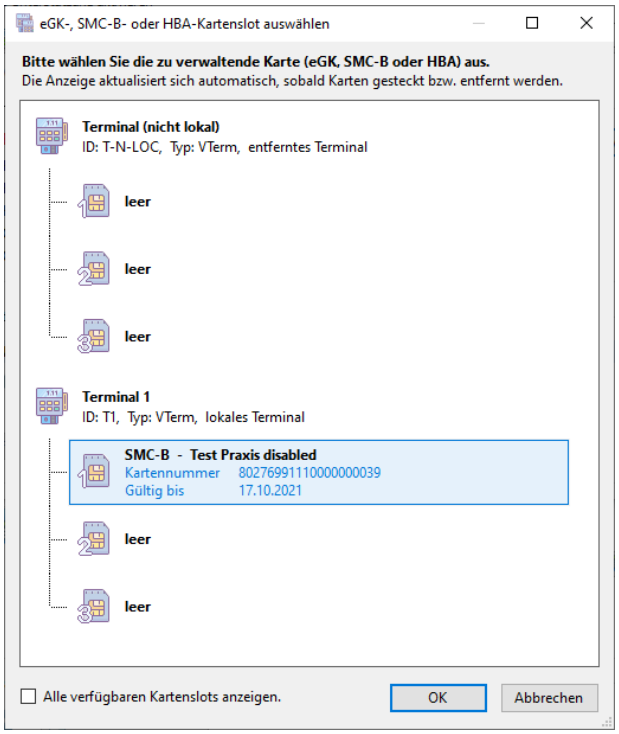


Der Kartenverwaltungsdialog sieht in diesem Fall so aus.

Wir empfehlen Ihnen aus Praktikabilitäts-gründen, die gleiche PIN für die Karte und die Signatur zu vergeben.

Bitte notieren Sie die neu vergebene PINs und verwahren Sie diese sicher.

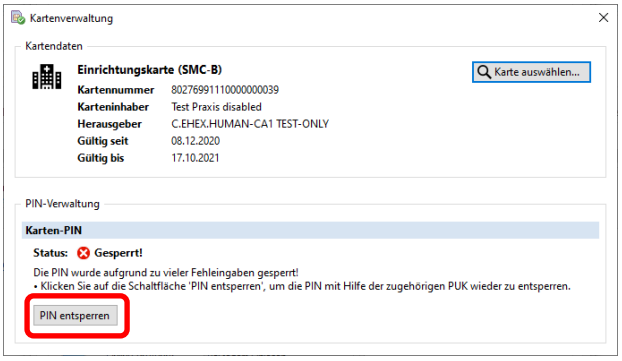
4.3 Entsperren einer gesperrten PIN mit Hilfe der PUK



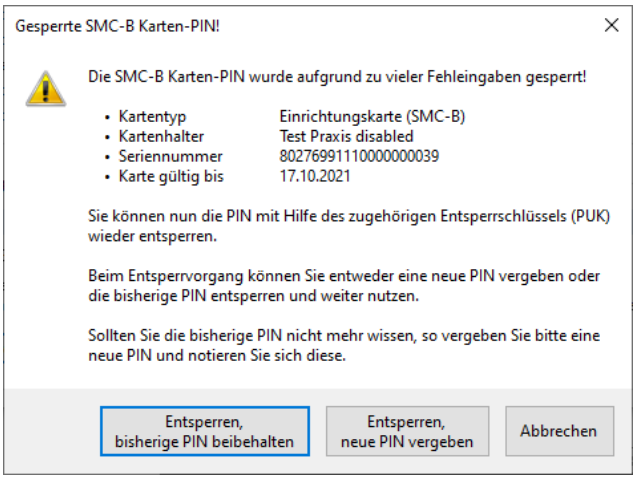
Falls Ihre Kryptokarte durch mehrmalige falsche PIN-Eingabe gesperrt sein sollte, so haben Sie die Möglichkeit die gesperrte PIN durch die Eingabe der PUK wieder freizuschalten.

Achtung: Die PUK können Sie nur 10 Mal für einen solchen Vorgang verwenden. Danach kann die Karte nicht mehr verwendet werden.

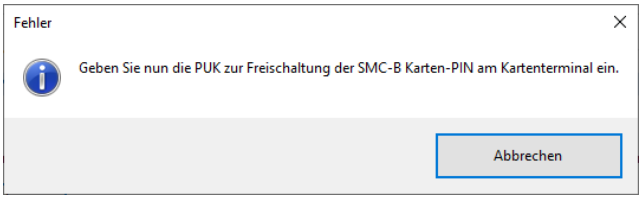
Öffnen Sie dazu bitte die Kartenverwaltung wie oben beschrieben und wählen Sie die Karte aus, deren PIN gesperrt ist.



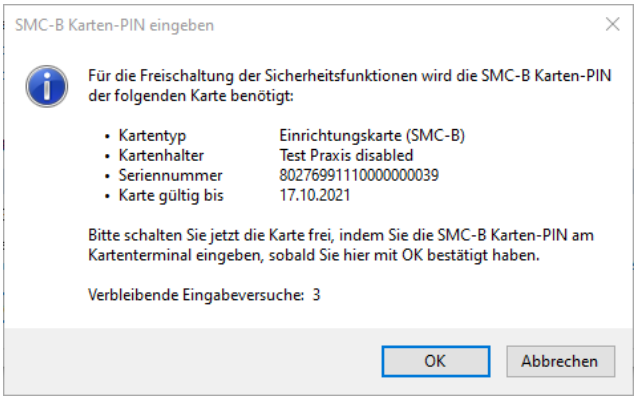
Es werden Ihnen im sich öffnenden Dialog im oberen Bereich die Informationen wie Kartennummer (ICCSN), Karteninhaber, Kartenherausgeber sowie Gültigkeitsdaten angezeigt. Im unteren Bereich werden Ihnen die PIN-Statusinformationen der Karte angezeigt und die vom PIN-Status abhängigen Funktionen zur Verfügung gestellt.
Klicken Sie hier auf „PIN entsperren“.



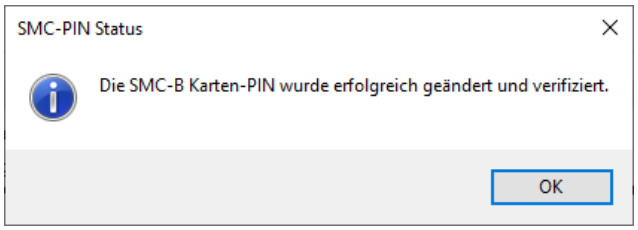
Es wird Ihnen ein Hinweis zum weiteren Ablauf angezeigt.
Sie haben hier zwei Optionen:
(1) die PIN unter Beibehaltung der bisherigen PIN zu entsperren
oder
(2) die PIN zu entsperren und dabei eine neue PIN zu vergeben.



Im Folgenden müssen Sie die Anzeige Ihres Kartenterminals beachten. Sie werden dazu aufgefordert zuerst die PUK einzugeben und danach entweder die bisherige PIN (1) **oder** eine neue PIN (2) durch zweimalige Eingabe zu vergeben.
Bitte notieren Sie die neu vergebene PIN und verwahren Sie diese sicher.



Danach werden Sie ggf. nochmals aufgefordert, Ihre PIN zur Freischaltung der Sicherheitsfunktionen der Karte am Kartenterminal einzugeben.



Sie erhalten eine Erfolgsmeldung, wenn die gesperrte PIN erfolgreich entsperrt und ggf. geändert wurde.