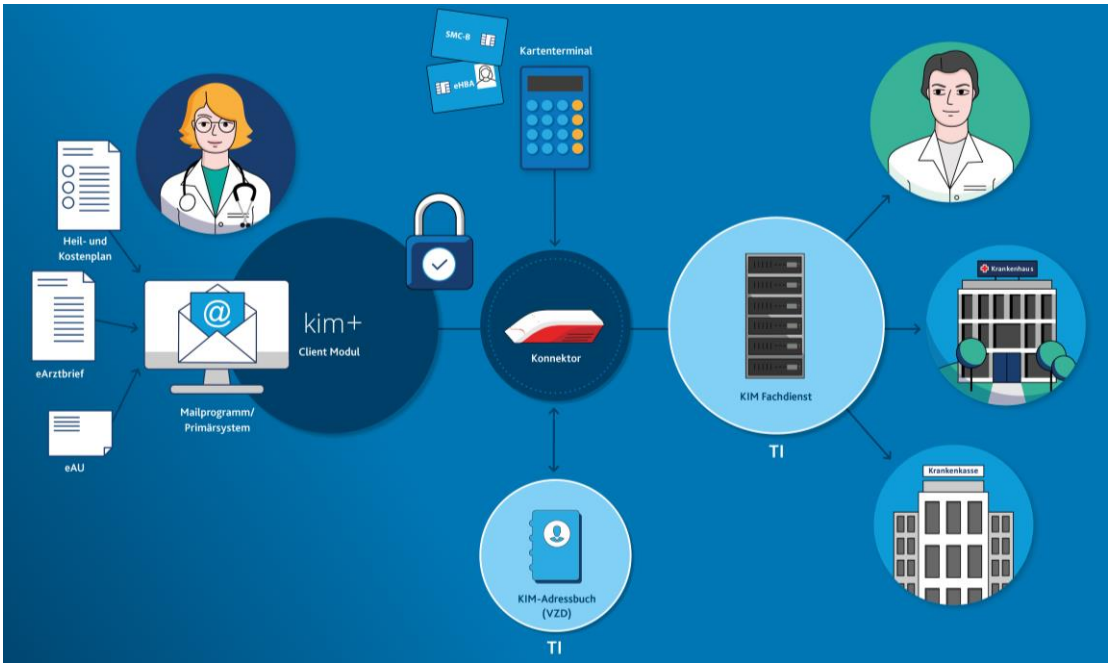
# kim+ Anwenderhandbuch - Arvato Systems Digital GmbH




| | |
|---|---|
| Dokumenten Version: | 2.2 |
| Zu kim+ Produktversion | 1.4.5 |
| Stand: | 29.09.2022 |
| Status: | Freigabe |
| Klassifizierung: | Vertraulich |
| Referenzierung: | [ARV_Anwenderhandbuch_KIM] |

## Dokumentenhistorie (gekürzt)

| Version | Stand | Kap | Grund der Änderung | Bearbeitet durch | Kommentar |
|---|---|---|---|---|---|
| 0.1.0 | 05.11.2020 | alle | Initiale Erstellung | Jan Gebelt | Entwurf |
| 1.0.0 | 06.11.2020 | alle | Ergänzungen | Sophie Pitka | Freigabe |
| 1.4 | 16.06.2021 | 4.1 | Update zu kim+ Rel 1.1.0 | Marcel Bennicke | Freigabe |
| 1.4.1 | 01.07.2021 | 4.1 | Gültigkeit Registrierungslink angepasst | Jan Gebelt | Freigabe |
| 1.4.2 | 03.08.2021 | 4.4 | Voraussetzungen für Zertifikatsbezug ergänzt | Jan Gebelt | |
| 1.4.3 | 11.08.2021 | 2.2.1, 2.4, 3, 5.2 | Update zu kim+ Rel 1.2.1.0 | Marcel Bennicke | Freigabe |
| 1.5.0 | 30.09.2021 | 4.1 | Update zu kim+ Rel 1.3.0: Erfassung IK-Nummer, Ablauf Frist Registrierungslink | Marcel Bennicke | Freigabe |
| 1.6.0 | 26.11.2021 | 2, 2.7, 3, 3.6, 5.2 | Titelbild hinzugefügt, allgemeine Korrekturen, Überblick über TLS Zertifikate, Update zu kim+ Rel. 1.3.2: Anbieter-Sperre und Anbieter-Deregistrierung | Rebecca Werdehausen | Freigabe |
| 1.7.0 | 21.12.2021 | 4.3 | Update zu Rel 1.4.0: Installation, Inbetriebnahme und Konfiguration des Clientmoduls als Dienst hinzugefügt. | Rebecca Werdehausen | Freigabe |
| 1.8.0 | 01.02.2022 | 4.3 | Update Installation als Dienst | Sophie Pitka | Freigabe |
| 2.0 | 01.04.2022 | alle | Update zu kim+ Release 1.4.3: Produktname, Produktlogo, Abrufintervall E-Mails, statische Route Mac | Sophie Pitka / Alexandra Schmidt | Freigabe |
| 2.1 | 09.09.2022 | 4.1.4 4.7 | Update zu kim+ Release 1.4.4: Update-Funktion des kim+ Clientmoduls | Sophie Pitka / Alexandra Schmidt | Freigabe |
| 2.2 | 29.09.2022 | 4.3.1 4.7 | Update zu kim+ Release 1.4.5: Update-Funktion des kim+ Clientmoduls, Statische Route Windows | Sophie Pitka / Alexandra Schmidt | Freigabe |

## Inhaltsverzeichnis

# 1 Einleitung

Dieses Handbuch dient der Beschreibung des Produktes kim+. Insbesondere werden die einzelnen Funktionen sowie Vorgaben und Hinweise für die Verwendung und den Betrieb von kim+ dargestellt.

Die Schritte zur Inbetriebnahme von kim+ sind in Kapitel 2.7 erklärt. Die Konfiguration erfolgt über verschiedene Komponenten, deren Funktionen und Konfigurationsmöglichkeiten in separaten Abschnitten beschrieben werden:

- Die **Teilnehmeranwendung** unterstützt Nutzer bei der Inbetriebnahme und Außerbetriebnahme von kim+-E-Mail-Konten.
- Das **Clientmodul** stellt die Verbindung zum lokalen Konnektor und damit zum kim+ Fachdienst und zur Telematik Infrastruktur her. Es sorgt dafür, dass E-Mails signiert und verschlüsselt empfangen und versendet werden können.
- Über den **Account** Manager aktivieren Sie Ihr E-Mail-Konto. Es stehen außerdem weitere Funktionen für die Administration des Benutzeraccounts zur Verfügung, z. B. Änderungen der Stammdaten, Zurücksetzen des Passworts oder Einstellung einer Abwesenheitsnotiz.

# 2 Produktbeschreibung kim+

## 2.1 Was ist kim+?

kim+ ermöglicht den sicheren Austausch von medizinischen Dokumenten über ein sicheres Übermittlungsverfahren. Das Produkt kann mit einem gültigen kim+-E-Mail-Konto verwendet werden durch:

- Ärzte, Psychotherapeuten, Heilberufler und medizinisches Personal,
- Krankenhäuser (Ärzte und Pflegepersonal) und
- Basis- / KTR-Consumer, z. B. Sachbearbeiter in Krankenversicherungen.

kim+ besteht aus einem Clientmodul (CM), dem Account Manager für die Verwaltung von kim+-E-Mail-Konten und notwendigen Schnittstellen zur TI-Infrastruktur. Zusätzlich bedarf es zur Nutzung des Produktes des Einsatzes von Konnektoren und Kartenlesegeräten (siehe Abschnitt 2.3).

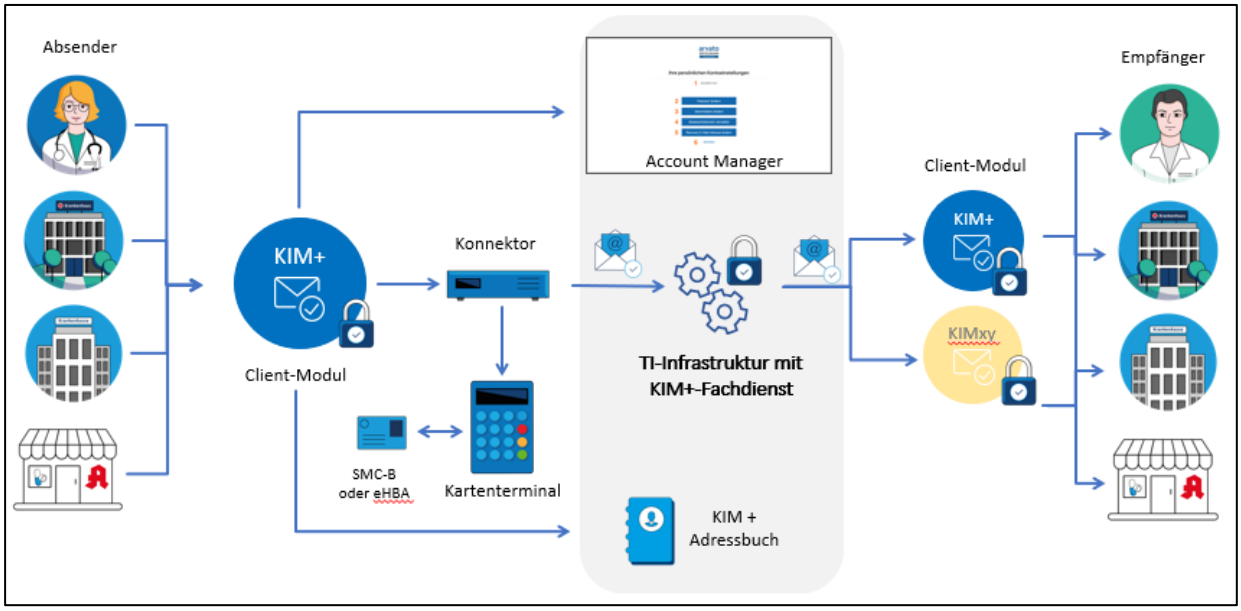



**Abbildung 1: Überblick kim+**

## 2.2 Funktionen von kim+

### 2.2.1 Nachrichtenversand

E-Mails können über den lokalen Port (SMTP-Port) des kim+ Clientmoduls 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.

### 2.2.2 Nachrichtenempfang

E-Mails können über den lokalen Port (POP3-Port) des kim+ Clientmoduls empfangen werden. Dabei wird überprüft, ob die Nachrichten einem kim+-S/MIME Profil entsprechen. Entsprechende Nachrichten werden entpackt, entschlüsselt und die enthaltene Signatur wird einer Prüfung am Konnektor des Benutzers unterzogen. Falls die Nachricht nicht entschlüsselt werden kann, wird der Nachricht ein entsprechender Vermerk hinzugefügt. Das Ergebnis der Prüfung wird in Form eines vereinfachten Prüfberichts im textuellen Teil der ursprünglichen E-Mail angehängt. Danach werden alle Nachrichten an den E-Mail-Client weitergeleitet. Nachrichten, die nicht einem kim+-S/MIME Profil entsprechen, werden nicht verarbeitet (gemäß gematik Anforderung KOM-LE-A_2042).

### 2.2.3 Verwaltung des Benutzeraccounts über den Account Manager

Der Account Manager bietet dem Anwender diverse Funktionen (siehe Abschnitt 5) für die Verwaltung der kim+-E-Mail-Konten für die Leistungserbringer und -Institutionen an. Der Benutzer kann dort beispielsweise 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 5.1) und kann sich dann bei Bedarf mit seinen Zugriffsdaten anmelden (siehe Abschnitt 5.2).

## 2.3 Systemvoraussetzungen für kim+

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

### 2.3.1 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
    - **Anmerkung:** Die Installation des KIM Clientmoduls als Dienst ist gegenwärtig nur auf Windows möglich (getestet mit Version 10 und Server 2019).
- Java Runtime Environment (JRE) ab Version 11 inklusive JavaFX (wird mit dem Clientmodul ausgeliefert)
- Mail Client Software wie Thunderbird oder Outlook (in aktueller Version)
- Internet Browser (Chrome, Firefox oder Edge)
- Internetverbindung
- 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`)

### 2.3.2 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 die Datenübertragung über den Konnektor in die Telematik Infrastruktur (TI) funktioniert, müssen zusätzliche Netzwerk-Konfigurationen vorgenommen werden.

- Routen in die TI müssen zum Konnektor zeigen für die direkte Datenübertragung über POP3/SMTP und DNS.
- 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 kommunizieren, müssen die gleiche Firmware Version haben. Ansonsten kann es zu Kommunikationsproblemen kommen, da unterschiedliche Konnektorversionen unterschiedliche Sicherheitsstandards unterstützen.

## 2.4 Sicherheitshinweise

### 2.4.1 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 somit auch das lokale Netzwerk zu schützen.

### 2.4.2 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 Produkts durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden. Die Administratoren müssen Authentisierungsinformationen geheim halten bzw. dürfen diese nicht an Unberechtigte weitergeben.

### 2.4.3 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. 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.

## 2.5 Lieferbestandteile des Produktes kim+

Folgende Bestandteile werden mit der Version 1.4.3 des Produktes kim+ ausgeliefert:

| Bestandteile | Beschreibung |
|---|---|
| kim+ Anwenderhandbuch.pdf | kim+ Installations- & Anwenderhandbuch (dieses Dokument) |
| Registrierungsmöglichkeit am Account Manager | Zur Verwaltung des Benutzeraccounts kann sich der Benutzer am Account Manager registrieren und hat dann die Möglichkeit, spezielle Funktionen zu nutzen wie bspw. „Passwort zurücksetzen“ usw. |
| kimplus-clientmodul_1_4_5_0_AR_windows-x64.exe | kim+ Clientmodul Installer für Windows 64bit |
| clientmodul-installer_1_4_5_0_AR_windows-x32.exe | kim+ Clientmodul Installer für Windows 32bit |
| kimplus-clientmodul_1_4_5_0_AR_macos.dmg | kim+ Clientmodul Installer für MacOS |
| kimplus-clientmodul_1_4_5_0_AR_linux.deb<br>kimplus-clientmodul_1_4_5_0_AR_linux.rpm | kim+ Clientmodul Installer für Linux |

**Tabelle 1: Bestandteile des Produktes kim+**

## 2.6 TLS Zertifikate für die Nutzung von kim+

Vor der Installation und Inbetriebnahme des kim+ müssen entsprechende TLS Zertifikate und Schlüsselmaterial lokal vorhanden sein, die für den Betrieb notwendig sind. Dabei muss der Nutzer sicherstellen, dass nur vertrauenswürdige Zertifikate und Schlüssel in die Komponente eingebracht werden.

Die Zertifikate werden über die TLS Konfigurationseinstellungen in das Clientmodul eingebracht. Dies gilt sowohl initial für die Ersteinrichtung als auch periodisch vor Ablauf des jeweils aktuell verwendeten Zertifikats.

In Abbildung 2 werden alle für KIM+ benötigten TLS Zertifikate dargestellt:

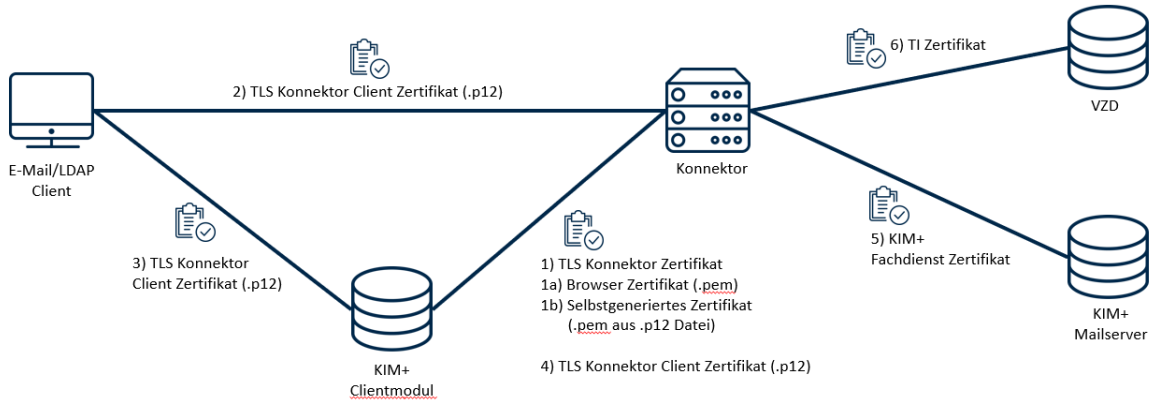



**Abbildung 2: Übersicht der verwendeten TLS Zertifikate**

Wie die Zertifikate in den einzelnen Komponenten verwendet werden, wird im Folgenden beschrieben. Für die Konnektoren von secunet und RISE wird auf die betreffenden Menüpunkte verwiesen. Das Menü der KoCoBox kann von der Beschreibung abweichen. Prüfen Sie ggf. das Handbuch Ihres Konnektors.

### 1) TLS Konnektor Zertifikat

Mit dem TLS Konnektor Server Zertifikat authentifiziert sich der Konnektor gegenüber dem Clientmodul.

**Konnektor:** Das TLS Konnektor Zertifikat (1a) wird im .pem Format im Menü des verwendeten Konnektors heruntergeladen.

Im secunet Konnektor erfolgt dies über den Menüpunkt `Praxis > Clientsysteme` und die Option „Konnektor-Zertifikat herunterladen“. Alternativ kann für secunet Konnektoren ein selbstgeneriertes Zertifikat aus einer .p12 Datei verwendet werden (1b). Dafür wird die Funktion „Software-Server-Zertifikat“ im secunet Konnektor-Menü unter `Praxis > Clientsysteme > Clientsystem-Einstellungen` aktiviert.

Im RISE Konnektor wird über Klick auf das rote Warndreieck im Browser die Zertifikatsprüfung geöffnet und über die Funktion „In Datei kopieren“ eine Zertifikats-Datei erstellt.

**Clientmodul:** Das heruntergeladene Server Zertifikat wird dann im Clientmodul unter `Einstellungen > TLS > Konnektor` im Feld „Serverzertifikat“ eingebracht (siehe Kapitel 4.3.2.4). Wird

für einen secunet Konnektor ein selbstgeneriertes Zertifikat verwendet, muss zunächst aus der .p12 Datei eine .pem Datei extrahiert werden (z. B. mit dem Tool KeyStore Explorer).

### 2) und 3) TLS Konnektor Client Zertifikat

Mit dem TLS Konnektor Client Zertifikat authentifiziert sich der E-Mail/LDAP Client gegenüber dem Konnektor und dem Clientmodul.

**Konnektor**: Zunächst muss der E-Mail/LDAP Client im Konnektor angelegt und das Zertifikat als .p12 Container erstellt werden.

Im secunet Konnektor wird das Clientsystem im Menü `Praxis > Clientsysteme > Clientsystem anlegen…` hinzugefügt. Anschließend klicken Sie auf das angelegte Clientsystem, um das Zertifikat zu erstellen.

Im RISE Konnektor finden Sie die Funktion im Menü `Clientsystem > Anbindung der Clientsysteme`.

