

Lokales KIM-Clientmodul Handbuch

Lokales KIM- Clientmodul Handbuch

support@rise-kim.de

Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
www.rise-world.com | support@rise-kim.de



Inhaltsverzeichnis

Inhaltsverzeichnis.....	I
1 Installation Vorbereitung.....	2
1.1 Firewall Freischaltung für KIM CM:.....	2
2 Einleitung.....	3
3 Produktbeschreibung KIM.....	3
3.1 Systemvoraussetzungen für KIM.....	4
3.2 Sicherheitshinweise.....	5
3.3 Lieferbestandteile des Produktes KIM.....	5
4 Inbetriebnahme KIM.....	5
5 Installation KIM Clientmodul.....	6
5.1 Basiseinstellungen.....	7
5.2 Erweiterte Konfiguration für Konnektor-Kommunikation.....	9
6 Konfiguration des E-Mail-Clients oder des Clientsystems.....	13
6.1 E-Mail Empfang.....	14
6.2 E-Mail Versand.....	14
6.3 Protokollierung.....	15
6.4 Ausnahme für Security-Tools.....	15
7 Account Manager.....	15
7.1 Registrieren am Account Manager.....	15
7.2 Login.....	16
7.3 Kartenauthentisierung.....	17
7.4 Stammdaten ändern.....	18
7.5 Abwesenheitsnotiz verwalten.....	18
7.6 Recovery E-Mailadresse ändern.....	18
7.7 Passwort ändern.....	19
7.8 Passwort zurücksetzen.....	19
7.9 Account entsperren.....	20
7.10 Logout.....	20
8 Anlagen und Verzeichnisse.....	21

Dokumentenhistorie

Version	Autor	Datum	Änderungsbeschreibung
1.1	RISE	01.02.2023	Initiale Version

Abkürzungen

Abkürzung	Erläuterung
CM	Clientmodul
DVO	Dienstleister vor Ort
KIM	Kommunikation im Medizinwesen
LE	Leistungserbringer (z.B. Ärzte
LEI	Leistungserbringerinstitutionen (wie Arztpraxen und Krankenhäuser)
TI	Telematikinfrastruktur
VM	Virtuelle Maschine

Zielgruppe des Dokuments

Administratoren bei Dienstleistern vor Ort (DVO) oder in Arzt Verbänden, in Krankenhäuser und Rechenzentren, die das KIM Clientmodul für Rechenzentren nutzen.

Ergänzend bietet RISE das Clientmodul als zentrales (Server-basiertes) KIM CM an, mit dem auch mehrere Konnektoren gleichzeitig angebunden werden können. Hierfür existiert eine eigene Installationsroutine.

Zielsetzung des Dokuments

Das Dokument erklärt Administratoren die Installation des lokalen RISE Clientmoduls (als Java Applikation) in der lokalen IT-Umgebung auf einem Stand Alone PC.

1 Installation Vorbereitung

Beim Betrieb auf einem Server: Debian (64bit).

1.1 Firewall Freischaltung für KIM CM:

1. Zwischen den eMail-Clients und der Clientmodul-VM: SMTP und POP auf jeden jeweiligen Ports
2. Zwischen der Clientmodul-VM und den Konnektoren: Port 80 und 443 zur Kommunikation
3. Zwischen der Clientmodul-VM und Zielen im Internet: Port 80 und 443 für OCSP und Package install

2 Einleitung

Dieses Dokument dient der Beschreibung des Produktes KIM. Insbesondere werden die einzelnen Funktionen dargestellt, der Installationsprozess des Clientmoduls sowie dessen Konfigurationsoptionen. Ebenso finden Sie hier Vorgaben und Hinweise für die Verwendung und den Betrieb des Produktes KIM und eine Beschreibung des Account Managers, der dem KIM Teilnehmer für die Administration seines Benutzeraccounts zur Verfügung steht.

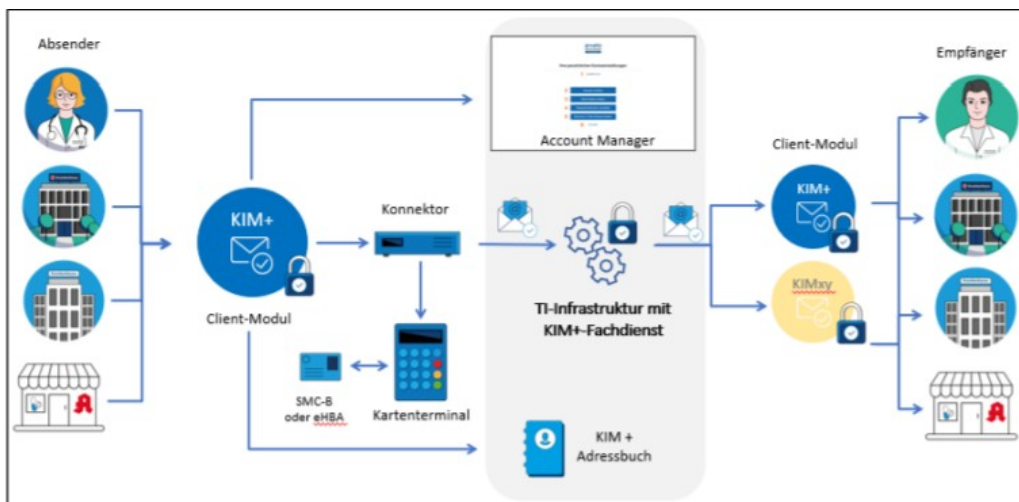
3 Produktbeschreibung KIM

Was ist KIM? KIM ermöglicht den sicheren Austausch von medizinischen Dokumenten über ein sicheres Übermittlungsverfahren. Das Produkt kann mit einem gültigen KIM-Benutzeraccount durch:

- Ärzte, Psychotherapeuten, Heilberufler und medizinisches Personal
- Krankenhäusern (Ärzten und Pflegepersonal) und
- KTR Basisconsumer, z.B. Sachbearbeiter in Krankenversicherungen verwendet werden.

Das Produkt KIM kann auch durch alternative Anbieter eingesetzt werden.

KIM besteht aus einem Clientmodul (CM), dem Account Manager für die Verwaltung von KIMBenutzerkonten (Accounts) und notwendige Schnittstellen zur TI-Infrastruktur. Zusätzlich bedarf es zur Nutzung des Produktes des Einsatzes von Konnektoren und Kartenlesegeräten (siehe Abschnitt 2.2)



Nachrichtenversand

E-Mails können über den lokalen Port (SMTP-Port) des KIM Clientmodul versendet werden. Diese Nachrichten werden über einen konfigurierten Konnektor beim Teilnehmer signiert, verschlüsselt und in

Form eines KIM-S/MIME Profils verpackt. Danach wird diese signierte, verschlüsselte und verpackte Nachricht an den eigentlichen Ziel-SMTP-Server weitergeleitet.

Nachrichtempfang

E-Mails können über den lokalen Port (POP3-Port) des KIM Clientmodul empfangen werden. Diese Nachrichten werden überprüft, ob sie einem KIM-S/MIME Profil entsprechen. Entsprechende Nachrichten werden entpackt, entschlüsselt und ihre enthaltene Signatur wird einer Prüfung am Konnektor des Benutzers unterzogen. Falls die Nachricht nicht entschlüsselt werden kann, wird ein entsprechender Vermerk der Nachricht hinzugefügt. Das Ergebnis der Prüfung wird in Form eines vereinfachten

Prüfberichts im textuellen Teil der ursprünglichen E-Mail angehängt. Danach werden alle Nachrichten an der Mail Client weitergeleitet. Nachrichten, die nicht einem KIM-S/MIME Profil entsprechen, werden nicht verarbeitet (gemäß Gematik Anforderung KOM-LE-A_2042).