**Clientmodul**: Das Zertifikat wird im Clientmodul in den Konfigurationseinstellungen `TLS > Proxy /Clientsystem` unter dem Punkt „TLS mit zertifikatsbasierter Client-Authentifizierung“ hochgeladen (siehe Kapitel 4.3.2.4).

**E-Mail/LDAP Client**: In der Zertifikatsverwaltung des E-Mail/LDAP Clients wird das Zertifikat importiert. Des Weiteren müssen im E-Mail/LDAP Client Ausnahmeregeln für das Senden und Empfangen über die verwendeten Server hinzugefügt werden. Für Thunderbird wird dies in Kapitel 4.5.3 erklärt.

Außerdem müssen die folgenden Zertifizierungsstellen im E-Mail/LDAP Client bekannt sein:

- GEM.KOMP-CA3 (PU)
- GEM.KOMP-CA4 (PU)
- GEM.KOMP-CA5 (PU)
- GEM.KOMP-CA6 (PU)
- GEM.KOMP-CA7 (PU)
- GEM.KOMP-CA27 (RU)
- GEM.KOMP-CA28 (RU)

Diese sind für den jeweiligen Lizenzstand und die Umgebung zu beziehen:

| Lizenz | Umgebung | Download Zertifizierungsstellen |
|---|---|---|
| PTV-3 | PU | https://download.tsl.ti-dienste.de/ |
| | RU | https://download-ref.tsl.ti-dienste.de/ |
| PTV-4 | PU | https://download.tsl.ti-dienste.de/ECC/ |
| | RU | https://download-ref.tsl.ti-dienste.de/ECC/ |

### 4) TLS Konnektor Client Zertifikat

Mit dem TLS Konnektor Client Zertifikat als .p12 Container authentifiziert sich das Clientmodul gegenüber dem Konnektor.

Das Zertifikat aus dem Konnektor (siehe vorheriger Punkt) wird im **Clientmodul** in den Konfigurationseinstellungen `TLS > Konnektor > Client-Authentifizierung` unter „TLS mit zertifikatsbasierter Client-Authentifizierung“ hochgeladen (siehe Kapitel 4.3.2.4).

### 5) kim+ Fachdienst Zertifikat

Das Zertifikat authentifiziert das Clientmodul gegenüber dem kim+ Fachdienst. Sie erhalten die Zertifikats-Datei und das Zertifikatspasswort im Rahmen der Registrierung (siehe Kapitel 3.1). Im **Clientmodul** wird das Zertifikat unter `Einstellungen > TLS > Fachdienst` hochgeladen (siehe Kapitel 4.3.2.4). Dieses Zertifikat wird auch als „Clientmodul-Zertifikat“ referenziert.

### 6) TI Zertifikat

Das Zertifikat authentifiziert den Verzeichnisdienst (VZD) gegenüber dem Konnektor. Es ist bereits im **Konnektor** hinterlegt.

## 2.7 Inbetriebnahme kim+

Führen Sie folgende Schritte aus, um die E-Mail-Funktionen eines kim+ E-Mail-Kontos nutzen zu können:

| Schritte zur Inbetriebnahme eins kim+ E-Mail Kontos | | |
|---|---|---|
| **Schritt** | **Aktivität** | **Beschreibung** |
| 1 | **E-Mail-Konto registrieren** | Über die **Teilnehmeranwendung** registrieren Sie zunächst ein neues kim+ E-Mail-Konto mit einer frei wählbaren E-Mail-Adresse.<br>Näheres zur Registrierung über die Teilnehmeranwendung finden Sie in Kapitel 3. |
| 2 | **Installation kim+ Clientmodul** | Installieren Sie das kim+ **Clientmodul** und verbinden Sie es mit dem Praxis-Konnektor.<br>Näheres zur Installation & Konfiguration des Clientmoduls finden Sie in Kapitel 4. |
| 3 | **Legitimation über Heilberufsausweis (HBA) oder SMC-B** | Legitimieren Sie Ihr kim+ E-Mail-Konto über den **Account Manager** unter Eingabe der PIN für den HBA oder die Nutzung einer SMC-B und vergeben Sie ein Passwort für das Konto.<br>Näheres zur Legitimation und Abschluss der Registrierung finden Sie in Kapitel 3. |
| 4 | **Verbinden kim+ Software mit der TI** | Verbinden Sie das kim+ Clientmodul mit der Telematik Infrastruktur, indem Sie das Clientmodul-Zertifikat herunterladen und im Clientmodul unter `TLS > Fachdienst` hochladen.<br>Näheres zur Anbindung des Clientmoduls und den Download von elektronischen Schlüsselinformationen über die Teilnehmeranwendung finden Sie in Kapitel 3.4. |
| 5 | **Anbindung E-Mail-Client** | Binden Sie einen marktüblichen E-Mail-Client (oder PVS) zur Nutzung des kim+ E-Mail-Kontos an.<br>Näheres zur Anbindung des E-Mail-Client finden Sie in Kapitel 4.5 |

**Tabelle 2: Schritte zur Inbetriebnahme kim+**

# 3 Teilnehmeranwendung

Für den Fall, dass ein eingesetztes Primärsystem (PVS, KIS, …) keine integrierten Funktionen zur Nutzung von kim+ bereitstellt, können Teilnehmer alternativ über die KIM+ Teilnehmeranwendung zentrale Funktionen zur Verwaltung tätigen.

Die Teilnehmeranwendung kim+ bietet im Überblick folgende Funktionen:

| Übersicht Funktionen Teilnehmeranwendung KIM+ | |
|---|---|
| **Webseite** | **Beschreibung** |
| https://ssp.kimplus.de/registrieren | **Registrierung** eines neuen kim+ Teilnehmers & einer neuen kim+ E-Mail. |
| https://ssp.kimplus.de/deregistrieren | **De-Registrierung** eines kim+ Teilnehmers und einer bestehenden kim+ E-Mail. |
| https://ssp.kimplus.de/accountEntsperren | **Entsperren** einer bestehenden kim+ Mailadresse. |
| https://ssp.kimplus.de/zertifikat | Herunterladen von **elektronischen Zertifikaten und Schlüsseln** für eine sichere Kommunikation mit der Telematik Infrastruktur. |

**Tabelle 3: Funktionen Teilnehmeranwendung kim+**

Hinweis: Beim Verwenden der Funktionen erscheint eine Fehlermeldung? Dies kann darauf zurückzuführen sein, dass Ihr Anbieter den Vertrag gesperrt oder das Konto deregistriert hat. Mehr Informationen dazu erhalten Sie in Kapitel 3.6.

## 3.1 Konto und Teilnehmer registrieren

Die Registrierung eines kim+ E-Mail-Kontos für Teilnehmer kann über folgende Internet-Adresse erreicht werden:

https://ssp.kimplus.de/registrieren

In 3 Schritten werden Sie durch die Registrierung geführt. Dafür sind folgende Informationen bereitzuhalten:

- **Eine öffentlich erreichbare E-Mail-Adresse zum Erhalt weiterer Registrierungsinformationen, Pflicht**
- **kim+ Contract ID (vom Anbieter im Vorfeld übermittelt), Pflicht**
- LANR (Lebenslange Arztnummer), optional
- BSNR (Betriebsstättennummer), optional
- Für Zahnärzte die KZV Abrechnungsnummer, optional
- IK-Nummer (Institutskennzeichen lt. § 293 SGB V), optional


**Abbildung 3: Angabe Registrierungsinformationen**

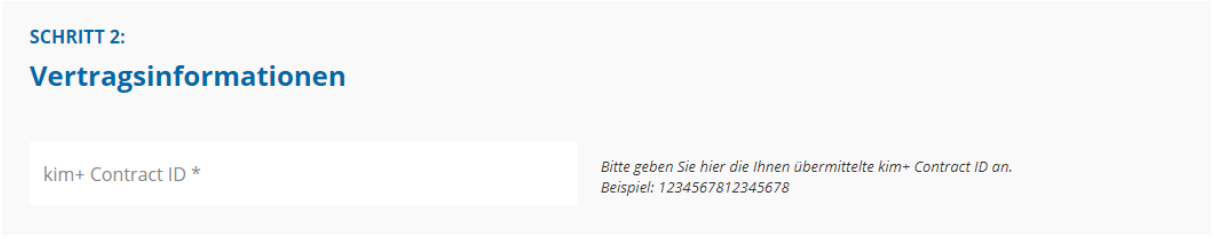



**Abbildung 4: Angabe Vertragsinformationen**

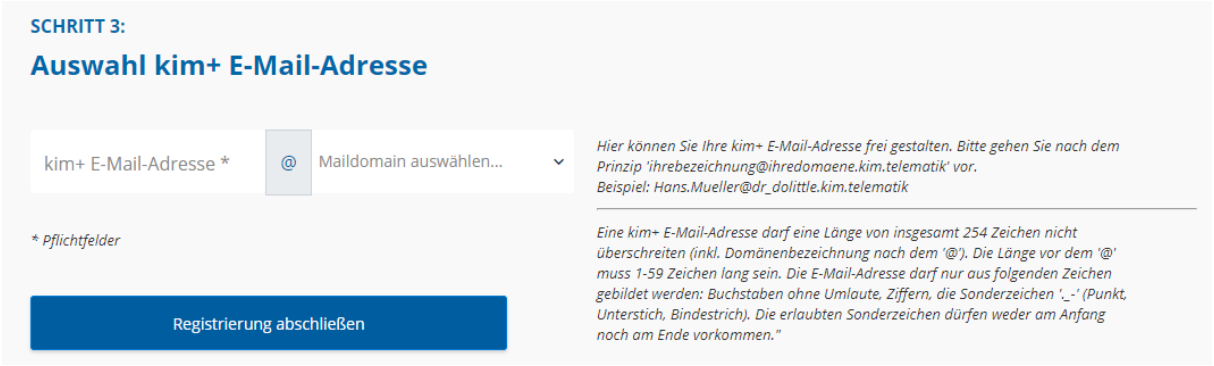



**Abbildung 5: Auswahl kim+ E-Mail-Adresse**

Es werden auch alternative Mail-Domänen (der Teil hinter dem @ in der kim+-E-Mail-Adresse) unterstützt. Anwender können während der Registrierung einer kim+-E-Mail-Adresse unter verschiedenen Mail-Domänen auswählen, sofern diese Option konfiguriert wurde. Die Eingabefelder für Schritt 3 sind erst aktiv, wenn eine gültige kim+ Contract ID in Schritt 2 eingegeben wurde. Mail-Domänen müssen im Vorfeld durch den Anbieter freigeschaltet werden. Wenn nichts anderes vereinbart ist, wird nur die Standarddomäne `mail.kim.telematik` angeboten.

Sobald die Registrierung über die Schaltfläche **REGISTRIERUNG ABSCHLIESSEN** abgeschlossen wird, erhalten Teilnehmer weiterführende E-Mails an die angegebene öffentliche E-Mail-Adresse gesendet. Diese beinhalten:

1. Willkommensmail mit Angaben zum Download von kim+ Clientmodul und Link zum Zertifikatsdownload sowie die Zertifikatsnummer
2. Separate E-Mail mit einem geschützten Passwort zu Schlüsselinformationen
3. Separate E-Mail mit einem Registrierungslink zur Legitimation

**Der Registrierungslink zur Legitimation kann erst nach erfolgter Installation und Vorkonfiguration des kim+ Clientmoduls (siehe Kapitel 4.2 ff.) aufgerufen werden. Der Link muss auf dem Rechner geöffnet werden, auf dem auch das kim+ Clientmodul installiert ist. Der Link ist 96 Stunden gültig. Weitere Informationen zur Kartenauthentisierung finden Sie im Kapitel 5.3.**

Sollte die Registrierung nicht innerhalb der Frist zu Ende geführt werden, werden sämtliche bis dahin erfasste Informationen wieder verworfen, auch die „Vorreservierung“ der kim+ E-Mail-Adresse. Nach Ablauf der Frist kann der Registrierungsvorgang dann erneut gestartet werden, sofern bis dahin nicht anders vergeben, auch mit der identischen kim+ E-Mail-Adresse.

## 3.2 Konto und Teilnehmer de-registrieren

Die De-Registrierung eines kim+ E-Mail-Kontos kann über folgende Internet-Adresse erreicht werden:

https://ssp.kimplus.de/deregistrieren

**Halten Sie dafür folgende Informationen bereit**:

- kim+ E-Mailadresse
- Passwort für kim+ E-Mailadresse
- kim+ Contract ID

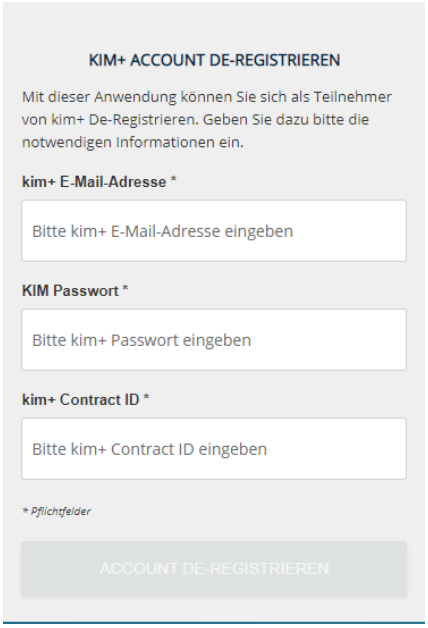



**Abbildung 6: De-Registrierung**

Sobald die De-Registrierung über die Schaltfläche **ACCOUNT DE-REGISTRIEREN** ausgelöst wird, erhalten Teilnehmer eine E-Mail mit einem Link zur Bestätigung der De-Registrierung an die öffentliche E-Mailadresse, die bei der Registrierung hinterlegt wurde.

**Die De-Registrierung kann nur erfolgreich abgeschlossen werden, wenn der Link zur Bestätigung der De-Registrierung von dem Rechner aus aufgerufen wird, auf dem auch das kim+ Clientmodul installiert ist.**

## 3.3 Konto entsperren

Sollte ein kim+ E-Mail-Konto einmal gesperrt sein (beispielsweise durch mehrmalige Eingabe eines falschen Passworts) kann dieses Konto nach einer Legitimation mit dem HBA/SMC-B wieder entsperrt werden.

Das Entsperren eines kim+ E-Mail-Kontos kann über folgende Internet-Adresse erreicht werden:

https://ssp.kimplus.de/accountEntsperren

**Halten Sie dafür folgende Informationen bereit**:

- kim+ E-Mail
- kim+ Contract ID

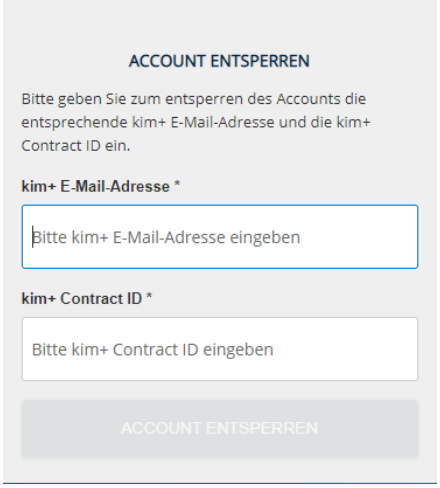



**Abbildung 7: Account entsperren**

Sobald das Entsperren über die Schaltfläche **ACCOUNT ENTSPERREN** ausgelöst wird, erhalten Sie eine E-Mail mit einem Link zur Bestätigung der Entsperrung an die öffentliche E-Mailadresse, die bei der Registrierung hinterlegt wurde.

**Die Entsperrung kann nur erfolgreich abgeschlossen werden, wenn der Link zur Bestätigung der Entsperrung von dem Rechner aus aufgerufen wird, auf dem auch das kim+ Clientmodul installiert ist.**

## 3.4 Einen Zertifikatsschlüssel für das Clientmodul beziehen

Im Rahmen der Inbetriebnahme eines kim+ E-Mail-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 (siehe Kapitel 4.3.1 und 4.3.2 ff.), sowie die Registrierung der kim+ Adresse durch Legitimation abgeschlossen (siehe Kapitel 3.1) werden. Der Schlüssel kann anschließend von Teilnehmern wie folgt bezogen werden:

1. Über den Link in der Willkommens-E-Mail zu kim+ (Zertifikate beziehen) ODER über den Aufruf folgender Website der Teilnehmeranwendung:

   https://ssp.kimplus.de/zertifikat

2. Geben Sie die nötigen Informationen im Anmeldedialog an:
   - kim+ E-Mail
   - kim+ Contract ID
   - Zertifikatsnummer (Siehe Willkommens-E-Mail zu kim+)
   - kim+ Passwort

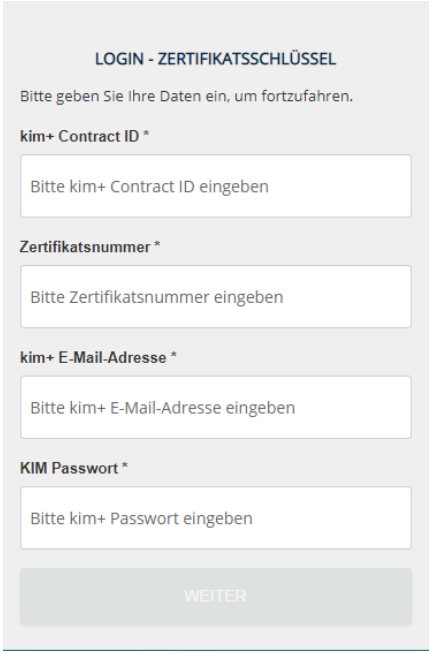



**Abbildung 8: Anmeldung Download Zertifikatsschlüssel**

3. Laden Sie den hinterlegten Schlüssel mit der angegebenen Zertifikats-Nr. (siehe Willkommens-E-Mail) herunter.

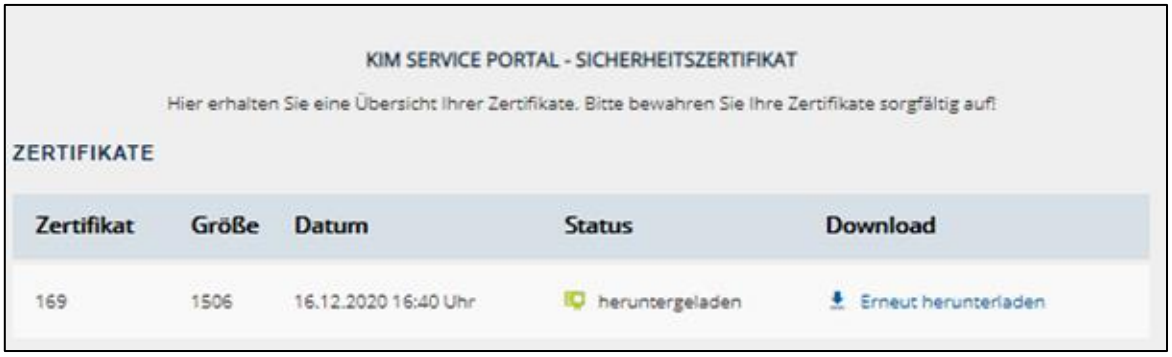



**Abbildung 9: Download Zertifikatsschlüssel**

**Bitte bewahren Sie diese Schlüsseldatei sorgfältig auf. Sie wird für die weitere Anbindung des Clientmoduls an die Telematik Infrastruktur benötigt (auf dem PC, auf dem das Clientmodul installiert ist).**

## 3.5 Benachrichtigung bei Austausch von Zertifikaten

Nähert sich ein Zertifikat, das im Rahmen der Verbindung zwischen Clientmodul und Telematik Infrastruktur eingesetzt wird, seinem Gültigkeitsende werden Teilnehmer über die öffentliche E-Mailadresse mindestens 30 Tage vorher darüber informiert. In diesem Fall wird den Teilnehmern ein neues Zertifikat zugewiesen, das über den oben genannten Weg bezogen werden kann.

## 3.6 Sperrung oder De-registrierung durch den Anbieter

In Ausnahmefällen kann es vorkommen, dass der Anbieter Ihren Vertrag **gesperrt** hat. Durch das Sperren des Vertrags, identifiziert über die kim+ Contract ID, werden auch alle zur kim+ Contract ID angelegten kim+ E-Mail-Konten gesperrt. Das bedeutet:

- Sie können mit den betreffenden kim+ E-Mail-Konten keine Nachrichten versenden.
- Sie können mit den betreffenden kim+ E-Mail-Konten keine Nachrichten empfangen.
- Sie können sich mit den betreffenden kim+ E-Mail-Konten nicht mehr im Account Manager einloggen, um z. B. eine Abwesenheitsnotiz zu setzen.

Des Weiteren hat eine solche Vertragssperrung folgende Auswirkungen auf die Funktionen der Teilnehmeranwendung:

- Zu dem gesperrten Vertrag können keine neuen kim+ E-Mail-Konten registriert werden.
- Sie können die seitens Anbieter gesperrten kim+ E-Mail-Konten nicht wieder selbst entsperren.
- Sie können aber weiterhin ein bestehendes kim+ E-Mail-Konto des gesperrten Vertrags selbst de-registrieren.

Die anbieterseitige Sperrung der kim+ Contract ID und der Konten kann nur durch den Anbieter wieder aufgehoben werden. Nach Aufhebung der Anbieter-seitigen Sperre, befinden sich alle Konten zum Vertrag wieder im vorhergehenden Zustand vor der Sperre. Es kann vorkommen, dass ein Konto zuvor bereits durch den Teilnehmeraktionen gesperrt wurde (durch dreimalige Falscheingabe des Passworts). Sie müssen dieses Konto dann erst über die Teilnehmeranwendung selbst entsperren (siehe Kapitel 3.3).

Wenn Ihr Konto durch Sie oder den Anbieter **de-registriert** wurde, ist es über die Teilnehmeranwendung nur möglich ein neues Konto zu registrieren. Eine deregistrierte E-Mail-Adresse kann nicht erneut registriert werden.

# 4 kim+ Clientmodul

## 4.1 Komponenten

Das kim+ Clientmodul (CM) ist eine eigenständige Software-Komponente, die in der Einsatzumgebung des LE / der LEI verwendet wird. Es besteht aus zwei Sub-Komponenten, die sich auch je nach Ausprägung des Clientmoduls separat installieren lassen.

### 4.1.1 Mail Proxy

Der Teil „Mail Proxy“ des kim+ Clientmoduls stellt die eigentlichen Funktionalitäten für das Versenden und Empfangen von E-Mails zur Verfügung. Die Aufgabe des Mail Proxys ist das Aufbringen und Aufheben des Schutzes der Integrität und Vertraulichkeit der zwischen den kim+-Teilnehmern ausgetauschten E-Mail-Nachrichten. Dabei kommuniziert der Mail Proxy mit dem Clientsystem des Anwenders, dem KIM-Fachdienst des Anbieters, und nutzt über den Konnektor des Anwenders mehrere Dienste der TI-Plattform. Das verwendete kim+-S/MIME-Profil konkretisiert die S/MIME-Spezifikation und stellt sicher, dass die Interoperabilität zwischen den verschiedenen kim+-Komponenten sowie der Schutz von Integrität und Vertraulichkeit für alle personenbezogenen, medizinischen Daten gewährleistet werden.

### 4.1.2 Authentication Client (Auth Client)

Der Authentication Client (Auth Client) wurde in das kim+ Clientmodul integriert, um die Authentifizierung des LE / der LEI mittels des AUT Zertifikats der HBA bzw. SMC-B zu ermöglichen. Eine Authentifikation ist immer notwendig, wenn wesentliche Statusänderungen an einem kim+ E-Mail-Account vorgenommen werden (beispielsweise Registrierung, Entsperren, Stammdatenänderung, Passwort ändern).

### 4.1.3 Ausprägungen

Das kim+ Clientmodul lässt sich auf zwei Arten betreiben und installieren

1. Installation als Applikation (mit Mail Proxy und Auth Client)
2. Installation als Dienst (nur mit Mail Proxy).

Die Installation als Applikation ist vor allem für kleine Betriebsumgebungen geeignet, bei dem sowohl E-Mail-Client als auch das Clientmodul (inkl. E-Mail-Proxy und Auth Client) alle auf einem Rechner (z. B. dem Arbeitsplatzrechner des Leistungsempfängers) betrieben werden. Wird das Clientmodul auf diese Weise installiert, ist es nur aktiv, wenn sich der installierende Benutzer auch auf dem jeweiligen Rechner eingeloggt hat.

Die Installation des Clientmoduls als Dienst richtet sich primär an Rechenzentrumsbetrieb und Administratoren. Bei dieser Form wird nur die Mail Proxy-Funktionalität installiert. Der Auth Client kann aber weiterhin als Applikation (über den Applikations-Installer) installiert werden. Eine Installation des Auth Client als Teil der Dienst-Installation ist nicht möglich. Nach erfolgreicher Installation des Clientmoduls als Dienst, kann die Mail Proxy-Funktionalität des Clientmoduls nicht zusätzlich über den Applikations-Installer installiert werden.

Mit der Installation als Dienst läuft der Mail Proxy des Clientmoduls ohne Benutzerschnittstelle im Hintergrund und startet standardmäßig beim Hochfahren des Betriebssystems, so dass kein Login eines Benutzers notwendig ist.

Im Folgenden werden die Installation, Inbetriebnahme und Konfiguration als Applikation beschrieben. In Kapitel 4.4 wird die Installation, Inbetriebnahme und Konfiguration des kim+ Clientmoduls als Dienst dargestellt.

## 4.2 Konfigurationsparameter des Clientmoduls

Das kim+ Clientmodul verfügt über verschiedene Parameter zur Konfiguration, die in Tabelle 4 mit Name, Beschreibung und Einstellmöglichkeiten aufgelistet sind. Die genannten Einstellungen sind sowohl für das Clientmodul als Applikation als auch als Dienst relevant. Lediglich die farblich markierten Einstellungen beziehen sich nur auf die Applikation.

Die Konfigurationsdatei mit den Parametern befindet sich im Applikationsverzeichnis des Clientmoduls `kimCm` im Windows-Verzeichnis unter `C:\Windows\System32\config\systemprofile\kimCm\cm.properties`.

Ist in der Konfigurationsdatei eine Einstellung (Property) nicht vorhanden, so wird vom Clientmodul der Default-Wert angenommen. Wenn ein anderer Wert als der Default-Wert verwendet werden soll, muss die Konfigurationseinstellung (falls noch nicht vorhanden) hinzugefügt und entsprechend gesetzt werden. Dabei muss beachtet werden, dass URLs mit einem “/” escaped werden.

| Name | Name in Konfigurationsdatei | Beschreibung | Default-Wert | Wertebereich | Neustart erforderlich |
|---|---|---|---|---|---|
| SMTP Port | clientmodul.proxy.smtp.port | SMTP-Port für Clientsysteme | 25 | 1-65535 | ja |
| POP3 Port | clientmodul.proxy.pop3.port | POP3-Port für Clientsysteme | 995 | 1-65535 | ja |
| SMTP Timeout Server | clientmodul.proxy.smtp.timeout.server | Timeout für Antworten vom SMTP-Server auf SMTP-Kommandos (in Sekunden) | 300 | 1-86400 | ja |
| SMTP Timeout Client | clientmodul.proxy.smtp.timeout.client | Timeout für das Warten auf neue SMTP-Kommandos vom Clientsystem (in Sekunden) | 300 | 1-86400 | ja |
| POP3 Timeout Sever | clientmodul.proxy.pop3.timeout.server | Timeout für Antworten vom POP3-Server auf POP3-Kommandos (in Sekunden) | 300 | 1-86400 | ja |
| POP3 Timeout Client | clientmodul.proxy.pop3.timeout.client | Timeout für das Warten auf neue POP3-Kommandos vom Clientsystem (in Sekunden) | 300 | 1-86400 | Nein |
| Hostname oder IP-Adresse des Konnektors | clientmodul.core.konnektor.uri | URI des DVD des Konnektors (z. B. "https://192.168.1.46/connector.sds"), Angabe verpflichtend | - | | ja |
| Timeout Verbindungsherstellung | clientmodul.core.konnektor.connection.timeout | Timeout für die Herstellung der Verbindung mit dem Konnektor (in Sekunden) | 10 | 1-86400 | ja |
| Timeout Anfragebearbeitung | clientmodul.core.konnektor.receive.timeout | Timeout für Anfragen an den Konnektor (in Sekunden) | 60 | 1-86400 | ja |

| Name | Name in Konfigurationsdatei | Beschreibung | Default-Wert | Wertebereich | Neustart erforderlich |
|---|---|---|---|---|---|
| Time-to-live Cache Dienstverzeichnisdienst | clientmodul.core.konnektor.dvd.cache.maxTtl | Maximale Time to Live für gecachte Serviceendpunktinformationen des Dienstverzeichnisdiensts (in Sekunden) | 3600 | 1-86400 | ja |
| Time-to-live Cache Verschlüsselungszertifikate Verzeichnisdienst | clientmodul.core.konnektor.vzd.cache.maxTtl | Maximale Time to Live für gecachte Verschlüsselungszertifikate vom Verzeichnisdienst (in Sekunden) | 86400 | 1-86400 | Ja |
| Größe Verbindungs-Pool Verzeichnisdienst | clientmodul.core.konnektor.vzd.poolSize | Größe des Verbindungs-Pools für den Verzeichnisdienst | 4 | 1-20 | Ja |
| Time-to-live Cache Zuordnungen E-Mail-Adresse zu ICCSN der HBA/SM-B | clientmodul.core.konnektor.certificates.cache.maxTtl | Maximale Time to Live für gecachte Zuordnungen von Emailadressen der Sender bzw. Empfänger zu ICCSNs von deren HBAs/SM-Bs (in Tagen) | 30 | 1-60 | Ja |
| NTP Zeitsynchronisationsintervall | clientmodul.core.konnektor.ntp.updateDelay | Aktualisierungsintervall für NTP-Synchronisation mit dem Konnektor (in Sekunden) | 3600 | 1-86400 | ja |
| Mandant-ID | clientmodul.core.konnektor.context.mandantId | Mandant-ID des Kontexts für den Konnektor | - | | ja |
| Arbeitsplatz-ID | clientmodul.core.konnektor.context.workplaceId | Arbeitsplatz-ID des Kontexts für den Konnektor | - | | ja |
| Clientsystem-ID | clientmodul.core.konnektor.context.clientSystemId | Clientsystem-ID des Kontexts für den Konnektor | - | | ja |

| Name | Name in Konfigurationsdatei | Beschreibung | Default-Wert | Wertebereich | Neustart erforderlich |
|---|---|---|---|---|---|
| User-ID | clientmodul.core.konnektor.context.userId | User-ID des Kontexts für den Konnektor | - | | ja |
| Account Manager Authentication Service Endpoint | clientmodul.auth.service.endpoint | URI Endpoint des Account Managers muss für PU eingestellt sein auf: https://am.kim-plus.de/api/rest | https://local-host:8080/api/rest | | ja |
| Logging - Performanceprotokoll aktivieren | clientmodul.core.log.performance | Protokollierung von Performanceinformationen | true | true, false | ja |
| Logging - Ablaufprotokoll aktivieren | clientmodul.core.log.operation | Protokollierung von Ablaufinformationen | false | true, false | Nein |
| Logging - Time-to-live für Protokolldateien | clientmodul.core.log.retainDays | Maximale Time to Live für alle Protokolldateien (in Tagen) | 30 | 1-300 | ja |
| Konnektor - Serverzertifikat | | Auswahl einer lokal verfügbaren PEM Datei mit dem Server-Zertifikat des Konnektors | | | ja |
| Konnektor - Client-Authentifizierung | clientmodul.core.konnektor.tlsAuth | Art der Authentifizierung des Clientmoduls gegenüber dem Konnektor bei aktivierter TLS-Verbindung | CERTIFICATE | CERTIFICATE, PASSWORD, NONE | ja |
| Konnektor - zertifikatsbasierte Client-Authentifizierung | | Bei ausgewählter zertifikatsbasierter Client-Authentifizierung zum Konnektor: Auswahl einer lokal verfügbaren PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel | | | ja |

| Name | Name in Konfigurationsdatei | Beschreibung | Default-Wert | Wertebereich | Neustart erforderlich |
|---|---|---|---|---|---|
| Konnektor - passwortbasierte Client-Authentifizierung | | Bei ausgewählter, passwortbasierter Client-Authentifizierung zum Konnektor: Eingabe von Benutzername und Passwort | | | ja |
| Fachdienst - Clientzertifikat | | Auswahl einer lokal verfügbaren PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel für die erforderliche zertifikatsbasierte Client-Authentifizierung zum Fachdienst (das Fachdienst-Clientzertifikat erhalten Sie im Rahmen der Registrierung einer kim+ E-Mail-Adresse) | | | ja |
| Clientsystem - Client-Authentifizierung | clientmodul.proxy.tls | Authentifizierung des Clientsystems gegenüber dem Clientmodul (Proxy) | NONE | NONE, TLS, TLS_CLIENT_CERTIFICATE | ja |
| Clientsystem - zertifikatsbasierte Client-Authentifizierung | | Bei ausgewählter zertifikatsbasierter Client-Authentifizierung zum Clientmodul: Auswahl einer lokal verfügbaren PEM Datei mit dem Client-Zertifikat des Clientsystems | | | ja |
| SMTP Threads | clientmodul.proxy.smtp.threads | Anzahl der Threads zur Abarbeitung von SMTP Requests | Anzahl der logischen CPUs * 2 | 0-200 | Ja |
| POP3 Threads | clientmodul.proxy.pop3.threads | Anzahl der Threads zur Abarbeitung von POP3 Requests | Anzahl der logischen CPUs * 2 | 0-200 | Ja |
| AuthClient Port | clientmodul.auth.service.port | Der Port vom Auth Client Endpoint im Clientmodul | 12001 | 1-65535 | Ja |

| Name | Name in Konfigurationsdatei | Beschreibung | Default-Wert | Wertebereich | Neustart erforderlich |
|---|---|---|---|---|---|
| AuthClient Authentifizierung mit UI | clientmodul.auth.client.ui.enabled | Flag um die Authentifizierung via Auth Client UI ein- bzw. auszuschalten | true | true, false | Ja |
| AuthClient Authentifizierung ohne UI (Headless) | clientmodul.auth.client.headless.enabled | Flag um die direkte Authentifizierung ohne Auth Client UI ein- bzw. auszuschalten | false | true, false | Ja |
| Clientmodul UI | clientmodul.proxy.ui.enabled | Flag um das UI ein- bzw. auszuschalten | true | true, false | Ja |
| VZD LDAP Port | clientmodul.core.konnektor.vzd.ldaps.port | LDAPS-Port für den Verzeichnisdienst am Konnektor | 636 | 1-65535 | Ja |
| Proxy Aktivierung | clientmodul.proxy.enabled | Flag, um den Mail Proxy ein- bzw. auszuschalten | true | true, false | Ja |
| OCSP/CRL Check | clientmodul.core.tls.revocation.check | Aktivierung des OCSP bzw. CRL Checks des Account Manager-Zertifikats für die Kommunikation zwischen Account Manager (Teilkomponente des KIM Fachdiensts) und Auth Client | true | true, false | Ja |

**Tabelle 4: Konfigurationseinstellungen Clientmodul**

## 4.3 Clientmodul als Applikation

### 4.3.1 Installation

Für die Installation des kim+ Clientmoduls werden Installationspakete je Betriebsumgebung zur Verfügung gestellt. Die jeweils aktuelle Version des kim+ Clientmoduls wird unter

https://cm.kimplus.de/download/current/

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. Der installierende Benutzer muss die Signatur des Installationspakets prüfen.
4. Ausführung des Installationspakets, um den Installationsvorgang zu starten.

   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 (siehe Abbildung 10: Auswahl während der Installation). 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.

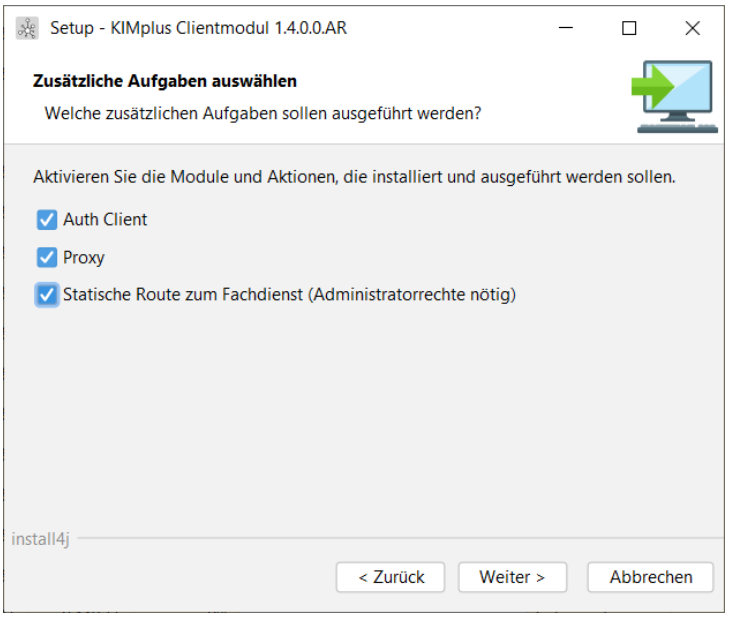



**Abbildung 10: Auswahl während der Installation**

Per Default sind alle Auswahlfelder aktiviert. Für bestimmte Client-Server-Konstellationen ist es notwendig, die Module separat installieren zu können. Weitere Informationen finden Sie dazu im Integratorhandbuch.

**Statische Route zum Fachdienst**: Um die netzwerkseitige Erreichbarkeit des kim+ Fachdienstes über einen Konnektor sicherzustellen, muss in einem folgenden Schritt die IP-Adresse des Konnektors angegeben werden (siehe Abbildung 11: Statische Route zum Fachdienst). Das Setzen der Netzwerk-Route erfordert Administrator-Rechte während des Installationsvorgangs und ist nur unter Windows verfügbar. Voraussetzung ist dafür, dass das Windows-Betriebssystem unter der Partition C installiert wurde. Andernfalls muss die statische Route manuell gesetzt werden.

Die Konfiguration einer Route muss gewöhnlich nur während der Erstinstallation des Clientmoduls erfolgen, da sie dann dauerhaft im System verankert wird. Bei der Aktualisierung eines bereits installierten Clientmoduls muss diese Option nicht aktiviert werden.