Verwaltung des Benutzeraccounts über den Account Manager

Der Account Manager bietet dem Anwender diverse Funktionen (siehe Abschnitt 7) für die Verwaltung des KIM Benutzeraccounts für den Leistungserbringer und -Institutionen an. Er kann dort unter anderem sein Passwort ändern oder zurücksetzen lassen. Er kann seinen Account im Bedarfsfall entsperren

lassen oder auch seine Stammdaten anpassen. Um diese Funktionen nutzen zu können, muss sich der Anwender am Account Manager registrieren (siehe Abschnitt 7.1) und kann sich dann bei Bedarf mit seinen Zugriffsdaten anmelden (siehe Abschnitt 7.2).

3.1 Systemvoraussetzungen für KIM

Der Leistungserbringer (LE) / die Leistungserbringer -Institution (LEI) muss sowohl in physischer, als auch logischer Hinsicht, eine sichere Betriebsumgebung bereitstellen.

Funktionale Anforderungen an die Betriebsumgebung

Das KIM besitzt einige funktionelle Anforderungen, welche der LE / die LEI durch Komponenten oder das lokale Netzwerk bereitstellen muss, um einen vollständigen und ordnungsgemäßen Betrieb ermöglichen zu können:

- Bereitstellung eines zertifizierten Konnektors nach BSI-DSZ-CC-1052.1
- Bereitstellung von Kartenterminals und Chipkarten gem. Bedienungsanleitung des vom Benutzer eingesetzten Konnektors.

Außerdem werden für eine korrekte Nutzung des KIM bestimmte Systemkonfigurationen vorausgesetzt:

- Betriebssystem: Windows (ab Version 7), MacOS oder Linux
- Aktueller Browser Edge, Firefox oder Chrome.
- Installationsrechte
- Java Runtime Environment (JRE) ab Version 11 inklusive JavaFX (wird mit dem Clientmodul ausgeliefert)
- Mail Client Software wie Thunderbird oder Outlook (in aktueller Version)
- Unter Linux muss die Library libappindicator für GTK2 am System installiert sein (unter Ubuntu 18.04 ist es das Package libappindicator1, unter Arch Linux ist es das Package libappindicator-gtk2)
- Internetverbindung

Anforderungen an die Netzwerk- und Konnektor-Konfiguration

Wenn der Konnektor im Parallel-Modus betrieben wird, dann ist in der Regel der Konnektor nicht der Default-Gateway des Clientsystems (auf dem das Clientmodul läuft). Damit der Traffic in die TI trotzdem

zum Konnektor findet, müssen zusätzliche Netzwerk-Konfigurationen vorgenommen werden.

- Routen in die TI müssen zum Konnektor zeigen für den direkten POP3/SMTP und DNS Traffic.
- Der Konnektor muss auch als DNS-Resolver für die Telematik-Domäne verwendet werden.

Dies wird für die Auflösung des „KIM“-SMTP bzw. POP3-Servers benötigt.

- Alle Konnektoren, über die das Clientmodul kommuniziert, müssen die gleiche Firmware Version haben. Ansonsten kann es zu Kommunikationsproblemen kommen, da unterschiedliche Konnektorversionen unterschiedliche Sicherheitsstandards unterstützen.

3.2 Sicherheitshinweise

Schutz des LE- / LEI-Netzwerkes vor Angriffen

Für den optimalen Betrieb des Produktes KIM muss der Leistungserbringer bzw. die Institution die Sicherheit der Betriebsumgebung gewährleisten und einhalten. D.h. der LE/die LEI 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 aktuellen Stand sein (regelmäßige Updates), um sie gegen Schadsoftware zu schützen und infolgedessen das lokale Netzwerk.

Sichere Administration des KIM

Der Dienstleister bzw. interne IT-Verantwortliche eines Leistungserbringers oder einer entsprechenden Institution für den Betrieb des KIM Produktes muss dafür sorgen, dass administrative Tätigkeiten der lokalen und zentralen Administration in Übereinstimmung mit der Administrator-Dokumentation des Produktes durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdigen, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen geheim halten bzw. dürfen diese nicht an Unberechtigte weitergeben.

Schutz des Zielsystems, auf dem das KIM installiert wird

Das KIM verarbeitet sensitive Informationen temporär im Arbeitsspeicher. Des Weiteren speichert das KIM Clientmodul Zertifikate und Zugangsdaten für die verschlüsselte Kommunikation in einem passwortgeschützten 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. Das KIM Clientmodul schreibt (falls aktiviert) Protokolldateien, die eine Analyse der technischen Vorgänge erlauben. Der Benutzer muss durch geeignete Maßnahmen sicherstellen, dass diese Protokolldateien nur für autorisierte Personen zugänglich sind.

3.3 Lieferbestandteile des Produktes KIM

KIM Installations- & Anwenderhandbuch (dieses Dokument)

kimplus-clientmodul_1_4_5_0_PU_windows-x64.exe (Kim-Clientmodul)

clientmodul-installer-1.6.3-CMI-rise.kim.telematik-win64.exe (Installer für die Teilnehmer Registrierungen)

4 Inbetriebnahme KIM

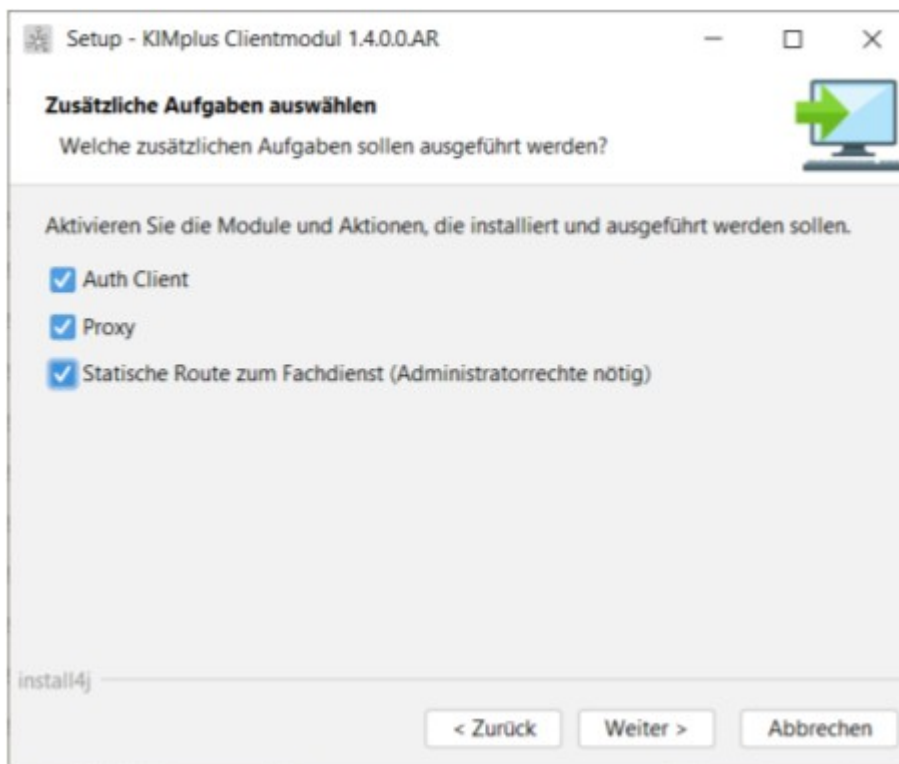
Um die E-Mail Funktionen eines KIM E-Mail Konto nutzen zu können, sind folgende Schritte zu tätigen:

1. Installieren und Einrichten von KIM-Clientmodul
2. Installation von rise-kim-installer und Registrationen von KIM-E-Mails
3. Anbindung E-Mail Client oder KIS System

5 Installation KIM Clientmodul

Für die Installation des KIM Clientmoduls werden Installationspakete je Betriebsumgebung zur Verfügung gestellt. Die jeweils aktuelle Version des KIM Clientmoduls wird per FileDrop bereitgestellt. Das KIM Clientmodul wird über die folgenden Schritte installiert (mit Benutzerinteraktion):