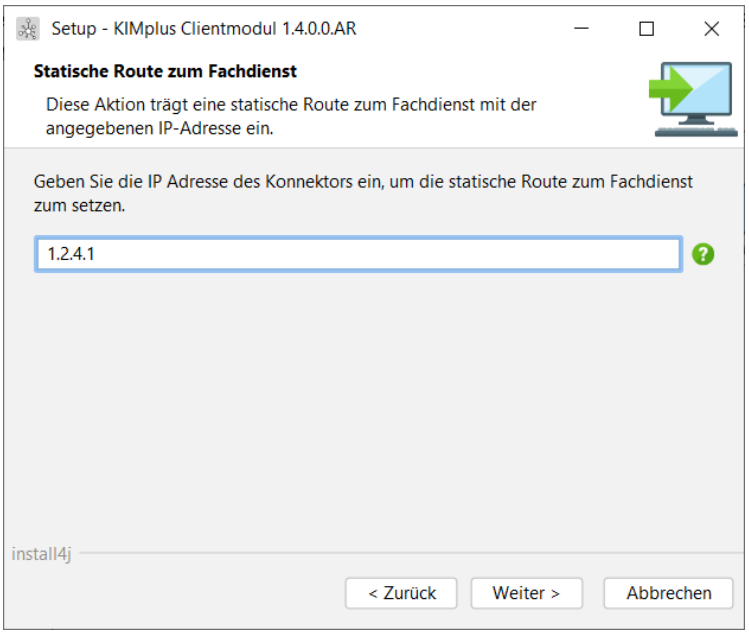



**Abbildung 11: Statische Route zum Fachdienst**

5. Die Installation des kim+ Clientmoduls erfolgt, abhängig vom Betriebssystem, im Standardordner.

Die Installation des Clientmoduls kann auch unbeaufsichtigt, ohne Benutzerinteraktion erfolgen. Informationen dazu finden Sie im Integratorhandbuch.

### 4.3.2 Konfiguration

In der grafischen Benutzeroberfläche des kim+ Clientmoduls können über bereitgestellte Konfigurationsmöglichkeiten Einstellungen vorgenommen werden, die es ermöglichen ein System auf unterschiedliche Weisen anzusprechen. In den folgenden Kapiteln sind alle Parameter mit Namen, Beschreibung und Einstellmöglichkeiten aufgelistet.

#### 4.3.2.1 Basiseinstellungen

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

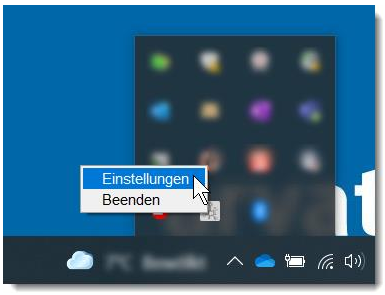



**Abbildung 12: Clientmodul in Windows Menüleiste**

1. Starten des kim+ Clientmoduls.
2. Öffnen Sie die Einstellungen über Rechtsklick auf das Clientmodul in der Menüleiste.
3. Unter den Einstellungen für den "Konnektor" (Abbildung 13: Konfigurationseinstellungen – Standardkonnektor) 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 lt. untenstehender Tabelle 5 eingestellt sein.
4. Unter den Einstellungen für "TLS" (Abbildung 15) 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: zertifikatsbasierte Authentifizierung, passwortbasierte Authentifizierung oder keine Client-Authentifizierung.
     - Bei ausgewählter zertifikatsbasierter Authentifizierung zum Konnektor: Auswählen einer lokal verfügbaren passwortgeschützten PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel sowie Eingabe des Passworts.
     - Bei ausgewählter passwortbasierter 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 (siehe Kapitel 3.4).

- Auswählen der zu verwendenden Art der Client-Authentifizierung vom Clientsystem: ohne TLS, TLS mit zertifikatsbasierter Client-Authentifizierung oder TLS ohne zertifikatsbasierte Client-Authentifizierung.
  - Die Option "ohne TLS" darf entsprechend der 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.

5. Nachdem alle Änderungen an der Konfiguration vorgenommen wurden, müssen die Einstellungen gespeichert werden.
6. Neustart des kim+ Clientmoduls, da die Konfigurationsänderungen erst danach wirksam werden.

### 4.3.2.2 Konfigurationseinstellungen Konnektor

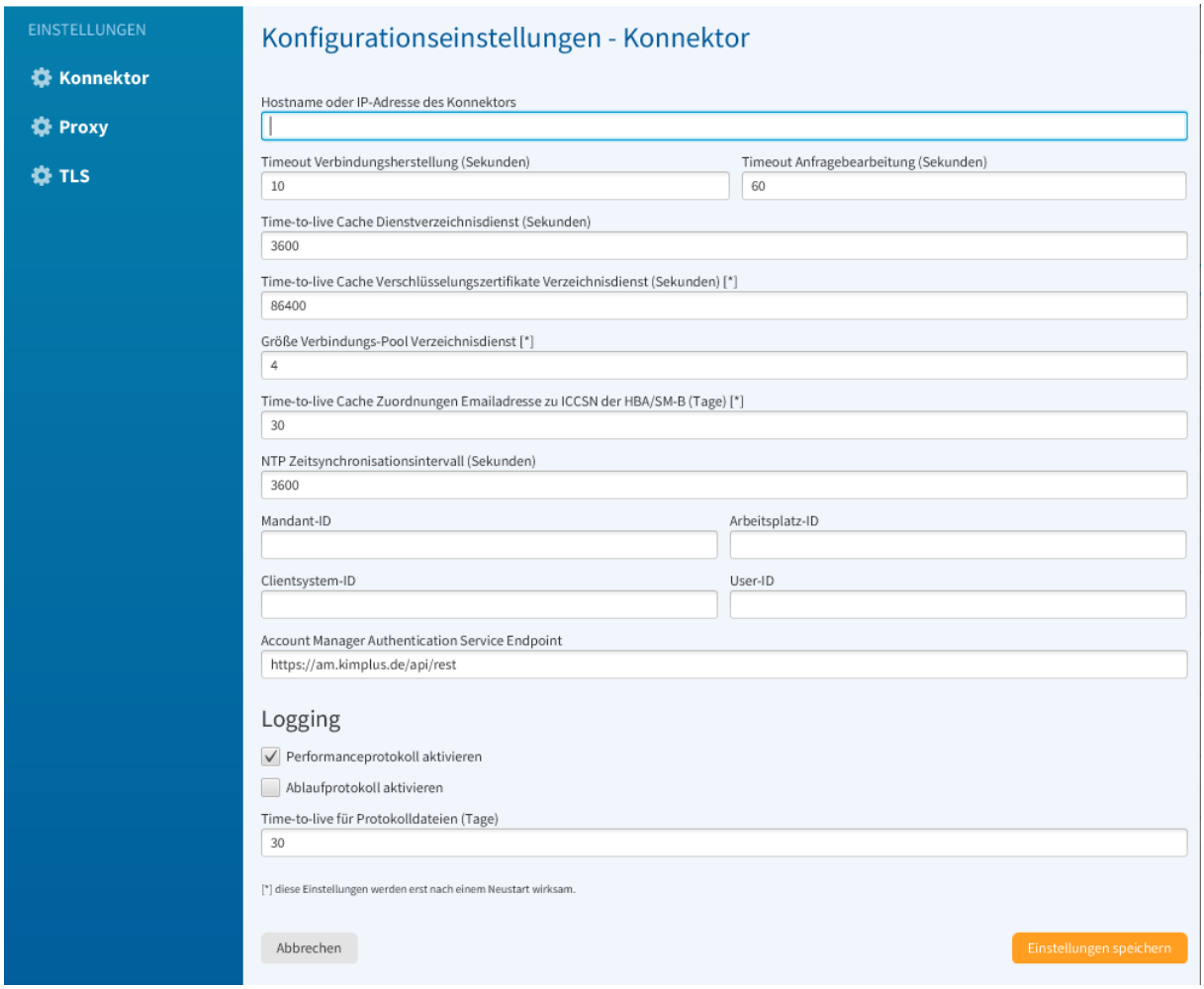



**Abbildung 13: Konfigurationseinstellungen – Standardkonnektor**

| Name | Beschreibung | default | Wertebereich | Neustart nötig |
|---|---|---|---|---|
| Hostname oder IP-Adresse des Konnektors | URI des DVD des Konnektors (z. B. "https://192.168.1.46/connector.sds"), Angabe verpflichtend | - | | Nein |
| Timeout Verbindungsherstellung | Timeout für die Herstellung der Verbindung mit dem Konnektor (in Sekunden) | 10 | 1-86400 | Nein |
| Timeout Anfragebearbeitung | Timeout für Anfragen an den Konnektor (in Sekunden) | 60 | 1-86400 | Nein |

| Name | Beschreibung | default | Wertebereich | Neustart nötig |
|---|---|---|---|---|
| Time-to-live Cache Dienstverzeichnisdienst | Maximale Time to Live für gecachte Serviceendpunktinformationen des Dienstverzeichnisdiensts (in Sekunden) | 3600 | 1-86400 | Nein |
| Time-to-live Cache Verschlüsselungszertifikate Verzeichnisdienst | Maximale Time to Live für gecachte Verschlüsselungszertifikate vom Verzeichnisdienst (in Sekunden) | 86400 | 1-86400 | Ja |
| Größe Verbindungs-Pool Verzeichnisdienst | Größe des Verbindungs-Pools für den Verzeichnisdienst | 4 | 1-20 | Ja |
| Time-to-live Cache Zuordnungen Emailadresse zu ICCSN der HBA/SM-B | Maximale Time to Live für gecachte Zuordnungen von E-Mail-Adressen der Sender bzw. Empfänger zu ICCSNs von deren HBAs/SM-Bs (in Tagen) | 30 | 1-60 | Ja |
| NTP Zeitsynchronisationsintervall | Aktualisierungsintervall für NTP-Synchronisation mit dem Konnektor (in Sekunden) | 3600 | 1-86400 | Nein |
| Mandant-ID | Mandant-ID des Kontexts für den Konnektor | - | | Nein |
| Arbeitsplatz-ID | Arbeitsplatz-ID des Kontexts für den Konnektor | - | | Nein |
| Clientsystem-ID | Clientsystem-ID des Kontexts für den Konnektor | - | | Nein |
| User-ID | User-ID des Kontexts für den Konnektor | - | | Nein |
| Account Manager Authentication Service Endpoint | URI Endpoint des Account Managers | https://am.kimplus.de/api/rest | | Nein |
| Logging - Performanceprotokoll aktivieren | Protokollierung von Performanceinformationen | JA | JA, NEIN | Nein |

| Name | Beschreibung | default | Wertebe-reich | Neu-start nötig |
|---|---|---|---|---|
| Logging - Ablaufprotokoll aktivieren | Protokollierung von Ablaufinfor-mationen | NEIN | JA, NEIN | Nein |
| Logging - Time-to-live für Protokolldateien | Maximale Time to Live für alle Protokolldateien (in Tagen) | 30 | 1-300 | Nein |

**Tabelle 5: Konfigurationseinstellungen - Konnektor**

#### 4.3.2.3 Konfigurationseinstellungen Proxy

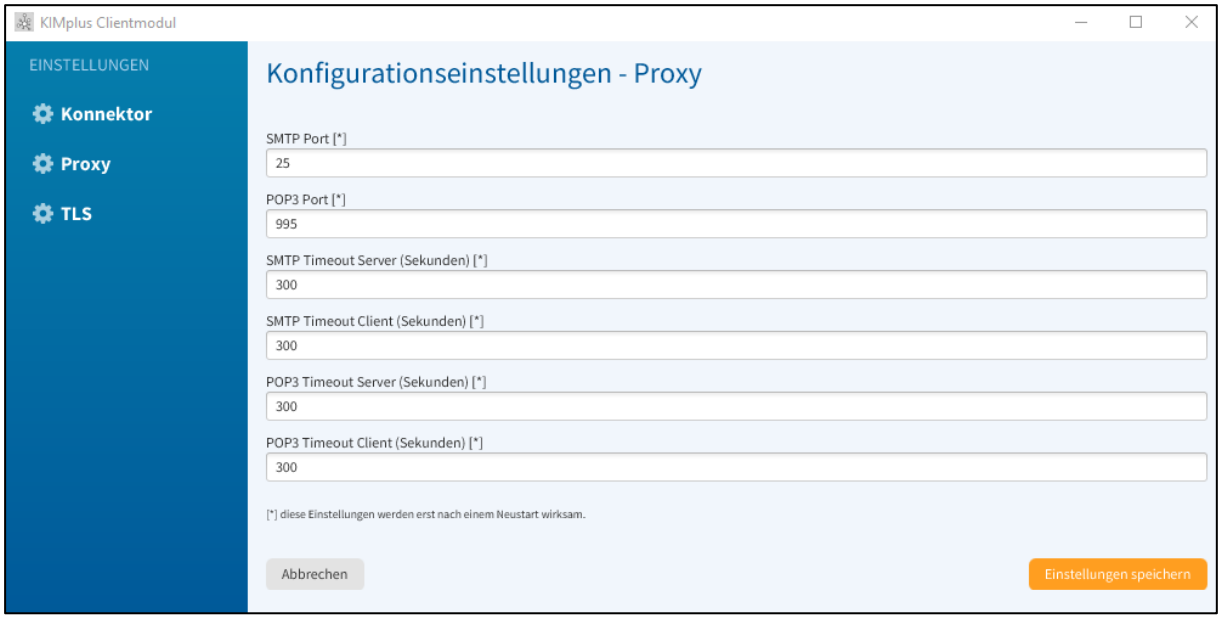



**Abbildung 14: Konfigurationseinstellungen - Proxy**

| Name | Beschreibung | default | Wertebereich | Neustart erforder-lich |
|---|---|---|---|---|
| SMTP Port* | SMTP-Port für Clientsysteme | 25 | 1-65535 | Ja |
| POP3 Port* | POP3-Port für Clientsysteme | 995 | 1-65535 | Ja |

| Name | Beschreibung | default | Wertebereich | Neustart erforder-lich |
|---|---|---|---|---|
| SMTP Timeout Server | Timeout für Antworten vom SMTP-Server auf SMTP-Kommandos (in Sekunden) | 300 | 1-86400 | Ja |
| SMTP Timeout Client | Timeout für das Warten auf neue SMTP-Kommandos vom Client-system (in Sekunden) | 300 | 1-86400 | Ja |
| POP3 Timeout Sever | Timeout für Antworten vom POP3-Server auf POP3-Kommandos (in Sekunden) | 300 | 1-86400 | Ja |
| POP3 Timeout Client | Timeout für das Warten auf neue POP3-Kommandos vom Client-system (in Sekunden) | 300 | 1-86400 | Ja |

**Tabelle 6: Konfigurationseinstellungen – Proxy**

* für Unix-Systeme (Linux, MacOS) muss hier ein Wert ab 1024 verwendet werden. Ports bis 1023 sind nur mit administrativen Rechten verfügbar.

#### 4.3.2.4 Konfigurationseinstellungen TLS

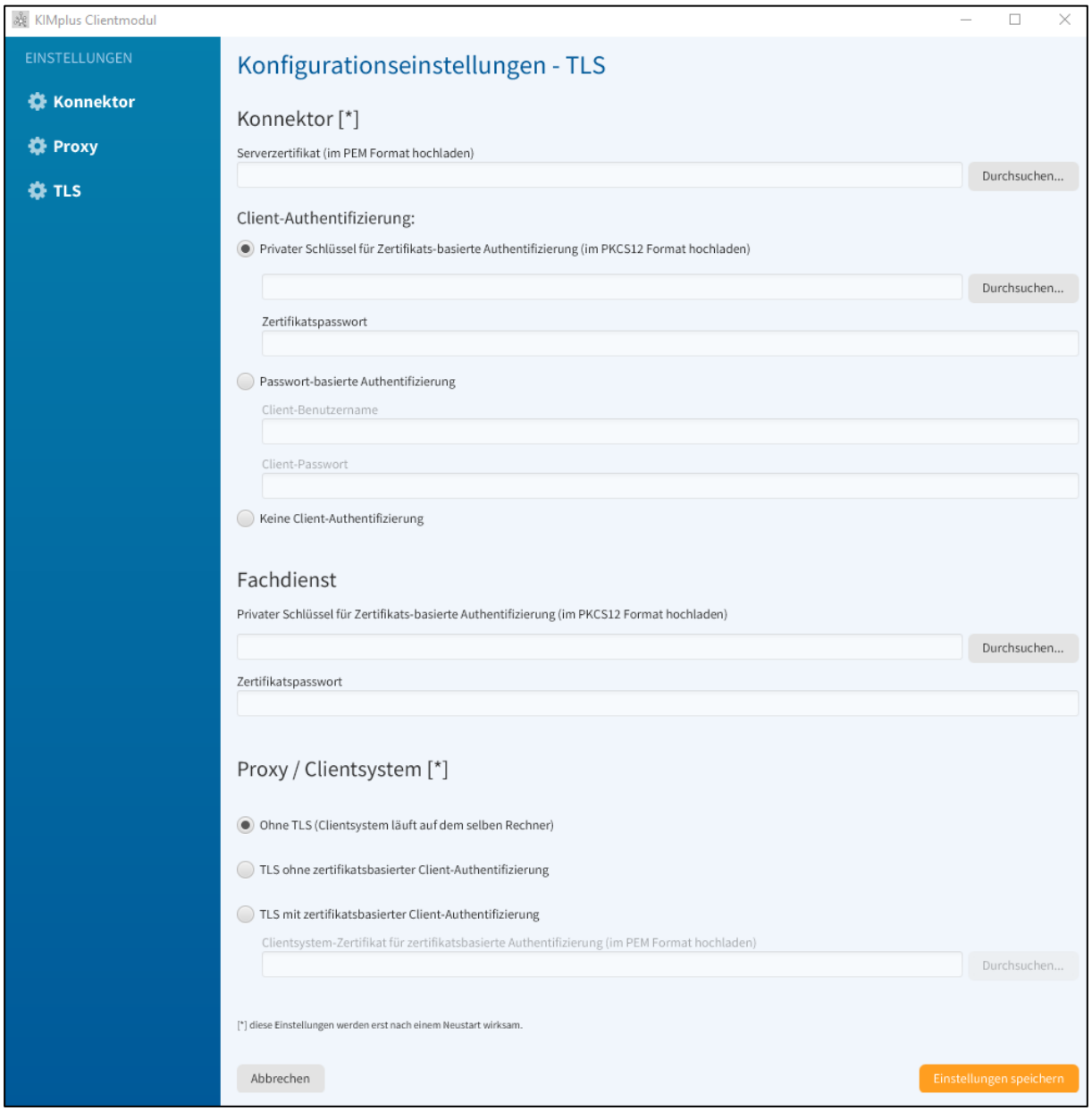



**Abbildung 15: Konfigurationseinstellungen - TLS**

Mehr Informationen zu den verwendeten TLS Zertifikaten finden Sie im Kapitel 2.6.

| Name | Beschreibung | default | Wertebereich | Neustart erforderlich |
|---|---|---|---|---|
| Konnektor - Serverzertifikat | Auswahl einer lokal verfügbaren PEM Datei mit dem Server-Zertifikat des Konnektors | | | Ja |
| Konnektor - Client-Authentifizierung | Art der Authentifizierung des Clientmoduls gegenüber dem Konnektor bei aktivierter TLS-Verbindung | zertifikatsbasiert | zertifikatsbasiert, passwortbasiert, ohne Authentifizierung | Ja |
| Konnektor - zertifikatsbasierte Client-Authentifizierung | Bei ausgewählter zertifikatsbasierter Client-Authentifizierung zum Konnektor: Auswahl einer lokal verfügbaren passwortgeschützten PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel | | | Ja |
| Konnektor - passwortbasierte Client-Authentifizierung | Bei ausgewählter passwortbasierter Client-Authentifizierung zum Konnektor: Eingabe von Benutzername und Passwort | | | Ja |
| Fachdienst - Clientzertifikat | Auswahl einer lokal verfügbaren passwortgeschützten PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel für die erforderliche zertifikatsbasierte Client-Authentifizierung zum Fachdienst | | | Ja |
| Clientsystem - Client-Authentifizierung | Authentifizierung des Clientsystems gegenüber dem Clientmodul (Proxy) | Ohne aktivierte TLS-Verbindung | ohne aktivierte TLS-Verbindung, TLS zertifikatsbasiert, TLS ohne Client-Authentifizierung | Ja |
| Clientsystem - zertifikatsbasierte Client-Authentifizierung | Bei ausgewählter zertifikatsbasierter Client-Authentifizierung zum Clientmodul: Auswahl einer lokal verfügbaren PEM Datei mit dem Client-Zertifikat des Clientsystems | | | Ja |

**Tabelle 7: Konfigurationseinstellungen - TLS**

#### 4.3.2.5 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 Installation unter Windows (siehe Abschnitt 4.3.1 Installation) 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 100.102.8.6 MASK 255.255.255.255 <IP des Konnektors> METRIC 1
```

eingeben.

**Statische Routen in Mac eintragen (nicht permanent):**

Im Terminal den Befehl

```
sudo route add -net 100.102.8.6 -netmask 255.255.255.255 <IP des Konnektors>
```

eingeben.

**Statische Routen in Mac eintragen (permanent):**

Im Terminal den Befehl

```
sudo networksetup -setadditionalroutes "<Netzwerkschnittstelle>" 10.30.8.6 255.255.255.255 <IP des Konnektors>
```

eingeben.

Zur Auflistung der Netzwerkschnittstellen kann der Befehl

```
networksetup -listnetworkserviceorder
```

verwendet werden.

**Statische Routen in Linux eintragen:**

Im Terminal den Befehl

```
sudo ip route add 100.102.8.6/24 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.