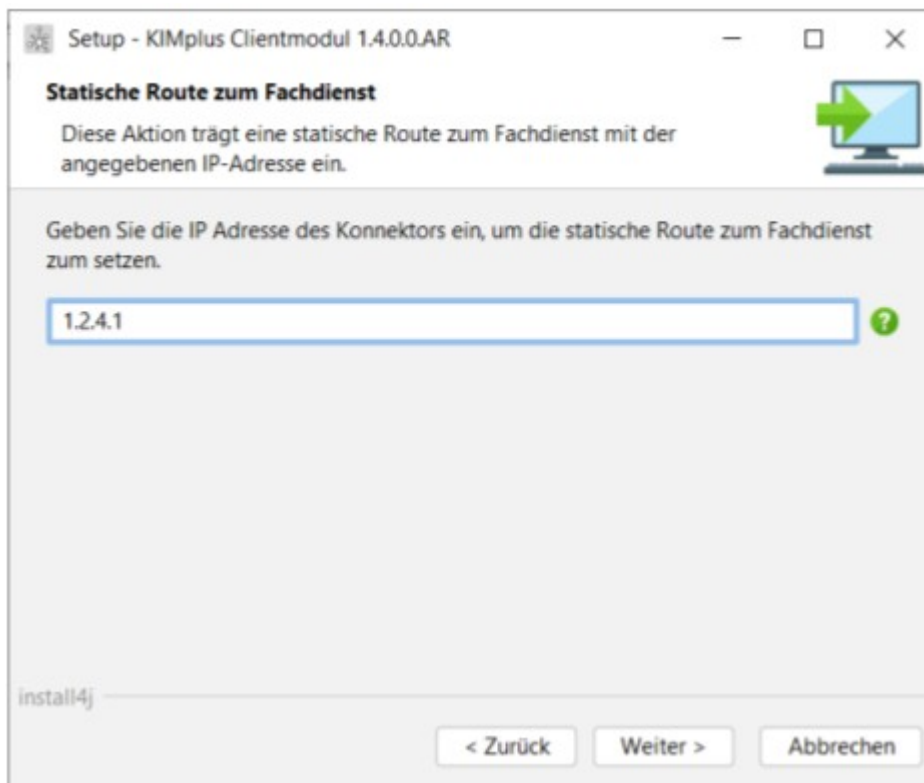
1. Vor der Installation des KIM Clientmoduls müssen alle Systemanforderungen überprüft und die Betriebsumgebung entsprechend vorbereitet werden.
2. Herunterladen des Installationspakets für das vorgesehene Betriebssystem (Windows, MacOS, Linux).
3. Ausführung des Installationspakets, um den Installationsvorgang zu starten.
4. Die Installation des Clientmoduls bietet über die Benutzeroberfläche die Option der separaten Aktivierung/Deaktivierung des Auth Clients, Proxys und das Setzen der statischen Route zum KIM Fachdienst an. Anhand der getätigten Benutzerinteraktion werden die entsprechenden Werte in der Konfigurationsdatei des Clientmoduls eingetragen und damit der Auth Client und/oder Proxy im Clientmodul aktiviert/deaktiviert.



Im Standard sind alle Auswahlfelder aktiviert.

Bei gewählter Option, die netzwerkseitige Erreichbarkeit des KIM Fachdienstes über einen Konnektor sicherzustellen, muss in einem folgenden Schritt die IP-Adresse des Konnektors angegeben werden. Das Setzen der Netzwerk Route erfordert Administrator-Rechte während des Installationsvorgangs und ist nur unter Windows verfügbar. Die Konfiguration einer Route muss gewöhnlich nur während der

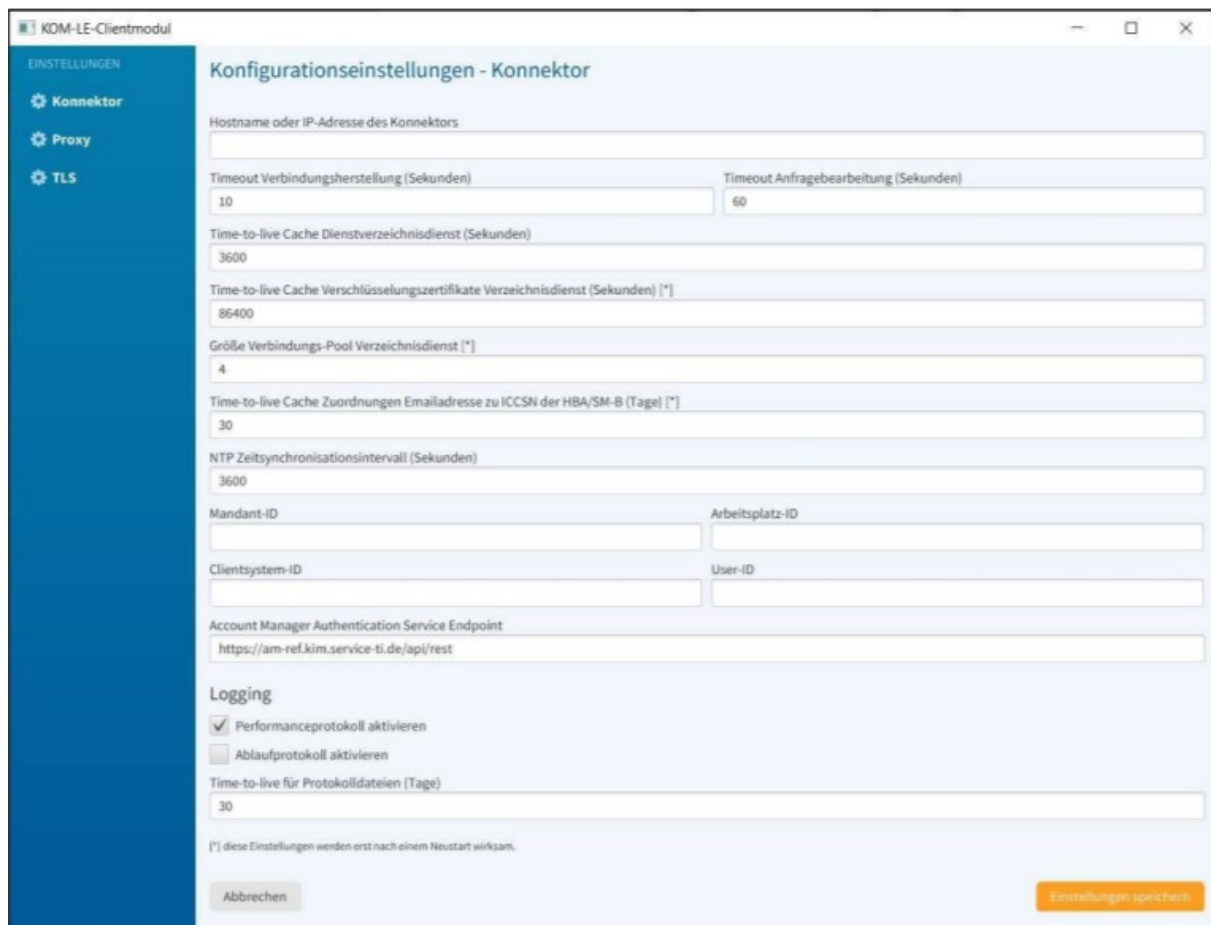
Erstinstallation des Clientmoduls gesetzt werden, da sie dann dauerhaft im System verankert wird. Bei der Aktualisierung eines bereits installierten Clientmoduls muss diese Option nicht aktiviert werden.



5.1 Basiseinstellungen

Bei der ersten Inbetriebnahme des KIM Clientmoduls müssen grundlegende Einstellungen in der grafischen Benutzeroberfläche vorgenommen werden, bevor es verwendet werden kann.