## 4.4 Clientmodul als Dienst

### 4.4.1 Installation als Dienst

Die Installation des Clientmoduls als Dienst ist nur durch einen Administrator möglich, da Administratorrechte notwendig sind. Das Clientmodul als Dienst arbeitet als Mail-Proxy, übernimmt aber keine Authentifizierung des Benutzers mittels Karte (HBA oder SMCB). Dafür muss der Auth-Client des kim+ Clientmoduls als eigene Applikation installiert werden (siehe dazu Abschnitt 4.2). Dieser steht nicht als Dienst zur Verfügung, kann aber auch auf einem separaten System (als dem Dienst-Client-System) installiert werden.

Das kim+ Clientmodul wird über die folgenden Schritte als Dienst installiert (mit Benutzerinteraktion):

1. Vor der Installation des kim+ Clientmodul als Dienst müssen alle Systemanforderungen überprüft und die Betriebsumgebung entsprechend vorbereitet werden.
2. Herunterladen des Installationspakets.
3. Der installierende Benutzer muss die Signatur des Installationspaketes prüfen.
4. Ausführung des Installationspakets, um den Installationsvorgang zu starten.
    a. Installation als Dienst:
        - **Mail Proxy:** Der kim+ Clientmodul Dienst unterstützt nur die Aktivierung des Mail Proxys. Eine Aktivierung des Auth Clients ist nicht möglich.
        - **Statische Route:** Das automatische Setzen einer statischen Route über den Konnektor zum Fachdienst wird bei der Installation des kim+ Clientmodul Diensts nicht unterstützt.
5. Die Installation des kim+ Clientmodul Diensts erfolgt, abhängig vom Betriebssystem, im Standardordner.

### 4.4.2 Unbeaufsichtigte Installation

Die Installation kann auch ohne Benutzerinteraktion durchgeführt werden, indem alle notwendigen Einstellungen beim Starten übergeben werden. Alle Einstellungen werden über Kommandozeilenoptionen und eine Responsedatei (Steuerungsdatei) getroffen.

#### 4.4.2.1 Kommandozeilenoptionen

Es stehen die folgenden Kommandozeilenoptionen zur Verfügung:

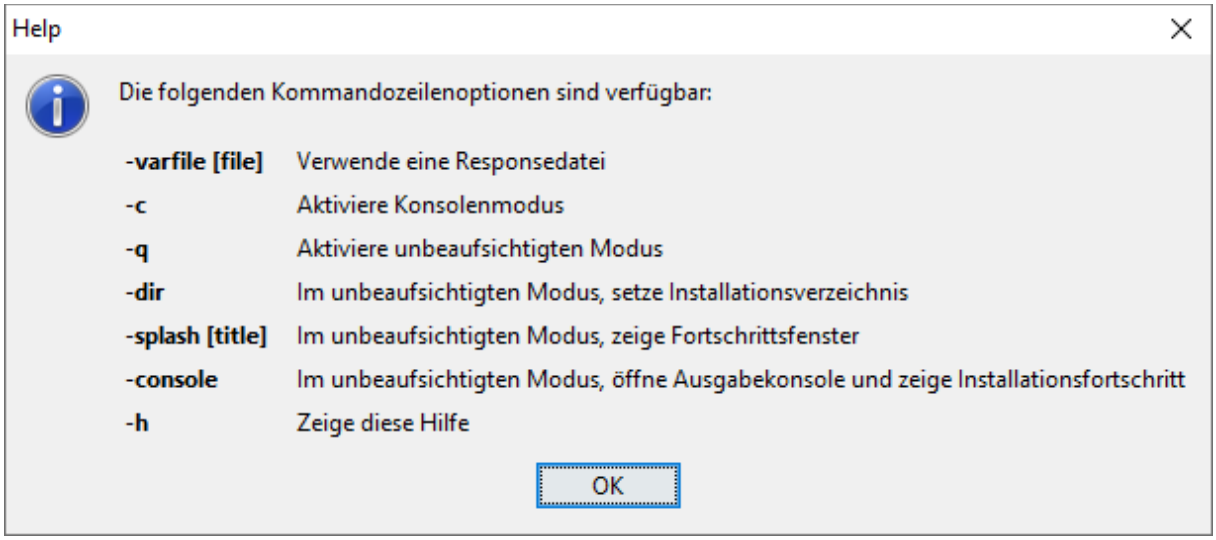



**Abbildung 16: unbeaufsichtigte Installation - Kommandozeilenoptionen**

#### 4.4.2.2 Responsedatei

Die Responsedatei beinhaltet pro Zeile einen Attributnamen und einen Wert für dieses Attribut. Die möglichen Attribute sind in der folgenden Tabelle beschrieben.

**Responsedatei**

| Attribut | Beschreibung | Werte | Anmerkung |
|---|---|---|---|
| `executeLauncherAction` | Start der Applikation nach Abschluss der Installation | true/false (default: false) | |
| `initialConfig` | Pfadangabe einer Clientmodul Konfigurationsdatei, welche zur Initialisierung herangezogen wird. | text | Bei einer bestehenden Installation werden neue Eigenschaften hinzugefügt und bestehende überschrieben |
| `initialConfigRelative` | Bestimmt, ob die Pfadangabe relativ zum Installer-Pfad aufgelöst wird oder absolut | true/false (default: true) | |

**Anmerkung**: Die Anführung der Attribute als Kommandozeilenoptionen bei der Ausführung der Installation (z. B. installer -VinitialConfig="Pfad/zur/Datei") wird aufgrund von Fehlinterpretationen seitens der Betriebssysteme nicht unterstützt.

#### 4.4.2.3 Beispiel einer unbeaufsichtigten Installation unter Windows

Bei diesem Beispiel wird eine Responsedatei zur Steuerung der Installation und eine initiale Clientmodul Konfigurationsdatei für den zu installierenden Clientmodul Dienst verwendet. Die Installation wird im unbeaufsichtigten Modus gestartet.

**Verzeichnisinhalt**

```
C:\install>dir /b

cm.properties

installer.exe

response.varfile
```

**Inhalt der `cm.properties` Datei**

```
C:\install>more cm.properties

#Fri Oct 9 08:25:16 CEST 2020
clientmodul.proxy.smtp.port=465
clientmodul.proxy.pop3.port=965
```

**Inhalt der `response.varfile` Datei**

```
C:\install>more response.varfile

# install4j response file for Clientmodul service

# Startet den Clientmodul Dienst nach der Installation
executeLauncherAction$Boolean=true

# Initiale cm.properties Datei
initialConfig=cm.properties

# Pfadangabe des initialConfig ist relativ zum Installer
initialConfigRelative$Boolean=true
```

**Aufruf der Installation**

```
C:\install>installer -q -console -varfile response.varfile

C:\install>Preparing JRE ...

Das Installationsverzeichnis wurde auf C:\Program Files\kimplus-clientmodul-servic
e gesetzt.

Deinstalliere vorherige Version

Dateien werden ausgepackt ...

Installation wird beendet ...
```

### 4.4.3 Installation im Konsolenmodus

Die Installation des Clientmodul Diensts über die Konsole kann mit der Kommandozeilenoption `-c` gestartet werden. Der Installationsfortschritt wird in der Konsole ausgegeben und die Installationsoptionen werden über die Konsole vom Installer abgefragt. Abhängig von den Benutzereingaben werden die jeweiligen Optionen installiert.

#### 4.4.3.1 Beispiel einer Konsolenmodus-Installation unter Windows

In diesem Beispiel wird der Clientmodul Dienst über den Konsolenmodus installiert. Alle Benutzereingaben wurden aus Verständlichkeitsgründen mit `#Benutzereingaben` gekennzeichnet.

**Aufruf der Installation**

```
C:\install>installer -c

C:\install>Preparing JRE ...

Der Setup-Assistent wird KIMplus Clientmodul Dienst auf Ihren Computer installiere
n.
OK [o, Eingabe], Abbrechen [c]
o #Benutzereingaben

Klicken Sie auf "Weiter", um fortzufahren oder auf "Abbrechen", um den
Assistenten zu verlassen.
Eingabe #Benutzereingaben

Bitte geben Sie an, in welchen Ordner Sie KIMplus Clientmodul Dienst installieren
wollen, und klicken Sie danach auf "Weiter".
Wohin soll KIMplus Clientmodul Dienst installiert werden?
[C:\Program Files\kimplus-clientmodul-service]
Eingabe #Benutzereingaben (Standardverzeichnis bestätigen)

Dateien werden ausgepackt ...
Setup hat die Installation von KIMplus Clientmodul Dienst auf Ihren Computer abges
chlossen.

KIMplus Clientmodul Dienst starten?
Ja [y, Eingabe], Nein [n]
y #Benutzereingaben
```

### 4.4.4 Inbetriebnahme des Dienstes

Bei der ersten Inbetriebnahme des kim+ Clientmodul Diensts müssen grundlegende Einstellungen vorgenommen werden, bevor der Dienst verwendet werden kann. Der Clientmodul Dienst besitzt keine grafische Benutzeroberfläche. Die Einstellungen müssen deshalb über eine Konfigurationsdatei und mit dem Keytool eingespielt werden. Vor der Installation und Inbetriebnahme müssen entsprechende Zertifikate und Schlüsselmaterial lokal vorhanden sein, die für den Betrieb notwendig sind. Dabei muss der Nutzer sicherstellen, dass nur vertrauenswürdige Zertifikate und Schlüssel in die Komponenten eingebracht werden.

Auf der anderen Seite muss der KIM-Anbieter ein TLS-Client-Zertifikat (C.CM.TLS-CS für die TLS-Kommunikation mit dem Fachdienst) und TLS-Server-Zertifikat (für die Kommunikation mit den Clientsystem) aus der Komponenten-PKI der TI über einen beidseitig authentisierten Kanal unter Wahrung der Vertraulichkeit und Integrität zur Verfügung stellen, die in das Clientmodul eingebracht

werden. Dies gilt sowohl initial für die Ersteinrichtung als auch periodisch vor Ablauf des jeweils aktuell verwendeten Zertifikats.

Im Kapitel 4.4.5 werden die zur Verfügung stehenden Konfigurationsparameter und Konfigurationsmethoden erklärt. Sollte bereits eine Konfigurationsdatei (cm.properties) einer vorherigen kim+ Clientmodul-Installation existieren, kann diese in Kopie für den Dienst verwendet werden.

Führen Sie die nachfolgenden Schritte durch, um den Clientmodul Dienst zu aktivieren:

1. Durchführung der notwendigen Konfigurationen über die Konfigurationsdatei:
    - Hostname oder IP-Adresse des Konnektors, der für die NTP-Synchronisation und die Zertifikatsprüfung beim Verbindungsaufbau zum Fachdienst benutzt wird.
    - Karten-Kontext für die Zertifikatsprüfung, bestehend aus
        - Mandant-ID des Kontexts für den Konnektor
        - Arbeitsplatz-ID des Kontexts für den Konnektor
        - Clientsystem-ID des Kontexts für den Konnektor
        - User-ID des Kontexts für den Konnektor (nur für HBA) (falls vorhanden für Zertifikatsprüfung und Auth Client)
    - Setzen der zu verwendenden Art der Client-Authentifizierung zum Konnektor: zertifikatsbasierte Authentifizierung, passwortbasierte Authentifizierung oder keine Client-Authentifizierung
    - Setzen der zu verwendenden Art der Client-Authentifizierung vom Clientsystem: ohne TLS, TLS mit zertifikatsbasierter Client-Authentifizierung oder TLS ohne zertifikatsbasierter Client-Authentifizierung.
2. Konfigurationen über das Keytool
    - Voraussetzung für das Keytool ist die Installation von Java 11 auf dem System
    - Einspielen des Server-Zertifikats des Konnektors
    - Client-Authentifizierung zum Konnektor: zertifikatsbasierte Authentifizierung, passwortbasierte Authentifizierung oder keine Client-Authentifizierung
        - Bei zertifikatsbasierter Authentifizierung zum Konnektor: Einspielen einer lokal verfügbaren PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel sowie Eingabe des Passworts.
        - Bei passwortbasierter Authentifizierung: Einspielen des Benutzernamen und Passworts.
    - Einspielen einer lokal verfügbaren, passwortgeschützten PKCS#12 Datei mit dem Zertifikat und privaten Schlüssel für die zertifikatsbasierte Client-Authentifizierung zum Fachdienst sowie Eingabe des Passworts. Die Kommunikation zwischen Clientmodul und Fachdienst findet ausschließlich verschlüsselt statt und ist daher ohne eine valide PKCS#12 Datei nicht möglich. Wird trotzdem versucht eine Verbindung aufzubauen, wird folgender Fehler in die `operations` Logdatei geschrieben: *GENERAL_CM_ERROR: Client certificates were not imported.*

- Client-Authentifizierung vom Clientsystem: ohne TLS, TLS mit zertifikatsbasierter Client-Authentifizierung oder TLS ohne zertifikatsbasierter Client-Authentifizierung.
  - Bei ausgewählter zertifikatsbasierter Client-Authentifizierung vom Clientsystem: Einspielen einer lokal verfügbaren PEM Datei mit dem Client-Zertifikat des Clientsystems.

3. Nach erfolgreicher Konfiguration muss der kim+ Clientmodul Dienst im Service Manager aufgesucht und neu gestartet werden.

## 4.4.5 Konfiguration des Dienstes

### 4.4.5.1 Konfiguration über Konfigurationsdatei

Die Konfigurationsdatei befindet sich im Applikationsverzeichnis des Clientmoduls `kimCm` im Windows-Verzeichnis unter `C:\Windows\System32\config\systemprofile\kimCm\cm.properties`. Die notwendigen Parameter finden Sie in Tabelle 4.

### 4.4.5.2 Konfiguration über Keytool

Neben der Konfiguration über die Konfigurationsdatei des kim+ Clientmodul Diensts müssen über das Keytool die TLS-Zertifikate, Schlüssel und Passwörter verwaltet und konfiguriert werden.

Initial wird der KIM Clientmodul Dienst mit einer Default-Konfiguration und ohne Zertifikate ausgeliefert. Die Konfiguration kann mittels der Konfigurationsdatei `cm.properties` angepasst werden. Die Zertifikate, private Schlüssel und Passwörter, die im Keystore bzw. Truststore gespeichert sind, müssen mit dem Keytool verwaltet werden:

- Import und Entfernung von Zertifikaten im Truststore
- Import und Entfernung von Private Keys im Keystore
- Import und Entfernung von Credentials im Keystore
- Auflisten der enthaltenen Daten vom Keystore und Truststore

Die jeweiligen Aliase können dabei gesetzt werden. Für den Truststore sind diese frei wählbar, für den Keystore werden sie entsprechend der Verwendung des Schlüssels automatisch generiert.

Das Keytool befindet sich im Installationsverzeichnis des Clientmoduls unter `keytool/bin/keytool.bat` (z.B `C:\Program Files\kimplus-clientmodul-service\keytool\bin\keytool.bat`).

Das Tool bietet die folgenden Sub-Commands, mit denen die jeweiligen Operationen ausgeführt werden können. Außerdem bietet es eine Usage Beschreibung:

**Verwendung von Keytool**

```
Usage: KeyTool [COMMAND]
This tool manages certificates and keys for the clientmodul
Commands:
  add-certificate         Adds a trusted certificate to the TrustStore
  add-client-keypair      Adds a private key for the clientmodul to the KeyStore
  add-client-password     Adds a client username and password for the
                            clientmodul to the KeyStore
  list-truststore         Lists stored certificates in the TrustStore
```

```
  list-keystore           Lists stored certificates in the KeyStore
  remove-certificate      Removes a trusted certificate from the TrustStore
  remove-client-keypair   Removes a client authentication private key from the
                            clientmodul KeyStore
  remove-client-password  Removes a client authentication username and password
                            from the clientmodul KeyStore
  help                    Displays help information about the specified command
```

Benutzernamen (Username) oder Passwörter (Password) werden nicht direkt als Parameter mit übergeben, sondern werden in einer eigenen "Prompt" abgefragt, um sie sicher eingeben zu können und damit sie nicht in der "History" erscheinen. Der jeweilige Parameter muss beim Aufruf gesetzt werden. Falls ein Sub-Command einen Partner-Type benötigt, muss die Eingabe einer Gegenstelle entsprechen, mit dem sich das Clientmodul verbindet. Mögliche Werte sind:

- "KON" (= der Konnektor)
- "FD" (= der Fachdienst)
- "CLIENT" (= das Clientsystem).