1. Starten des KIM Clientmoduls
2. Unter den Einstellungen für den "Konnektor" müssen folgende Konfigurationen vorgenommen werden:
 - Hostname oder IP-Adresse des Konnektors, der für die NTP-Synchronisation und die Zertifikatsüberprüfung beim Verbindungsaufbau zum Fachdienst benutzt wird
 - Karten-Kontext für die Zertifikatsüberprüfung und für den Auth Client, bestehend aus
 - Mandant-ID des Kontexts für den Konnektor (nur für die Zertifikatsüberprüfung)
 - Arbeitsplatz-ID des Kontexts für den Konnektor (für Zertifikatsüberprüfung und Auth Client)
 - Clientsystem-ID des Kontexts für den Konnektor (für Zertifikatsüberprüfung und Auth Client)
 - User-ID des Kontexts für den Konnektor (nur für HBA) (falls vorhanden für Zertifikatsüberprüfung und Auth Client)
 - Der Wert für „Account Manager Authentication Endpoint“ muss <https://am-ref.kim.service-ti.de/api/rest> sein



The screenshot shows the 'Konfigurationseinstellungen - Konnektor' window in the KIM-LE-Clientmodul. The left sidebar contains 'EINSTELLUNGEN' with sub-items 'Konnektor', 'Proxy', and 'TLS'. The main area is titled 'Konfigurationseinstellungen - Konnektor' and contains the following fields and sections:

- Hostname oder IP-Adresse des Konnektors: [Empty text box]
- Timeout Verbindungsherstellung (Sekunden): 10
- Timeout Anfragebearbeitung (Sekunden): 60
- Time-to-live Cache Dienstverzeichnisdienst (Sekunden): 3600
- Time-to-live Cache Verschlüsselungszertifikate Verzeichnisdienst (Sekunden) [*]: 86400
- Größe Verbindungs-Pool Verzeichnisdienst [*]: 4
- Time-to-live Cache Zuordnungen Emailadresse zu ICCSN der HBA/SM-B (Tage) [*]: 30
- NTP Zeitsynchronisationsintervall (Sekunden): 3600
- Mandant-ID: [Empty text box]
- Arbeitsplatz-ID: [Empty text box]
- Clientsystem-ID: [Empty text box]
- User-ID: [Empty text box]
- Account Manager Authentication Service Endpoint: <https://am-ref.kim.service-ti.de/api/rest>
- Logging section:
 - Performanceprotokoll aktivieren
 - Ablaufprotokoll aktivieren
 - Time-to-live für Protokolldateien (Tage): 30

[*] diese Einstellungen werden erst nach einem Neustart wirksam.

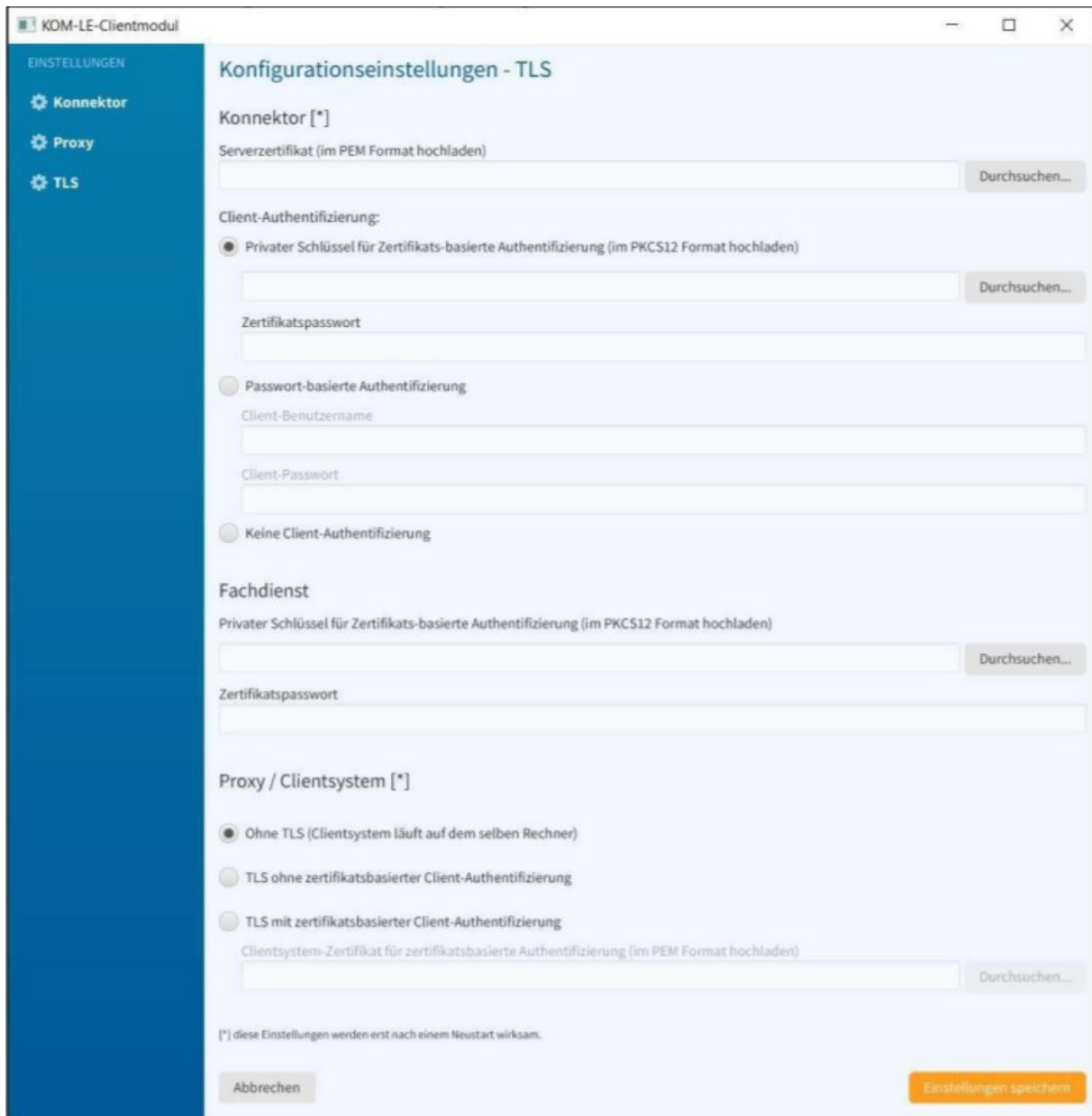
Buttons: 'Abbrechen' (grey) and 'Einstellungen speichern' (orange).

3. Unter den Einstellungen für "TLS" (Abbildung 12 Konfigurationseinstellungen - TLS) müssen folgende Konfigurationen vorgenommen werden:

- Auswählen einer lokal verfügbaren PEM Datei mit dem Server-Zertifikat des Konnektors.
- Auswählen der zu verwendenden Art der Client-Authentifizierung zum Konnektor: Zertifikats-basierte Authentifizierung, Passwort-basierte Authentifizierung oder keine Client-Authentifizierung.
 - Bei ausgewählter Zertifikats-basierter Authentifizierung zum Konnektor: Auswählen einer lokal verfügbaren passwortgeschützten PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel sowie Eingabe des Passworts.
 - Bei ausgewählter, Passwort-basierter Authentifizierung: Eingabe von Benutzername und Passwort.
- Auswählen einer lokal verfügbaren passwortgeschützten PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel für die zertifikatsbasierte Client-Authentifizierung zum Fachdienst sowie Eingabe des Passworts.
- Auswählen der zu verwendenden Art der Client-Authentifizierung vom Clientsystem:
 - ohne TLS, TLS mit zertifikatsbasierter Client-Authentifizierung oder TLS ohne Zertifikats-basierter Client-Authentifizierung.
 - Die Option "ohne TLS" darf entsprechend den Vorgaben der Gematik nur genutzt werden, wenn das Clientsystem und das KIM Clientmodul auf demselben Rechner laufen.
 - Bei ausgewählter zertifikatsbasierter Client-Authentifizierung vom Clientsystem: Auswählen einer lokal verfügbaren PEM Datei mit dem Client-Zertifikat des Clientsystems.

Hinweis: bei ausgewählter TLS Client-Authentifizierung muss im verwendeten

Client mindestens TLS 1.2 eingestellt werden.



The screenshot shows the 'KOM-LE-Clientmodul' configuration window, specifically the 'Konfigurationseinstellungen - TLS' tab. The window has a blue sidebar with 'EINSTELLUNGEN' and three options: 'Konnektor', 'Proxy', and 'TLS'. The main content area is titled 'Konfigurationseinstellungen - TLS' and contains the following sections:

- Konnektor [*]**: A text input field for 'Serverzertifikat (im PEM Format hochladen)' with a 'Durchsuchen...' button.
- Client-Authentifizierung:** Three radio button options:
 - Privater Schlüssel für Zertifikats-basierte Authentifizierung (im PKCS12 Format hochladen): Includes a 'Durchsuchen...' button and a 'Zertifikatspassword' field.
 - Passwort-basierte Authentifizierung: Includes 'Client-Benutzername' and 'Client-Passwort' fields.
 - Keine Client-Authentifizierung
- Fachdienst**: Includes a 'Privater Schlüssel für Zertifikats-basierte Authentifizierung (im PKCS12 Format hochladen)' field with a 'Durchsuchen...' button and a 'Zertifikatspassword' field.
- Proxy / Clientsystem [*]**: Three radio button options:
 - Ohne TLS (Clientsystem läuft auf dem selben Rechner)
 - TLS ohne zertifikatsbasierter Client-Authentifizierung
 - TLS mit zertifikatsbasierter Client-Authentifizierung: Includes a 'Clientsystem-Zertifikat für zertifikatsbasierte Authentifizierung (im PEM Format hochladen)' field with a 'Durchsuchen...' button.

At the bottom, there is a note: '[*] diese Einstellungen werden erst nach einem Neustart wirksam.' and two buttons: 'Abbrechen' and 'Einstellungen speichern'.

4. Nachdem alle Änderungen an der Konfiguration vorgenommen wurden, die Einstellungen speichern.

5. Neustart des KIM Clientmoduls, da die Konfigurationsänderungen erst danach wirksam werden.

5.2 Erweiterte Konfiguration für Konnektor-Kommunikation

Für die Kommunikation zwischen Clientmodul und Konnektor müssen folgende Einstellungen durchgeführt werden:

Statische Route eintragen:

Damit die Kommunikation des Clientmoduls über den Konnektor und nicht über das Internet erfolgt, muss eine statische Route auf dem System des Anwenders gesetzt werden. Im Rahmen der Installati-

on unter Windows erfolgt dies bei aktivierter Option bereits während der Installation automatisch und muss nicht manuell erfolgen.

Statische Routen in Windows eintragen:

Kommandozeile als Administrator öffnen und den Befehl

`route -p add 100.102.0.0 MASK 255.254.0.0 <IP des Konnektors> METRIC 1` eingeben.

Statische Routen in Mac eintragen:

Im Terminal den Befehl

`sudo route add -net 100.102.0.0 -netmask 255.254.0.0 <IP des Konnektors>` eingeben.

Hinweis: Die Route wird nicht dauerhaft gesetzt und muss bei jedem Neustart eingetragen werden.

Für eine permanente Lösung muss eine scriptbasierte Lösung genutzt werden.

Statische Routen in Linux eintragen:

Im Terminal den Befehl

`sudo ip route add 100.102.0.0/15 via <IP des Konnektors>` eingeben.

Hinweis: Die Route wird nicht dauerhaft gesetzt und muss bei jedem Neustart eingetragen werden.

Für eine permanente Lösung muss eine scriptbasierte Lösung genutzt werden.

Bezug Zertifikatsschlüssel für Clientmodul:

Im Rahmen der Inbetriebnahme eines KIM eMail Kontos ist es notwendig, das Clientmodul mit der Telematik Infrastruktur über einen verschlüsselten Kanal zu verbinden. Dazu werden Sicherheitszertifikate eingesetzt, die eine verschlüsselte Verbindung ermöglichen.

Das Clientmodul muss dafür entsprechend konfiguriert werden, indem ein Schlüssel eingebracht wird.

Um den Zertifikatsschlüssel zu beziehen, muss zunächst das Clientmodul installiert und vorkonfiguriert, sowie die Registrierung der KIM Adresse durch den Installer abgeschlossen werden. Der Schlüssel kann anschließend von Teilnehmern wie folgt bezogen werden:

1. Über den Link folgender Website der Teilnehmeranwendung:

<https://ssp.kim.service-ti.de/zertifikat>

2. Teilnehmer sollten die nötigen Informationen im Anmeldedialog angeben:

- KIM E-Mail
- KIM ContractID (per Mail)
- Zertifikatsnummer (per Mail)
- KIM Passwort

LOGIN - SICHERHEITZERTIFIKAT

Bitte geben Sie Ihre Daten ein, um fortzufahren.

Contract-ID *

Zertifikatsnummer *

KIM E-Mail *

Passwort *

WEITER

3. Laden Sie den hinterlegten Schlüssel mit der angegebenen Zertifikats-Nr. herunter.

KIM SERVICE PORTAL - SICHERHEITZERTIFIKAT

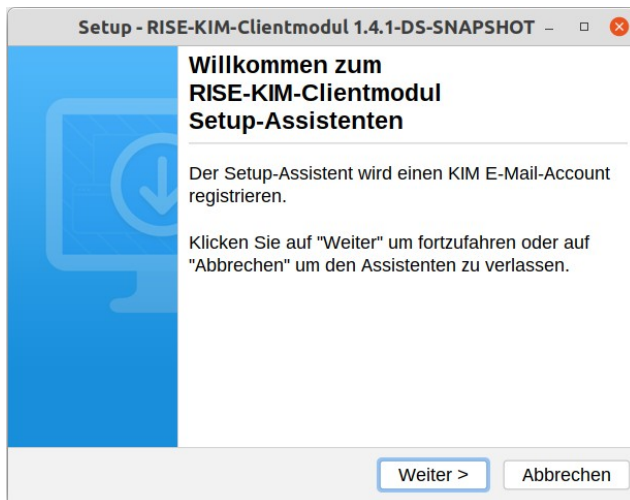
Hier erhalten Sie eine Übersicht Ihrer Zertifikate. Bitte bewahren Sie Ihre Zertifikate sorgfältig auf!