**Hinweis:** Das Keytool sollte mit Administratorrechten ausgeführt werden. Ansonsten können Passwörter für Key- und Truststores, die nicht als Administrator generiert wurden, im laufenden Betrieb nicht mehr hergestellt werden.

**Hinweis:** Das Keytool muss zur Konfiguration des Clientmoduls als Dienst über die CLI gestartet werden, um Fehler zu vermeiden.

#### 4.4.5.3 Sub-Command add-certificate ausführen

Mit diesem Sub-Command werden vertrauenswürdige Zertifikate in den Truststore importiert.

**Verwendung von** `add-certificate`

```
Usage: KeyTool add-certificate -a=<alias> -t=<trustStorePath> <cert file>
Adds a trusted certificate to the TrustStore
      <cert file>       The certificate file to import
  -a, --alias=<alias>   The alias under which the certificate is stored
  -t, --trust-store=<trustStorePath>
                        The TrustStore file in which the cert file is imported
```

Ein Beispielaufruf zum Hinzufügen eines Zertifikates:

**Beispielaufruf von** `add-certificate` **für das Konnektor-Zertifikat**

```
keytool.bat add-certificate -t C:\Windows\System32\config\systemprofile\kimCm\trus
tStore -a KON C:\Users\User\Desktop\konnektor.pem
```

#### 4.4.5.4 Sub-Command add-client-keypair ausführen

Mit diesem Sub-Command wird ein Private-Key in den Keystore importiert, mit dem sich das Clientmodul authentifiziert.

**Verwendung von** `add-client-keypair`

```
Usage: KeyTool add-client-keypair -p -k=<keyStorePath> -o=<partnerType>
                                  <private key file>
Adds a private key for the clientmodul to the KeyStore
      <private key file>   The private key file to import
```

```
  -k, --key-store=<keyStorePath>
                           The KeyStore file in which the client private key is
                             stored
  -o, --other-partner=<partnerType>
                           The partner identifier for which the client private
                             key file is added. This parameter is used to
                             generate the alias, the correct suffix
                             (_CERTIFICATE-pk) is automatically added.
  -p, --private-key-password
                           The password for the provided private key file.
```

Ein Beispielaufruf zum Hinzufügen eines Private-Key (Anmerkung: das Passwort vom Private-Key wird gesondert abgefragt):

**Beispielaufruf von `add-client-keypair` für das Clientmodul-Zertifikat**

```
keytool.bat add-client-keypair -k C:\Windows\System32\config\systemprofile\kimCm\k
eyStore -o FD -p C:\Users\User\Desktop\cm-fd.rsa.valid.p12
```

**Beispielaufruf von `add-client-keypair` für das Konnektor Client-Zertifikat**

```
keytool.bat add-client-keypair -k C:\Windows\System32\config\systemprofile\kimCm\k
eyStore -o KON -p C:\Users\User\Desktop\c.p12
```

**Beispielaufruf von `add-client-keypair` für das Clientmodul Client-Zertifikat**

```
keytool.bat add-client-keypair -k C:\Windows\System32\config\systemprofile\kimCm\k
eyStore -o CLIENT C:\Users\User\Desktop\eigeneszertifikat.pem
```

#### 4.4.5.5 Sub-Command add-client-password ausführen

Mit diesem Sub-Command wird ein Username und ein Passwort in den Keystore importiert, mit dem sich das Clientmodul authentifiziert.

**Verwendung von `add-client-password`**

```
Usage: KeyTool add-client-password -p -u -k=<keyStorePath> -o=<partnerType>
Adds a client username and password for the clientmodul to the KeyStore
  -k, --key-store=<keyStorePath>
                   The KeyStore file in which the credentials are stored
  -o, --other-partner=<partnerType>
                   The partner identifier for which the credentials are added.
                     This parameter is used to generate the alias, the correct
                     suffixes (_PASSWORD-cred$u and _PASSWORD-cred$p) are
                     automatically added.
  -p, --password   The password for authentication.
  -u, --username   The username for authentication.
```

Ein Beispielaufruf zum Hinzufügen eines Usernamens und Passworts (Anmerkung: der Username und das Passwort werden gesondert abgefragt):

**Beispielaufruf von `add-client-password` für Konnektor Client-Authentifizierung**

```
keytool.bat add-client-password -k C:\Windows\System32\config\systemprofile\kimCm
\keyStore -o KON -u -p
```

#### 4.4.5.6 Sub_Command list-truststore ausführen

Mit diesem Sub-Command werden alle enthaltenen Zertifikate im Truststore gelistet, denen vertraut wird.

**Verwendung von** `list-truststore`

```
Usage: KeyTool list-truststore -t=<trustStorePath>
Lists stored certificates in the TrustStore
  -t, --trust-store=<trustStorePath>
          The TrustStore file whose content is listed
```

Ein Beispielaufruf zum Auflisten aller Zertifikate im Truststore:

**Beispielaufruf von** `list-truststore`

```
keytool.bat list-truststore -t C:\Windows\System32\config\systemprofile\kimCm\trus
tStore
```

#### 4.4.5.7 Sub-Command list-keystore ausführen

Mit diesem Sub-Command werden alle enthaltenen Private-Keys, Usernamen und Passwörter (jeweils nicht im Klartext) im Keystore gelistet.

**Verwendung von** `list-keystore`

```
Usage: KeyTool list-keystore -k=<keyStorePath>
Lists stored certificates in the KeyStore
  -k, --key-store=<keyStorePath>
          The KeyStore file whose content is listed
```

Ein Beispielaufruf zum Auflisten aller Private-Keys, Usernamen und Passwörter im Keystore:

**Beispielaufruf von** `list-keystore`

```
keytool.bat list-keystore -k C:\Windows\System32\config\systemprofile\kimCm\keySto
re
```

#### 4.4.5.8 Sub-Command remove-certificate ausführen

Mit diesem Sub-Command wird ein vertrauenswürdiges Zertifikat aus dem Truststore entfernt.

**Verwendung von** `remove-certificate`

```
Usage: KeyTool remove-certificate -a=<alias> -t=<trustStorePath>
Removes a trusted certificate from the TrustStore
  -a, --alias=<alias>   The alias which should be deleted
  -t, --trust-store=<trustStorePath>
                        The TrustStore file from which the certificate is
                          deleted
```

Ein Beispielaufruf zum Entfernen eines Zertifikates:

**Beispielaufruf von** `remove-certificate`

```
keytool.bat remove-certificate -t C:\Windows\System32\config\systemprofile\kimCm\t
rustStore -a KON
```

#### 4.4.5.9 Sub-Command remove-client-keypair ausführen

Mit diesem Sub-Command wird ein Private-Key aus dem Keystore entfernt.

**Verwendung von** `remove-client-keypair`

```
Usage: KeyTool remove-client-keypair -k=<keyStorePath> -o=<partnerType>
Removes a client authentication private key from the clientmodul KeyStore
  -k, --key-store=<keyStorePath>
        The KeyStore file from which the client authentication is deleted
  -o, --other-partner=<partnerType>
        The partner identifier for which the client auth certificate is
          deleted. This parameter is used to generate the alias, the correct
          suffix (_CERTIFICATE-pk) is automatically added.
```

Ein Beispielaufruf zum Entfernen eines Private-Keys:

**Beispielaufruf von** `remove-client-keypair`

```
keytool.bat remove-client-keypair -k C:\Windows\System32\config\systemprofile\kimC
m\keyStore -o FD
```

#### 4.4.5.10 Sub-Command remove-client-password ausführen

Mit diesem Sub-Command wird ein Username und Password aus dem Keystore entfernt.

**Verwendung von** `remove-client-keypair`

```
Usage: KeyTool remove-client-password -k=<keyStorePath> -o=<partnerType>
Removes a client authentication username and password from the clientmodul
KeyStore
  -k, --key-store=<keyStorePath>
        The KeyStore file from which the client authentication is deleted
  -o, --other-partner=<partnerType>
        The partner identifier for which the client auth credentials is
          deleted. This parameter is used to generate the aliases, the correct
          suffixes (_PASSWORD-cred$u and _PASSWORD-cred$p) are automatically
          added and both entries are deleted.
```

Ein Beispielaufruf zum Entfernen eines Usernamens und Passwortes:

**Beispielaufruf von** `remove-client-keypair`

```
keytool.bat remove-client-password -k C:\Windows\System32\config\systemprofile\kim
Cm\keyStore -o FD
```

## 4.5 Konfiguration des E-Mail-Clients oder des Clientsystems

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 sind im jeweiligen Unterkapitel angegeben.

### 4.5.1 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 17: Aufbau POP3 Benutzername<br>Beispiel:<br>`erik.mustermann@mail.kim.telematik#100.102.8.6:995#Mandant1#ClientID1#Workplace1#UserID1` |
| Authentifizierung | abhängig von den Einstellungen im Clientmodul |
| Verbindungssicherheit | abhängig von den Einstellungen im Clientmodul |

**Tabelle 8: Konfiguration Mail Client E-Mail-Empfang**

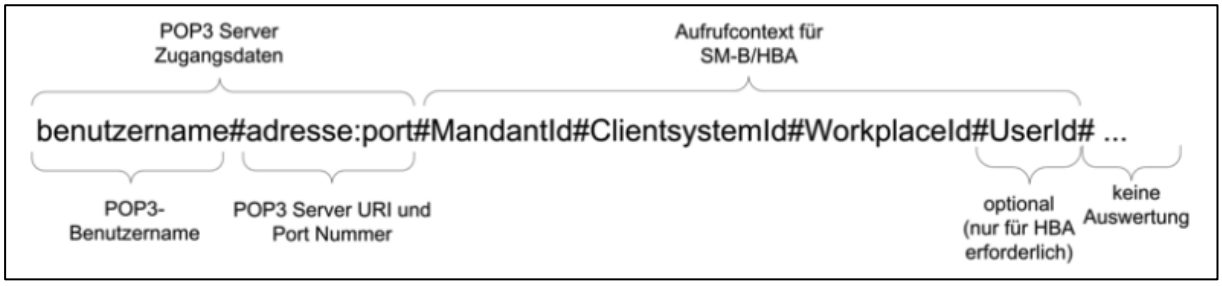



**Abbildung 17: Aufbau POP3 Benutzername**

**Empfehlung:**

Sie können das Intervall, um Ihre kim+-E-Mails abzurufen, frei wählen. Arvato empfiehlt eine Einstellung von mindestens 5 Minuten.

### 4.5.2 E-Mail-Versand

| Einstellung | Wert |
|---|---|
| Servertyp | SMTP |
| Server | `localhost` |
| Port | Einstellung wie in Clientmodul (SMTP Port) |
| Benutzername | Siehe Abbildung 18: Aufbau SMTP Benutzername |

| Einstellung | Wert |
|---|---|
| | Beispiel:<br>`erik.mustermann@mail.kim.telema-tik#100.102.8.6:465#Mandant1#ClientID1#Work-place1` |
| Authentifizierung | abhängig von den Einstellungen im Clientmodul |
| Verbindungssicherheit | abhängig von den Einstellungen im Clientmodul |
| 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.<br>Parameter: mailnews.tcptimeout<br>Standardwert: 100 Sek.<br>Erhöhung z. B. auf 300 Sek. testen |

**Tabelle 9: Konfiguration E-Mail-Client E-Mail-Versand**

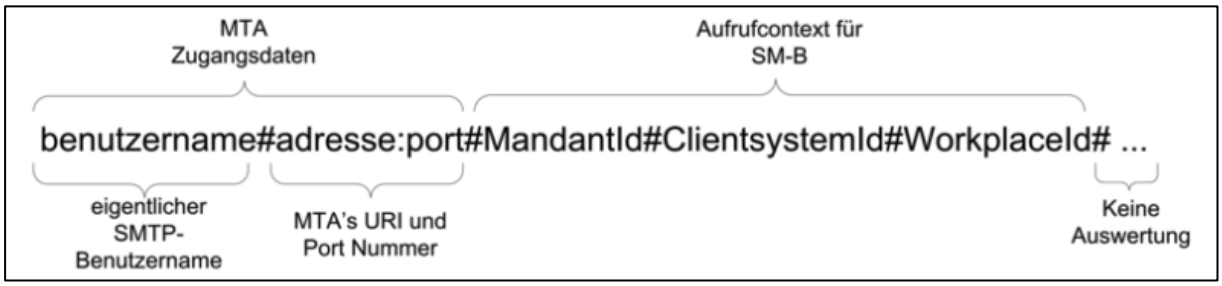



**Abbildung 18: Aufbau SMTP Benutzername**

### 4.5.3 Einrichtung des Adressbuchs im E-Mail-Client oder im Clientsystem

Um im E-Mail-Client nach Teilnehmern anhand von Name oder E-Mail-Adresse suchen zu können, ist es erforderlich das Adressbuch zu konfigurieren. Ein TI-Konnektor bietet die Möglichkeit, die Inhalte des Verzeichnisdienstes (VZD) als LDAP-Verzeichnisdienst verfügbar zu machen. Der Verzeichnisdienst speichert alle TI-Teilnehmer mit ihren Basisdaten (Name, Anschrift) kim+-E-Mail-Adressen (nachdem sich die Teilnehmer für eine kim+-E-Mail-Adresse registriert haben).

Nachfolgend ist die Einrichtung des Verzeichnisdiensts beispielhaft im Adressbuch von Thunderbird erläutert.

Um die Einrichtung zu beginnen, wählen Sie in den Einstellungen (Menü Einstellungen“) im Abschnitt „Adressieren“ den Punkt „LDAP Verzeichnisserver“

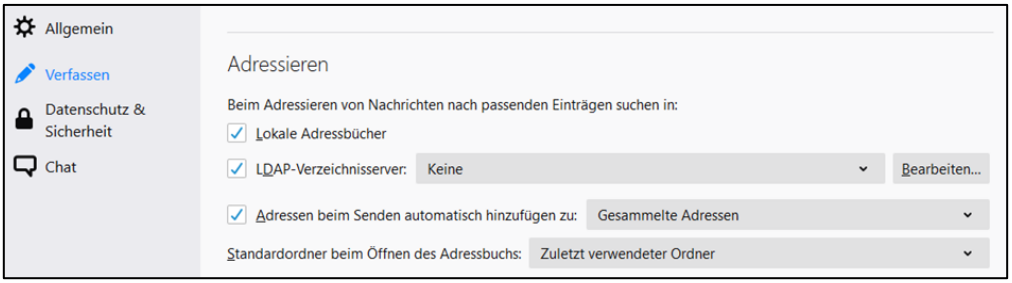



**Abbildung 19: Einstellung für LDAP Verzeichnisserver**

Unter „Bearbeiten“ einen neuen Verzeichnisserver anlegen. Im Eigenschaftsdialog (Abbildung 20) wählen Sie:

- **Name**: beliebiger Name für den Server, z. B. „VZD“
- **Serveradresse**: es muss die IP-Adresse des Konnektors eingetragen werden (befindet sich auf der Administrationsoberfläche des Konnektors)
- **Basis-DN**: Wert „dc=data,dc=vzd“
- **Port-Nummer**: 636
- **Verschlüsselte Verbindung**: „aktiv“

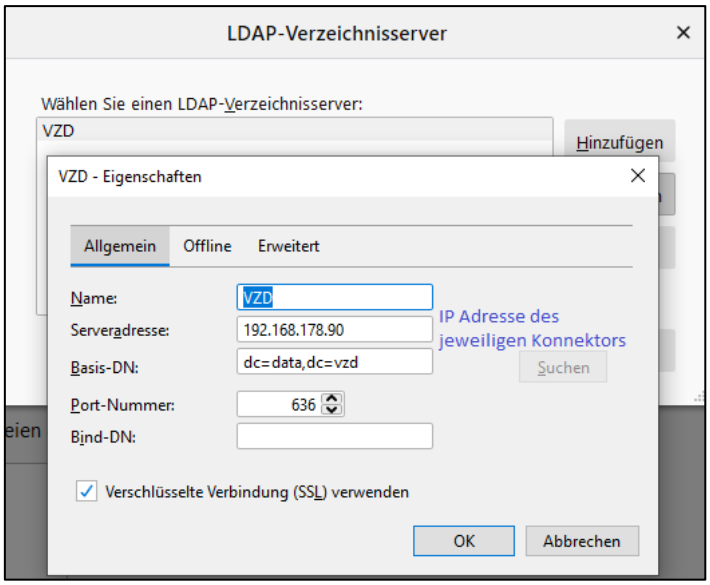



**Abbildung 20: Einrichtung LDAP**

Wenn im Clientmodul die zertifikatsbasierte Client-Authentifizierung ausgewählt wurde, muss das TSL Konnektor Client Zertifikat im Thunderbird unter `Einstellungen > Datenschutz & Sicherheit > Sicherheit > Zertifikate > Zertifikate verwalten` (Abbildung 21) hochgeladen werden.

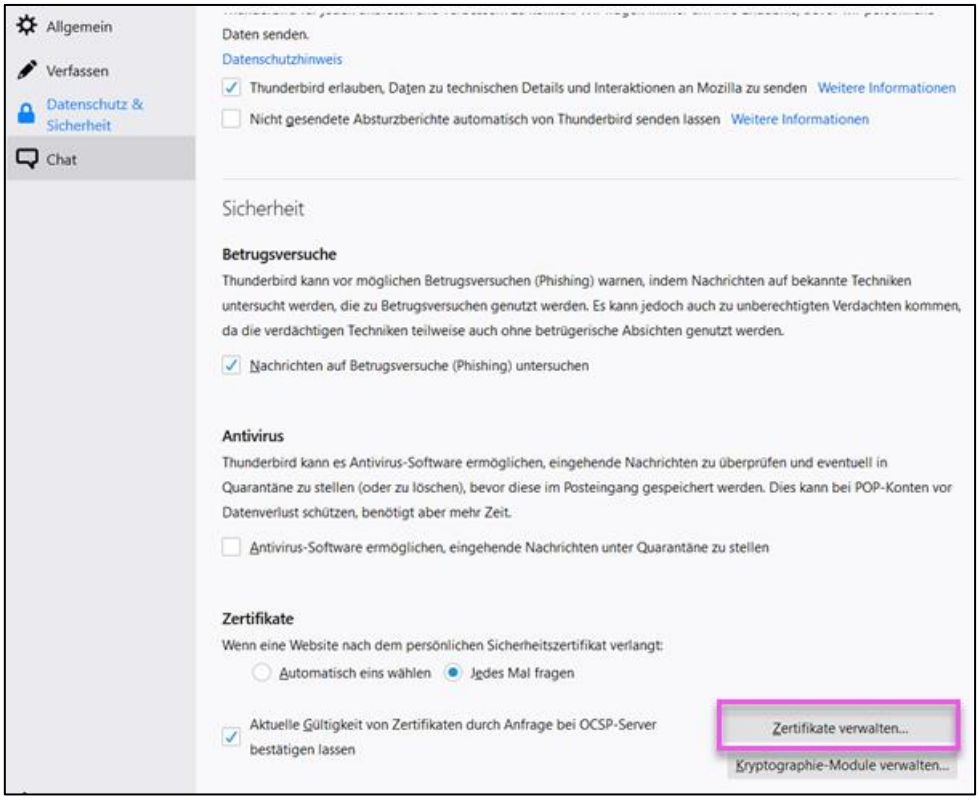



**Abbildung 21: Zertifikate verwalten**

Im Menüpunkt `Ihre Zertifikate > Importieren` das entsprechende Zertifikat auswählen und im nächsten Schritt das zugehörige Passwort eintragen.