ZERTIFIKATE

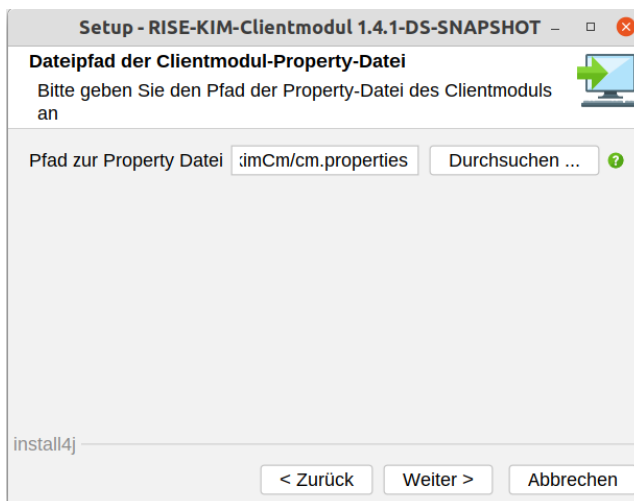
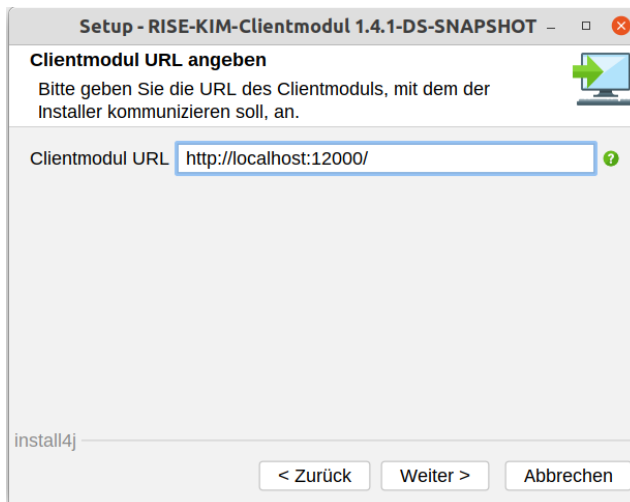
Zertifikat	Größe	Datum	Status	Download
169	1506	16.12.2020 16:40 Uhr	 heruntergeladen	 Erneut herunterladen

Installer Installieren

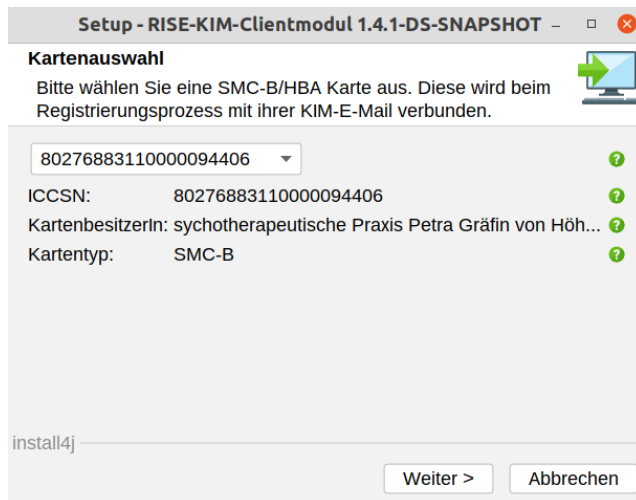
1. Bereitstellung des Installers erfolgt über FileDrop
2. Herunterladen des Installationspakets für das vorgesehene Betriebssystem (Windows, MacOS, Linux).
3. Ausführung des Installationspakets, um den Installationsvorgang zu starten.



4. Default Einstellungen so belassen und bis Kartenauswahl auf weiter klicken.



5. SMC-B oder HBA auswählen und auf weiter klicken

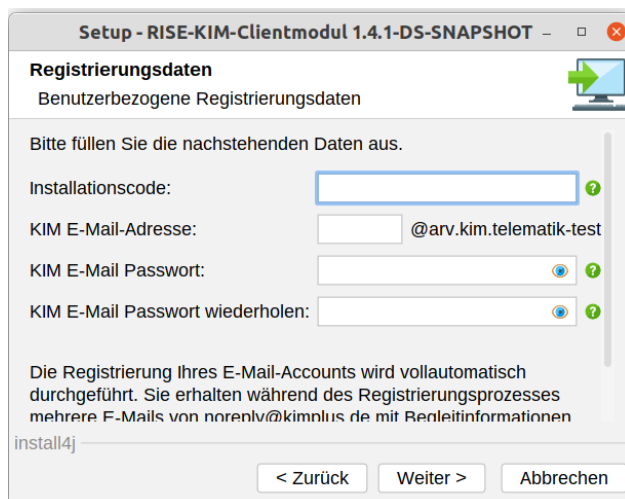


6. Konto & Teilnehmer Registrieren

6.1. Installationscode erhalten Sie in einem separaten E-Mail

6.2. Gewünschte E-Mail-Adresse eingeben

6.3. KIM E-Mail Passwort eingeben und die Registrierung abschließen.



6 Konfiguration des E-Mail-Clients oder des Client-systems

Um E-Mails über das KIM Clientmodul korrekt versenden und empfangen zu können, müssen die Zugangsdaten im E-Mail-Client (wie bspw. Thunderbird oder Outlook) oder dem Clientsystem angepasst werden. Eine Beschreibung der benötigten Einstellungen ist im jeweiligen Unterkapitel angegeben.

6.1 E-Mail Empfang

Einstellung	Wert
Servertyp	POP
Server	localhost (bzw. Adresse des Rechners auf dem das Clientmodul in Ihrer Umgebung installiert ist)
Port	Einstellung wie im Clientmodul (POP3 Port)
Benutzername	Siehe Abbildung 16 Aufbau POP3 Benutzername Beispiel: erik.mustermann@mail.kim.telema- tik#100.102.8.6:995#Mandant1#ClientID1#Work- place1#UserID1
Authentifizierung	Passwort, normal
Verbindungssicherheit	keine

6.2 E-Mail Versand

Einstellung	Wert
Servertyp	SMTP
Server	localhost
Port	Einstellung wie in Clientmodul (SMTP Port)
Benutzername	Siehe Abbildung 17 Aufbau SMTP Benutzername Beispiel: erik.mustermann@mail.kim.telema- tik#100.102.8.6:465#Mandant1#ClientID1#Work- place1
Authentifizierung	Passwort, normal
Verbindungssicherheit	Keine
Timeout	Anpassung des Standardwertes für timeouts unter Menü > Einstellungen > Allgemein > Konfiguration bearbeiten (ganz unten auf der Seite), wenn es zu timeouts beim Versand großer Mails kommt. Parameter: mailnews.tcptimeout Standardwert: 100 Sek. Erhöhung z.B. auf 300 Sek. testen

6.3 Protokollierung

Das KIM Clientmodul schreibt Protokolldateien, die ein Nachvollziehen der internen Abläufe ermöglichen. Es gibt ein Ablauf- und ein Performance-Protokoll, wobei beide unabhängig voneinander ein- und

ausgeschaltet werden können (siehe Abschnitt 5.3.2 Konfigurationseinstellungen Konnektor).

Die Protokolle liegen im Unterordner log des Applikationsverzeichnis des Clientmoduls kimCM im Home-Verzeichnis des Benutzers. Unter Windows ist das Verzeichnis unter C:\Users\\kimCM bzw. unter MacOS und Linux unter /home/<Username>/kimCM zu finden.

Um den Speicherplatzverbrauch der Protokoll-Dateien zu begrenzen, werden pro Tag pro Protokolltyp maximal 10 Dateien mit 100 MB Größe geschrieben. Sollten mehr als 1000 MB an Protokollen anfallen, so wird die älteste Protokolldatei überschrieben. Zusätzlich werden die Protokolldateien nach einer konfigurierbaren Anzahl von Tagen automatisch gelöscht.

6.4 Ausnahme für Security-Tools

Bei der Nutzung des KIM Dienstes kann es zu Problemen mit Security-Tools kommen (Virenschannern etc.). Vor allem, wenn das Zertifikat in irgendeiner Weise verändert wird, kommt die Fehlermeldung "[javax.net.ssl.SSLException: org.bouncycastle.tls.TlsFatalAlert: certificate_unknown\(46\)](#)". Hierzu müssen bestimmte Ausnahmen für folgende Namen in SecurityTools eingestellt werden:

[am.kimplus.de](#)

am.arv.kim.telematik

[am.kim.service-ti.de](#)

Die Serverzertifikate müssen validiert werden. Dazu ist es notwendig, dass folgende Zugriffe nicht durch eine Firewall blockiert werden:

[ocsp.digicert.com](#)

[status.geotrust.com](#)

7 Account Manager

In den nachfolgenden Abschnitten werden die verfügbaren Funktionen des Account Managers im Detail beschrieben.

Der Account Manager ist über die Internet-Adresse

<https://am.kimplus.de>

erreichbar.