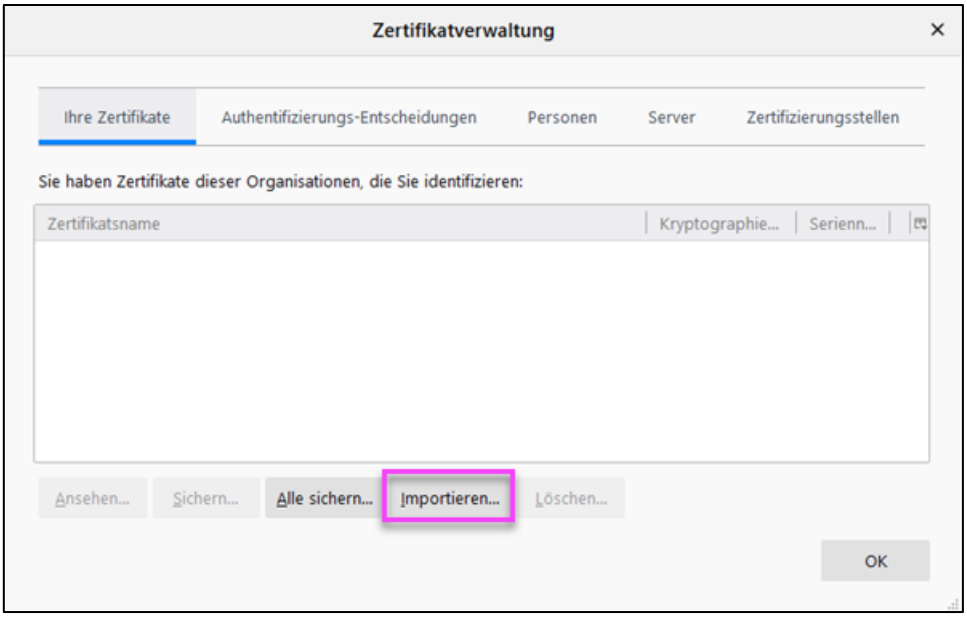



**Abbildung 22: Zertifikat importieren**

Nach der obigen Einrichtung kann man in die Suche des jeweiligen Adressbuchs wechseln. Bei der ersten Suche wird die untenstehende Sicherheitsausnahme-Meldung angezeigt (Abbildung 23), die Sie einfach bestätigen. Es wird dadurch ein Zertifikat im Zertifikatsspeicher des E-Mail-Programms abgelegt (Abbildung 24).

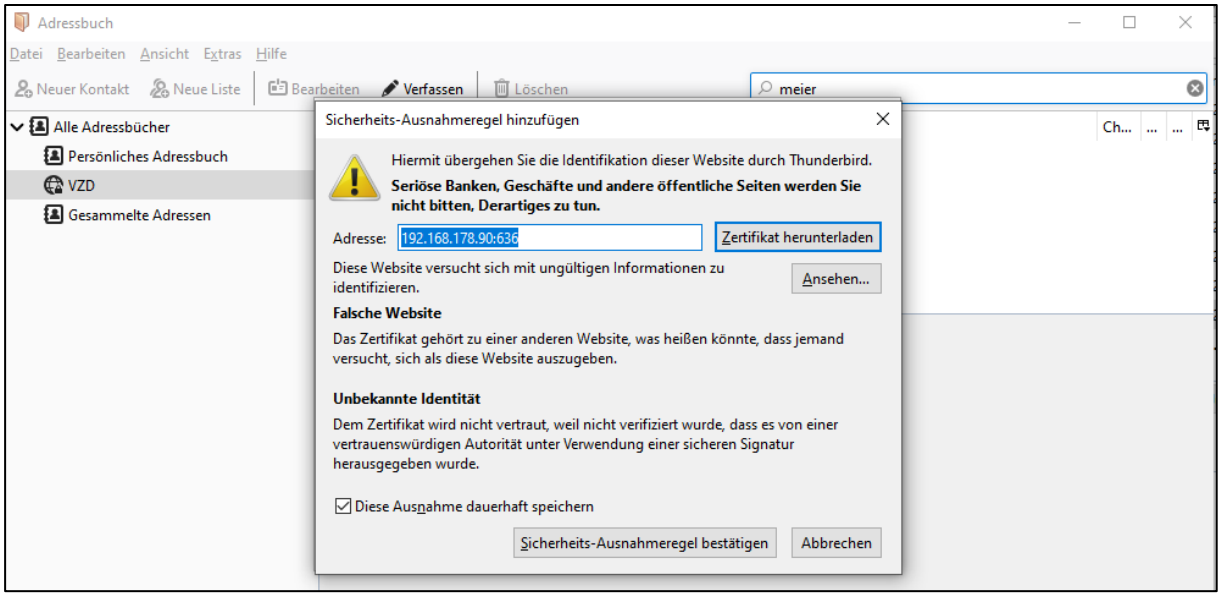



**Abbildung 23: Bestätigung Zertifikat**

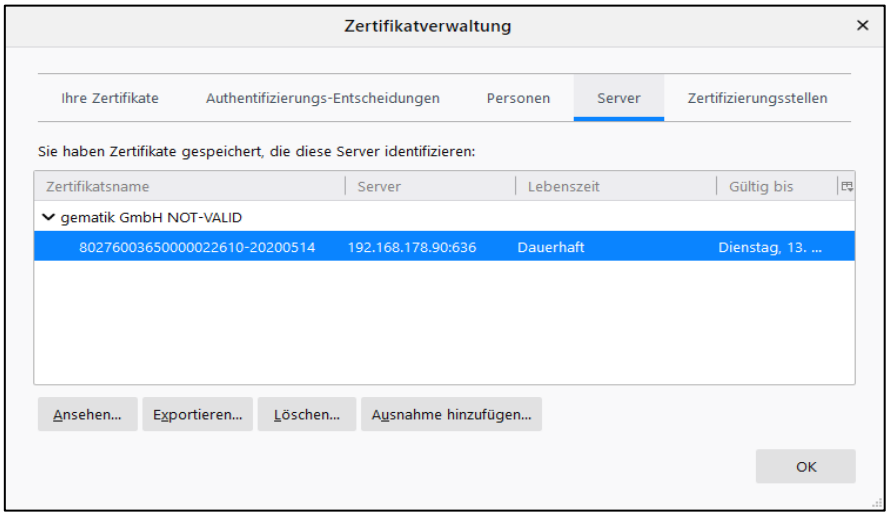



**Abbildung 24: Zertifikatsspeicher Mailprogramm**

Wenn das Zertifikat erfolgreich gespeichert wurde, muss die Suche ggfs. nochmal neu gestartet werden.

## 4.6 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 4.3.2.2 Konfigurationseinstellungen Konnektor).

Die Protokolle liegen im Unterordner `log` des Applikationsverzeichnis des Clientmoduls `kimCM` im Home-Verzeichnis des Benutzers. Für die Clientmodul Applikation befindet sich das Verzeichnis für Windows unter `C:\Users\<Username>\kimCm\log` bzw. für MacOS und Linux unter `/Users/<Username>/kimCm/log`. Für den Clientmodul Dienst befindet sich das Verzeichnis unter `C:\Windows\System32\config\systemprofile\kimCm\log`.

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

## 4.7 Update des Clientmoduls

Bis einschließlich der Version 1.4.3 muss das Update des kim+ Clientmoduls manuell erfolgen indem eine neue Version aus dem Downloadpunkt heruntergeladen und installiert wird.

Das kim+ Clientmodul verfügt ab der Version 1.4.4 über eine Autoupdate-Funktion, die regelmäßig auf die Verfügbarkeit einer neuen kim+ Clientmodul-Version prüft. Dazu muss das kim+ Clientmodul auf dem Client bzw. der Dienst aktiviert sein und der Computer muss über eine funktionsfähige Internetanbindung verfügen. Der Installer funktioniert für die folgenden Installationsarten:

- kim+ Clientmodul für Windows als Applikation
- kim+ Clientmodul für MacOS als Applikation
- kim+ Clientmodul für Linux als Applikation.

Für kim+ Clientmodul für Windows als Dienst steht die Funktion des automatischen Updates nicht zur Verfügung.

Ist eine neuere Version auf dem kim+ Clientmodul-Downloadpunkt verfügbar, dann bekommen Sie eine Nachricht mit der Option, diese neue Version herunterzuladen und zu installieren. Wenn Sie die Nachricht bestätigen, wird der aktuelle Installer heruntergeladen sowie gestartet. Möchten Sie die Aktualisierung zu einem späteren Zeitpunkt durchführen, dann schließen Sie die Nachricht. Ihnen wird zu einem späteren Zeitpunkt bei einer erneuten Prüfung die Nachricht wieder angezeigt.

Erkennt die Funktion eine neue Clientmodul-Version, werden Sie als Benutzer über den folgenden Dialog darüber informiert:

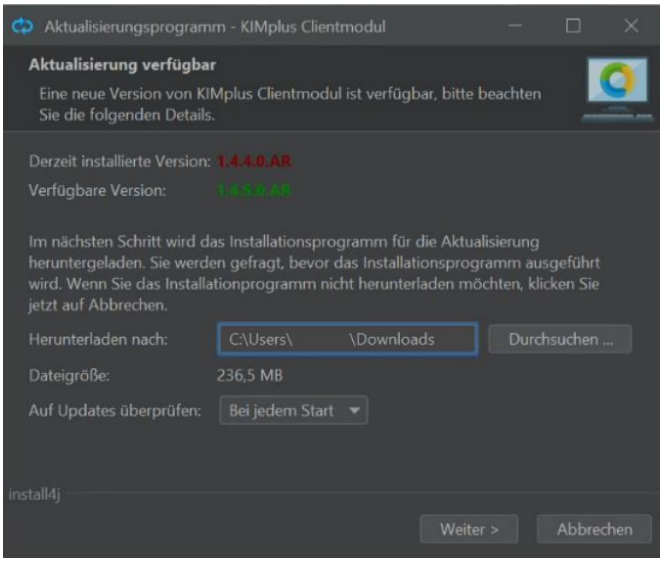



**Abbildung 25: Aktualisierung verfügbar**

Um die automatischen Updates zu aktivieren, müssen Sie sich am Ende der Installation in dem Feld **Auf Updates überprüfen** für einen Parameter entscheiden. Dabei stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung:

| Auswahl Prüfungsvariante | Beschreibung |
|---|---|
| Bei jedem Start | Es wird bei jedem Start des kim+ Clientmoduls geprüft, ob eine neue Version zur Verfügung steht. |
| Täglich | Einmal pro Tag wird eine Prüfung auf eine neue verfügbare Version durchgeführt. |
| Wöchentlich | Einmal pro Woche wird eine Prüfung auf eine neue verfügbare Version durchgeführt. |
| Monatlich | Einmal pro Monat wird eine Prüfung auf eine neue verfügbare Version durchgeführt. |
| Nie | Die Updatefunktionalität ist deaktiviert. Damit wird keine Prüfung auf neue Versionen durchgeführt. |

**Tabelle 10: Konfigurationsparameter Updatefunktion**

Über den Button **Abbrechen** beenden Sie das Update des Clientmoduls ohne es durchzuführen. Wenn Sie die neue Version des Clientmoduls installieren möchten, klicken Sie auf den Button **Weiter**. Es öffnet

sich ein Dialogfenster, welches den aktuellen Stand des Downloads des Installers in der neuen Version anzeigt. Ist der Installer fertig heruntergeladen, dann wird er automatisch gestartet. Das Starten des Installers beendet automatisch das aktuell ausgeführte kim+ Clientmodul und bietet Ihnen eine Neuinstallation des kim+ Clientmoduls in der neuen Version an (siehe auch Abschnitt 4.3.1).

Bestehende Konfigurationen (Konnektor, Zertifikate usw.) des kim+ Clientmoduls werden beim Update beibehalten und müssen nicht erneut konfiguriert werden.

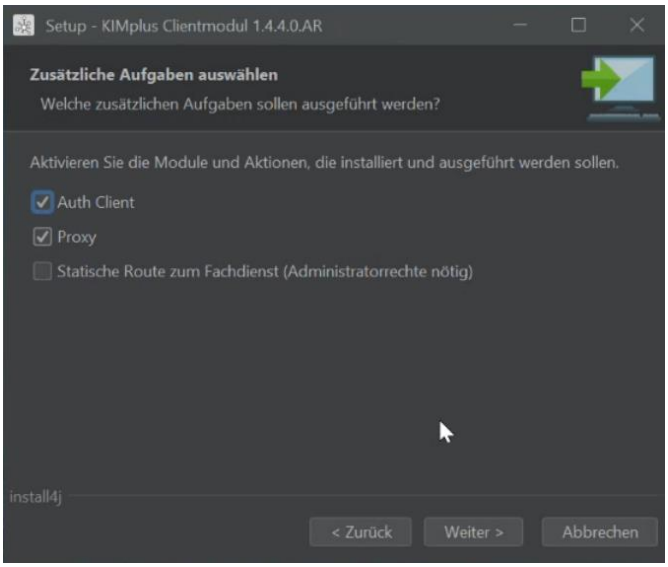



**Abbildung 26: Start Installation des Updates**

Sie können die Autoupdate-Funktion über die Einstellung **Nie** in dem Feld **Auf Updates überprüfen** deaktivieren. Mit dieser Einstellung erfolgt keine automatische Prüfung mehr. Sie müssen dann selbst kontrollieren, ob eine neue kim+ Clientmodul-Version vorliegt.

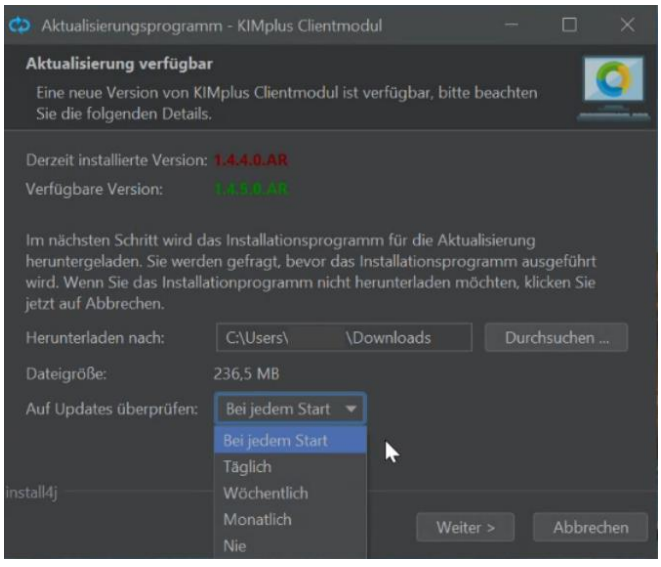



**Abbildung 27: automatische Updates deaktivieren**

## 4.8 Zertifikatstausch

Die im Produkt kim+ verwendeten Zertifikate sind nur für einen bestimmten Zeitraum gültig. Der Anwender erhält, wie im Abschnitt 4.5 beschrieben, vor Ablauf der Zertifikate einen Hinweis. Er ist dafür verantwortlich, diese nach Ablauf der Gültigkeit auszutauschen. Dafür muss das neue Zertifikat heruntergeladen und, wie im Abschnitt 4.3.2.4 beschrieben, in das Clientmodul integriert werden.

## 4.9 Deinstallation

Das Clientmodul kann über den Standardweg zur Deinstallation von Programmen auf einem Client deinstalliert werden. Gehen Sie dafür folgendermaßen vor:

1. Wählen Sie den Bereich „Programme hinzufügen und entfernen“ in Windows aus.
2. Wählen Sie dort im Bereich Apps & Features das kim+-Clientmodul aus und klicken Sie dann auf die Schaltfläche „Deinstallieren“.

## 4.10 Hinweise

### 4.10.1 Zertifikatsimport

Der Benutzer ist dafür verantwortlich, dass nur gültige und vertrauenswürdige Zertifikate importiert werden. Es findet keine technische Prüfung der Zertifikate durch das Clientmodul statt.

### 4.10.2 Nicht vertrauenswürdiges Zertifikat

Zertifikate, denen nicht mehr vertraut wird (u. a., weil die Zertifikate abgelaufen sind), müssen vom Benutzer über die verfügbaren Einstellmöglichkeiten ausgetauscht oder es muss der gesamte Truststore gelöscht werden.

### 4.10.3 E-Mail-Signierung

Wenn im übergebenen Aufrufkontext mehr als eine SMC-B vorhanden ist, dann wird die erste gefundene SMC-B für die Signierung der E-Mail verwendet.

### 4.10.4 E-Mail-Entschlüsselung

Wenn im übergebenen Aufrufkontext mehr als eine Karte vorhanden ist, mit der eine Nachricht entschlüsselbar ist, dann wird die erste gefundene verwendet.

### 4.10.5 OSS-Pakete

Das Clientmodul verwendet teilweise Open-Source-Pakete. Informationen über OSS-Pakete können auf der LoginSeite des Account Managers durch einen Klick auf den Button **OSS-Pakete** (Abbildung 29: Account Manager - Login, Markierung 3) heruntergeladen werden.

### 4.10.6 Ausnahme für Security-Tools

Bei der Nutzung des kim+ Dienstes kann es zu Problemen mit Security-Tools kommen (Virenscannern, etc.). 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 im Security-Tool eingestellt werden:

`am.kimplus.de`

`am.arv.kim.telematik`

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

`ocsp.digicert.com`

`status.geotrust.com`

## 4.11 Verwendung des Authentication Clients

Der Authentication Client (Auth Client) ist Teil des kim+ Clientmoduls und ermöglicht das Authentisieren von Aktionen mittels des verfügbaren Kartenmaterials einer gesteckten Karte am Konnektor. Anwendungsfälle, die eine solche Authentisierung benötigen, sind zum Beispiel die Registrierung eines neuen kim+ Accounts oder einer Account-Datenänderung. Um den Auth Client zu verwenden, muss das Clientmodul bereits gestartet und konfiguriert sein. Falls eine Authentisierung gefordert wird, öffnet sich das Fenster vom Auth Client. Dabei werden folgende Schritte mit dem Nutzer durchgeführt:

**Schritt 1: Auswahl des Mandanten für die Authentisierung**
Es wird ausgewählt, für welchen Mandanten die Authentisierung durchgeführt werden soll.

**Schritt 2: Auswahl des Kartentyps für die Authentisierung**
Es wird ausgewählt, ob das Kartenmaterial einer SMC-B oder einer HBA Karte zu verwenden ist. Nach Auswahl des Kartentyps werden die verfügbaren Karten entsprechend des Typs geladen und gelistet.

**Schritt 3: Auswahl der konkreten Karte für die Authentisierung**
Über den Button **Karten erneut laden** können die verfügbaren Karten neu geladen werden. Es wird eine Karte durch Selektion und einen Klick auf "Karte verwenden" für die Authentisierung ausgewählt.

**Schritt 4: Durchführung der Authentisierung**
Zuletzt wird durch einen Klick auf den Button **Authentisieren** die Aktion mittels des verfügbaren Kartenmaterials der ausgewählten Karte authentisiert. Sofern die Karte nicht freigeschalten ist, wird am Kartenterminal der PIN zur Freischaltung angefordert.

# 5 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.

## 5.1 Registrieren am Account Manager

Vorbedingung: Der Anbieter des kim+ Produktes hat einen Antrag für die Anmeldung des Anwenders / LEs bei der verantwortlichen Stelle gestellt. 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 28: Account Manager - Passwort setzen) führt.

Für Passwörter gelten aus Sicherheitsgründen folgende Kriterien:

- 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.
- Es müssen mindestens drei der vier genannten Zeichenkategorien verwendet werden.
- Es muss insgesamt mindestens 8 Zeichen lang sein.

Nach Abschluss des Vorgangs zum Setzen des Passwortes erfolgt eine Weiterleitung auf die Login-Seite des Account Managers (Abbildung 29: 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.

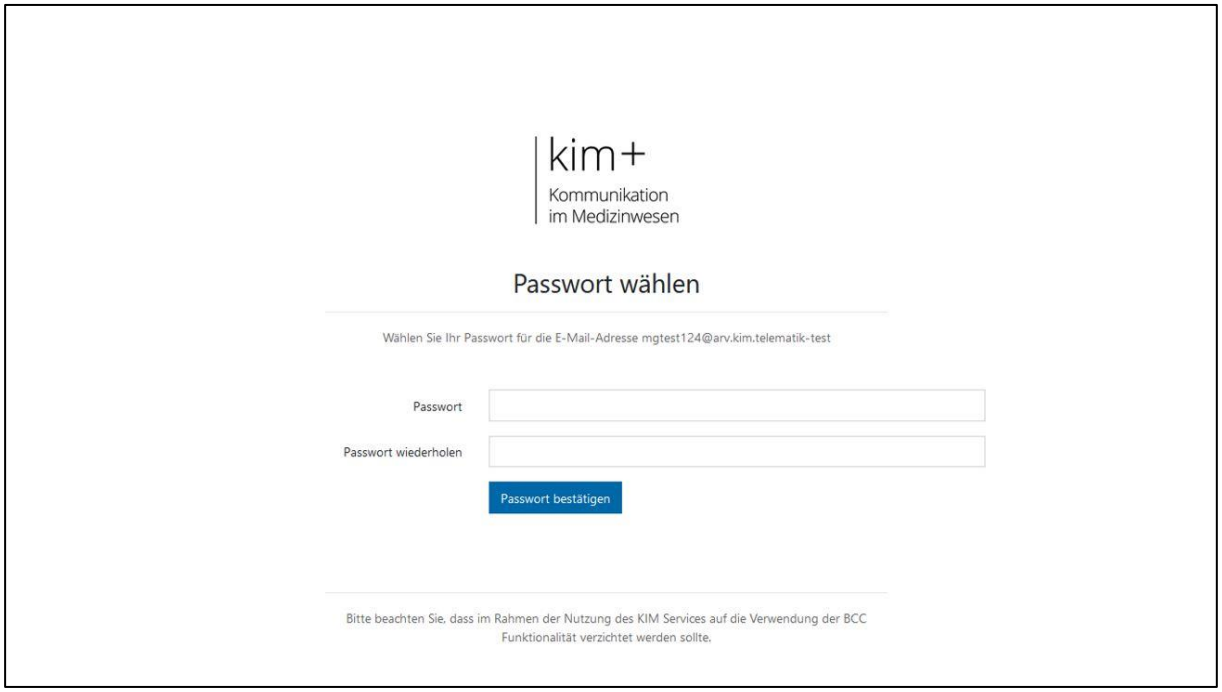



**Abbildung 28: Account Manager - Passwort setzen**

## 5.2 Login

Vorbedingung: Der Anwender verfügt über eine gültige kim+-E-Mail-Adresse und kennt das zugehörige Passwort.

Der Login erfolgt über eine Eingabemaske auf der Startseite der Anwendung (Abbildung 29: 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-Mail-Adresse des eingeloggten Anwenders dargestellt (Abbildung 30: Account Manager - Menü, Markierung 1).

Anmerkung: Nach dreimaligem Versuch, sich mit einem ungültigen oder fehlerhaften Passwort einzuloggen, wird der Account der angegebenen kim+-E-Mail-Adresse gesperrt. Der Account kann erst nach einer Entsperrung wiederverwendet werden (Abschnitt 5.9 Account entsperren).
Im Ausnahmefall kann es vorkommen, dass der Anbieter Ihren kim+ Vertrag gesperrt hat, dann schlägt ein Login am Account Manager ebenfalls fehl. In diesem Fall ist eine Entsperrung nur durch den Anbieter möglich. Mehr Informationen dazu erhalten Sie in Kapitel 3.6.

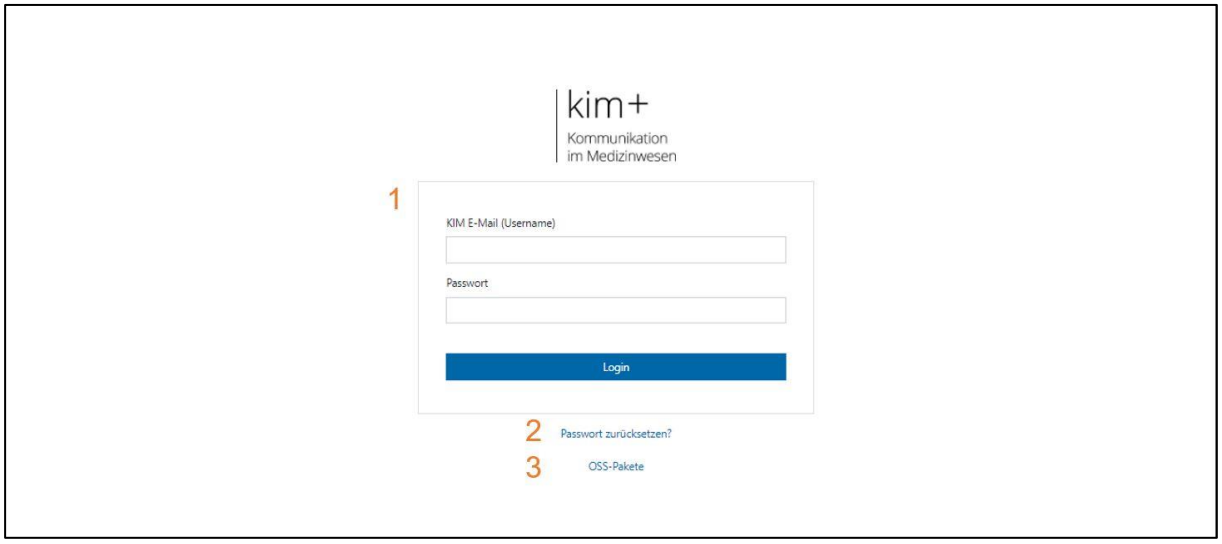



**Abbildung 29: Account Manager - Login**


**Abbildung 30: Account Manager - Menü**

## 5.3 Kartenauthentisierung

Bei einigen Anwendungsfällen ist eine zusätzliche Authentisierung via Kartenterminal notwendig. In diesem Fall folgen Sie den Anweisungen des Account Managers bzw. des Auth Client im kim+ Client-Modul.

In der Anwendung **Account Manager** öffnet sich zuerst ein Fenster mit dem Hinweis zur Eingabe des PINs der Karte am Kartenterminal (Abbildung 31: Account Manager - Kartenauthentisierung). Dieses Fenster schließt sich nach Abschluss der PIN-Eingabe automatisch.

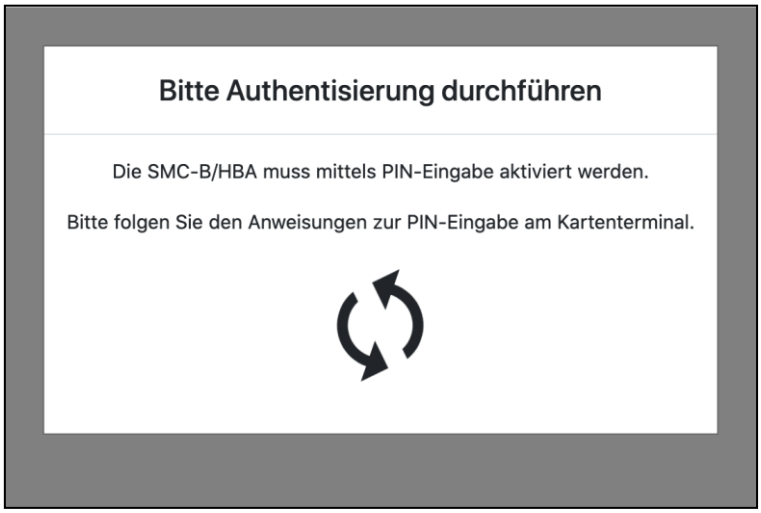



**Abbildung 31: Account Manager - Kartenauthentisierung**

Es öffnet sich nun ein Fenster des **Auth Clients** (Abbildung 31: Account Manager - Kartenauthentisierung). Wählen Sie hier den Kartentyp **SMC-B** oder **HBA** für die Authentisierung aus. Anschließend werden die Karten des Kartenterminals geladen. Dieser Vorgang kann einige Sekunden dauern.


**Abbildung 32: Auth Client – Auswahl Kartentyp**

Wählen Sie nun die Karte aus, die Sie für die Authentisierung verwenden wollen. Klicken Sie anschließend auf **Karte verwenden**.


**Abbildung 33: Auth Client – Auswahl der Karte**

Bestätigen Sie die Authentisierung über den Button **Authentisieren**. Die Durchführung der Authentisierung kann einige Sekunden dauern.

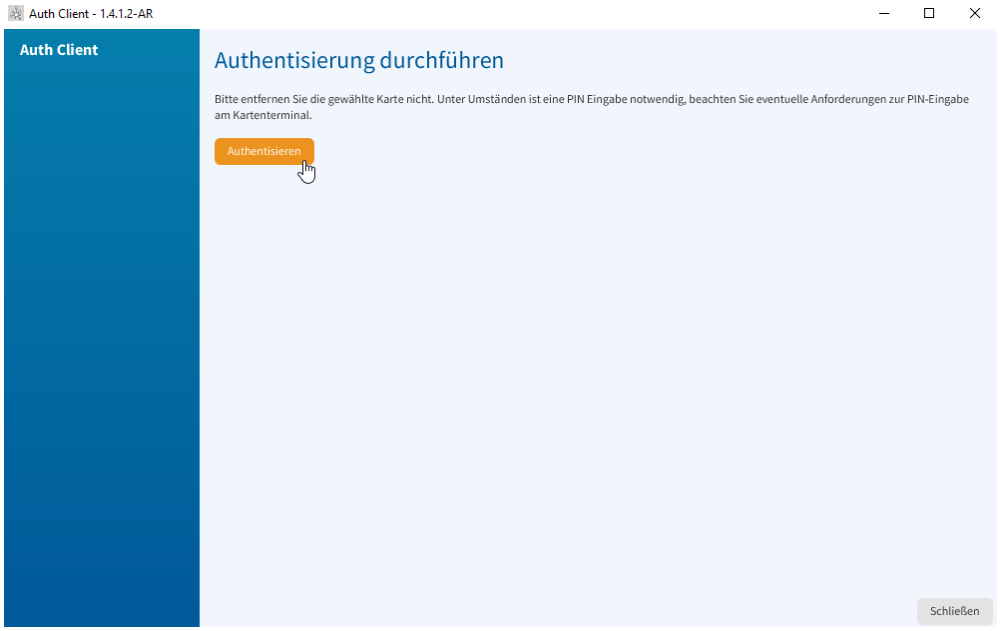



**Abbildung 34: Auth Client – Authentisierung durchführen**

Das Fenster des Auth Client schließt sich nach erfolgreicher Authentisierung selbstständig.

## 5.4 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 30: Account Manager - Menü, Markierung 3) aufgerufen werden.

## 5.5 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 30: Account Manager - Menü, Markierung 4) aufgerufen werden.

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

## 5.6 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 E-Mailadresse.

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 30: 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.

## 5.7 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 35: Account Manager - Passwort ändern) kann durch einen Klick auf den Button **Passwort ändern** (Abbildung 30: Account Manager - Menü, Markierung 2) aufgerufen werden. Der Vorgang kann durch einen Klick auf den Button **Abbrechen** abgebrochen werden.

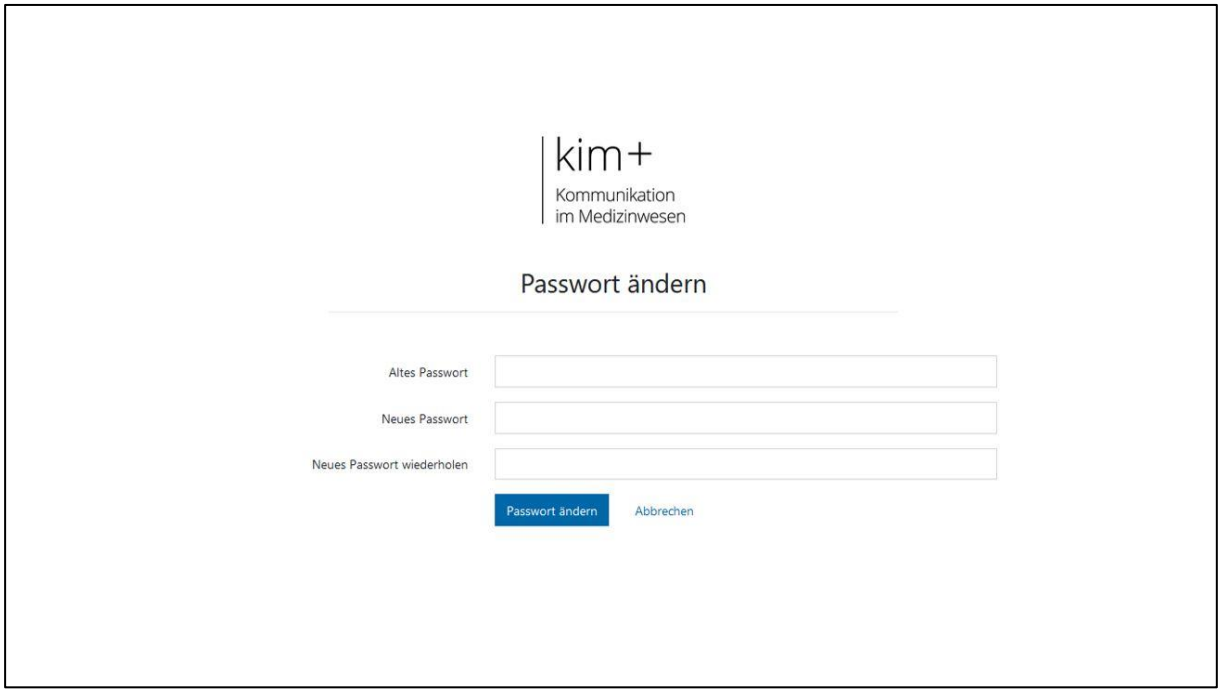



**Abbildung 35: Account Manager - Passwort ändern**

## 5.8 Passwort zurücksetzen

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

Der Vorgang zur Zurücksetzung eines Passworts kann durch einen Klick auf den Button **Passwort vergessen?** (Abbildung 29: Account Manager - Login, Markierung 2) gestartet werden. Nach dem Klick erfolgt eine Weiterleitung auf eine Eingabemaske, in der Sie die kim+-E-Mail-Adresse und die hinterlegte Recovery E-Mailadresse eingeben (Abbildung 36: 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.

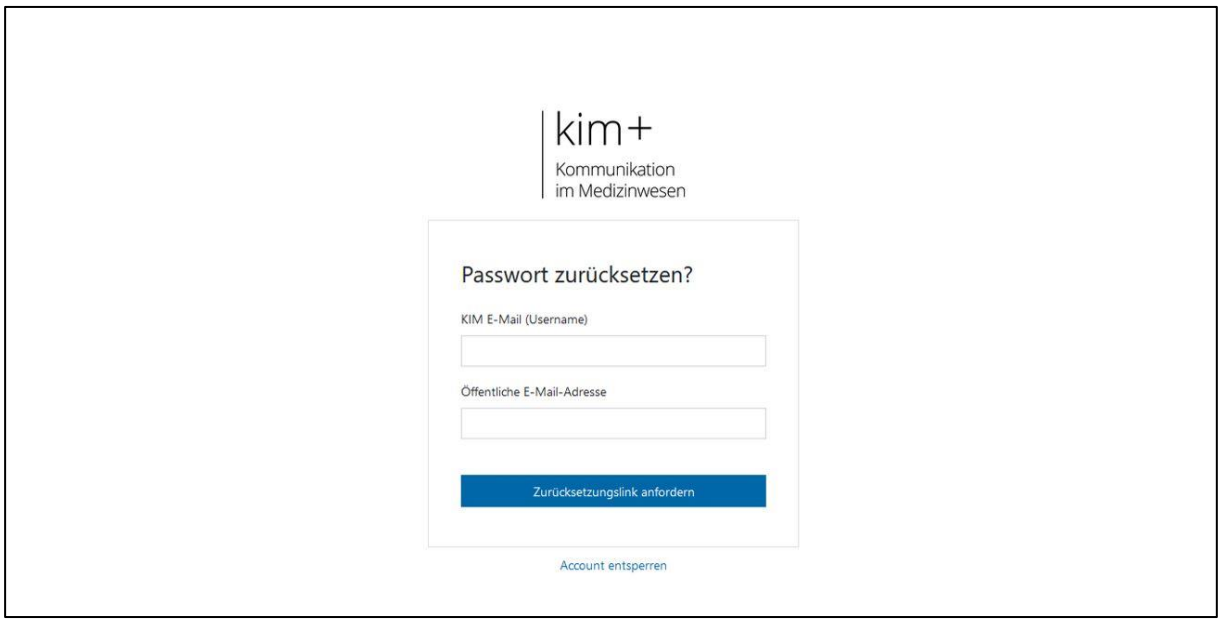



**Abbildung 36: Account Manager - Passwort vergessen**

## 5.9 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 Login-Seite des Account Managers (Abbildung 29: 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.

## 5.10 Logout

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

Der Logout wird durch einen Klick auf den Button **Abmelden** (Abbildung 30: Account Manager - Menü, Markierung 6) ausgelöst. Es erfolgt eine automatische Weiterleitung auf die Login-Seite.

## 5.11 De-Registrieren am Account Manager

Vorbedingung: Der De-Registrierungsprozess wurde von der verantwortlichen Stelle angestoßen. Der Anwender hat Zugriff auf das Postfach der hinterlegten Recovery E-Mail-Adresse.

Der Account Manager sendet einen Bestätigungslink an die angegebene Recovery E-Mail-Adresse. Nach einem Aufruf des Links wird der Account de-registriert.

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

# 6 Anlagen und Verzeichnisse

## Abkürzungsverzeichnis

| Begriff | Erklärung |
|---|---|
| CLI | Command Line Interface |
| CM | Clientmodul |
| DNS | Domain Name System |
| ff | fortfolgend |
| 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** 11**: Abkürzungsverzeichnis**

# Abbildungsverzeichnis

## Tabellenverzeichnis