7.1 Registrieren am Account Manager

Vorbedingung: Der Anbieter des KIM Produktes hat einen Antrag für die Anmeldung des Anwenders / Leistungserbringers bei der verantwortlichen Stelle. Der Anwender hat Zugriff auf das Postfach der zu hinterlegenden Recovery E-Mail-Adresse.

Der Account Manager sendet einen Registrierungslink an die angegebene Recovery E-Mail-Adresse,

der den Anwender zu einer Eingabemaske zum Setzen des Passworts (Abbildung 22 Account Manager

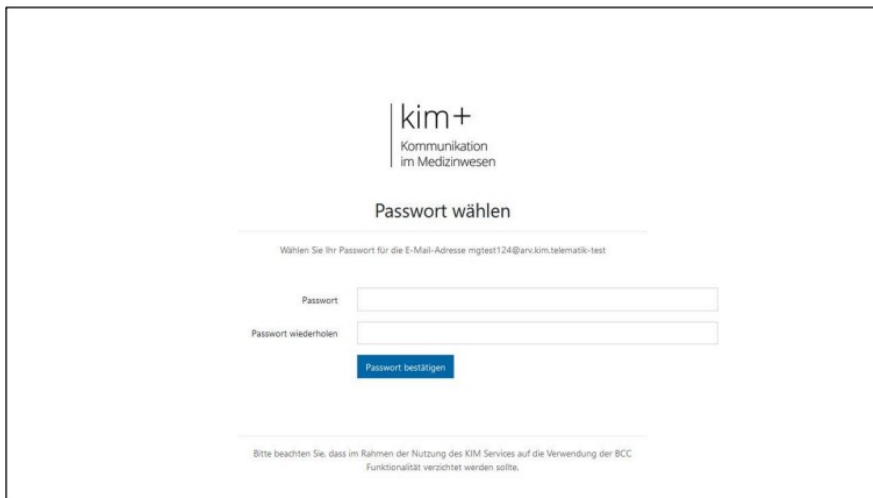
- Passwort setzen) führt.

Für Passwörter gelten aus Sicherheitsgründen folgende Kriterien:

- Es muss jährlich erneuert werden
- Es muss mindestens einen Kleinbuchstaben a-z enthalten
- Es muss mindestens einen Großbuchstaben A-Z enthalten
- Es muss mindestens ein Sonderzeichen/Umlaut enthalten
- Es muss mindestens eine Ziffer 0-9 enthalten
- Zumindest 50 % der Zeichen müssen sich unterscheiden

Nach Abschluss des Vorgangs zum Setzen des Passworts erfolgt eine Weiterleitung auf die Login Seite des Account Managers (Abbildung 23 Account Manager - Login). Der Anwender kann sich nun mit dem neu gesetzten Passwort einloggen.

Anmerkung: Nach dem Abschluss des Registrierungsvorgangs wird eine Benachrichtigung an die Recovery E-Mail-Adresse gesendet.



7.2 Login

Vorbedingung: Der Anwender verfügt über eine gültige KIM-E-Mailadresse und kennt das zugehörige Passwort.

Der Login erfolgt über eine Eingabemaske auf der Startseite der Anwendung (Abbildung 23 Account Manager-Login, Markierung 1), in welche die gültigen Logindaten einzugeben sind. Nach Bestätigung der Eingabe durch einen Klick auf den Button "Login" wird der Anwender - sofern die Eingabe korrekt war - auf die Menüseite weitergeleitet. Auf der Menüseite wird die KIM-E-Mailadresse des eingeloggenen

Anwenders dargestellt (Abbildung 24 Account Manager - Menü, Markierung 1).

Anmerkung: Nach dreimaligem Versuch, sich mit einem ungültigen oder fehlerhaften Passwort einzuloggen, wird der Account der angegebenen KIM-E-Mailadresse gesperrt. Der Account kann erst nach einer Entsperrung wiederverwendet werden.

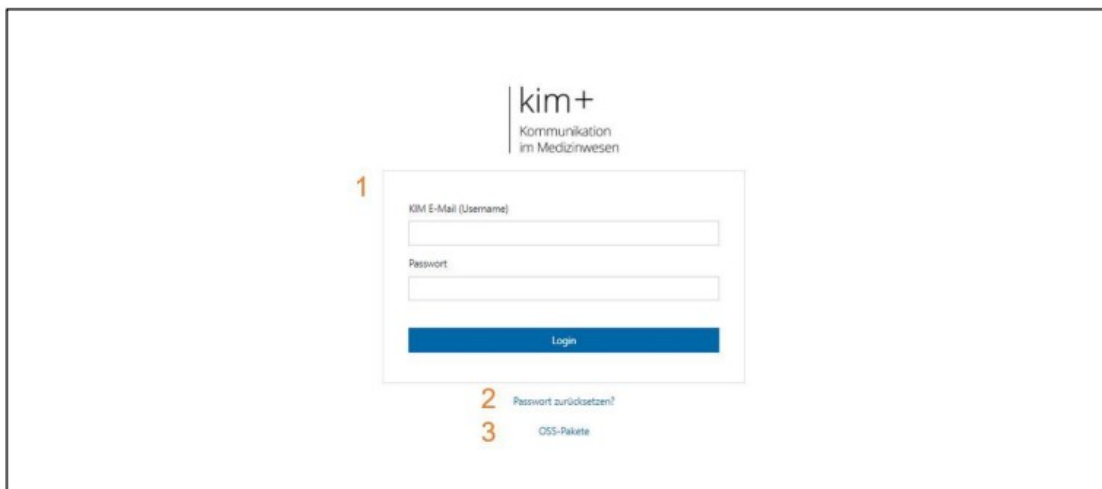


Abbildung 23 Account Manager-Login



Abbildung 24 Account Manager - Menü

7.3 Kartenauthentisierung

Bei einigen Anwendungsfällen ist eine zusätzliche Authentisierung via Kartenterminal notwendig. In diesem Fall erscheint in der Anwendung des Account Managers ein Fenster (Abbildung 25 Account Manager - Kartenaauthentisierung),

das nach Abschluss des Authentisierungsvorgangs automatisch wieder schließt.

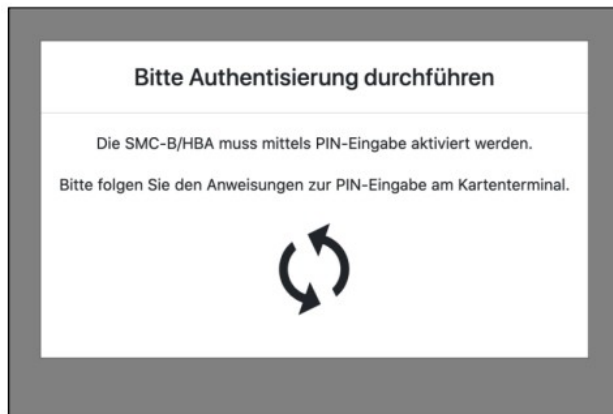


Abbildung 25 Account Manager - Kartenauthentisierung

7.4 Stammdaten ändern

Vorbedingung: Der Anwender ist eingeloggt, befindet sich auf der Menüseite und ist in der Lage, sich über das Kartenterminal zu authentisieren.

Das Formular zum Ändern der Stammdaten kann - analog zum Anwendungsfall "Passwort ändern" - durch einen Klick auf den Button "Stammdaten ändern" (Abbildung 24 Account Manager-Menü, Markierung 3) aufgerufen werden.

7.5 Abwesenheitsnotiz verwalten

Vorbedingung: Der Anwender ist eingeloggt, befindet sich auf der Menüseite und ist in der Lage, sich über das Kartenterminal zu authentisieren.

Das Formular zum Verwalten der Abwesenheitsnotiz kann - analog zu den Anwendungsfällen "Passwort ändern" und "Stammdaten ändern" - durch einen Klick auf den Button "Abwesenheitsnotiz verwalten" (Abbildung 24 Account Manager-Menü, Markierung 4) aufgerufen werden.

Bei aktivierter Abwesenheitsnotiz wird diese einmal pro Tag an die Absender geschickt.

7.6 Recovery E-Mailadresse ändern

Vorbedingung: Der Anwender ist eingeloggt, befindet sich auf der Menüseite, ist in der Lage, sich über das Kartenterminal zu authentisieren, und hat Zugriff auf das Postfach der neuen Recovery EMail-adresse.

Das Formular zum Ändern der Recovery E-Mailadresse kann - analog zu den obigen Anwendungsfällen - durch einen Klick auf den Button "Recovery E-Mail-Adresse ändern" (Abbildung 24 Account Manager-Menü, Markierung 5) aufgerufen werden. An die neue Recovery E-Mailadresse wird automatisch

eine E-Mail mit einem Bestätigungslink versendet. Die Änderung wird erst nach dem Klick auf den Bestätigungslink übernommen!

Anmerkung: An die alte Recovery E-Mailadresse wird eine Benachrichtigung über die bevorstehende Änderung verschickt.

7.7 Passwort ändern

Vorbedingung: Der Anwender ist eingeloggt, befindet sich auf der Menüseite und ist in der Lage, sich über das Kartenterminal zu authentisieren.

Das Formular zum Ändern des KIM Passworts (Abbildung 26 Account Manager - Passwort ändern) kann durch einen Klick auf den Button "Passwort ändern" (Abbildung 24 Account Manager - Menü, Markierung 2) aufgerufen werden. Der Vorgang kann durch einen Klick auf den Button "Abbrechen" abgebrochen werden.

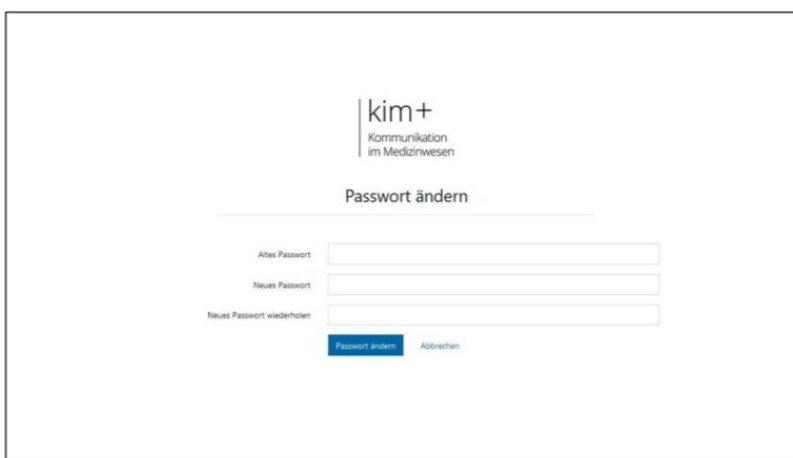


Abbildung 26 Account Manager - Passwort ändern

7.8 Passwort zurücksetzen

Vorbedingung: Der Anwender verfügt über eine gültige KIM-E-Mailadresse und hat Zugriff auf das Postfach der Recovery E-Mailadresse, die für die KIM-E-Mailadresse hinterlegt ist.

Der Vorgang zur Zurücksetzung eines Passworts kann durch einen Klick auf den Button "Passwort vergessen?" (Abbildung 23 Account Manager-Login, Markierung 2) gestartet werden. Nach dem Klick erfolgt eine Weiterleitung auf eine Eingabemaske, in welche die KIM-E-Mailadresse und die hinterlegte

Recovery E-Mailadresse einzugeben sind (Abbildung 27 Account Manager - Passwort vergessen).

Das

Formular kann durch einen Klick auf den Button "Zurücksetzungslink anfordern" abgesendet werden.

Der Account Manager überprüft die abgesendeten Daten und schickt automatisch einen Zurücksetzungslink an die Recovery E-Mailadresse. Dieser Vorgang kann bis zu 15 Minuten dauern. Der Zurücksetzungslink führt zu einer weiteren Eingabemaske,

über die ein neues Passwort gesetzt werden kann.

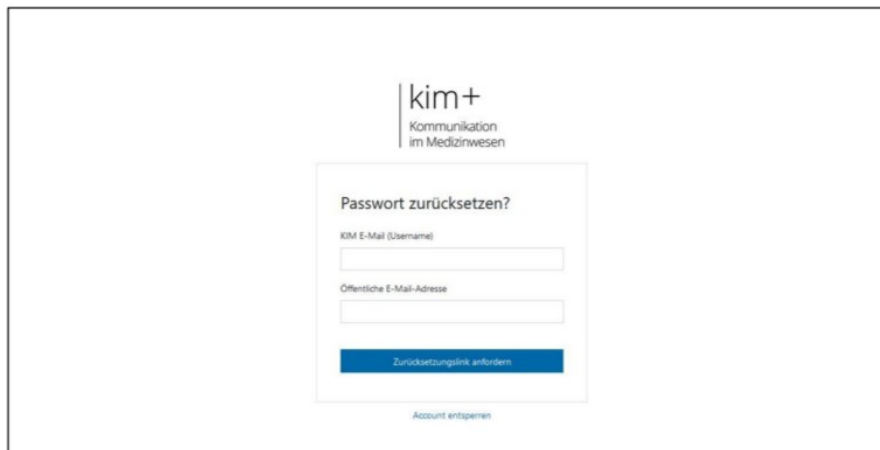


Abbildung 27 Account Manager - Passwort vergessen

7.9 Account entsperren

Vorbedingung: Der Account des Anwenders ist gesperrt. Dies erfolgt, wenn das Passwort dreimal falsch

eingegeben wird. Der Entsperrungsprozess wurde von der verantwortlichen Stelle angestoßen. Der Anwender hat Zugriff auf das Postfach der hinterlegten Recovery E-Mail-Adresse.

Der Account Manager sendet einen Link an die angegebene Recovery E-Mail-Adresse, der den Anwender zu einer Eingabemaske zum Setzen eines neuen Passworts führt. Nach Abschluss des Vorgangs erfolgt eine Weiterleitung zur Loginseite des Account Managers (Abbildung 23 Account Manager

- Login). Der Account ist nun entsperrt und der Anwender kann sich mit dem neu gesetzten Passwort einloggen.

Anmerkung: Nach dem Abschluss des Vorgangs wird eine Benachrichtigung an die Recovery E-Mail-Adresse gesendet.

7.10 Logout

Vorbedingung: Der Anwender ist eingeloggt und befindet sich auf der Menüseite.

Der Logout wird durch einen Klick auf den Button "Abmelden" (Abbildung 24 Account Manager - Menü,

Markierung 6) ausgelöst. Es erfolgt eine automatische Weiterleitung auf die Loginseite.

8 Anlagen und Verzeichnisse

Abkürzungsverzeichnis

Begriff	Erklärung
CM	Clientmodul
DNS	Domain Name System
HBA	Heilberufsausweis
ICCSN	Integrated Circuit Card Serial Number
IK-Nummer	Institutskennzeichen lt. § 293 SGB V
KIM	Kommunikation im Medizinwesen
LE	Leistungserbringer
LEI	Leistungserbringer-Institution
NTP	Network Time Protocol
OSS	Open Source Software
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POP3	Post Office Protocol (Version 3)
S/MIME	Secure / Multipurpose Internet Mail Extensions
SMC-B	Security Module Card - Betriebsstätte
SMTP	Simple Mail Transfer Protocol
TI	Telematik Infrastruktur
TLS	Transport Layer Security
URI	Uniform Resource Identifier

Tabelle 9 Abkürzungsverzeichnis

© Research Industrial Systems Engineering (RISE)
Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F
2320 Schwechat
Austria, Europe

<http://www.rise-world.com>
support@rise-kim.de