KV TELEMATIK

Ein Tochterunternehmen der
Kassenärztlichen Bundesvereinigung

Leistungsbeschreibung KV-Connect

Herausgeber:
KV Telematik GmbH

Inhaltsverzeichnis

Änderungshistorie

Vers.	Datum	Autor	Kap.	Änderung	Status
0.1		KVTG	alle	Initiale Erstellung	Entwurf

Herausgeber:
KV Telematik GmbH

1 Was ist KV-Connect?

KV-Connect ist ein sicherer, datenschutzkonformer Kommunikationsdienst der Kassenärztlichen Vereinigungen, der KBV und der KV Telematik GmbH.Da KV-Connect ausschließlich im „sicheren Netz der Kassenärztlichen Vereinigungen“ (SNK) zur Verfügung gestellt wird, ist der sichere Datenaustausch zwischen Ärzten, Psychotherapeuten, Krankenhäusern und Kassenärztlichen Vereinigungen gewährleistet. Durch KV-Connect werden alle übertragenen Nachrichten Ende-zu-Ende verschlüsselt.

Für verschiedene Anwendungsszenarien, z.B. Abrechnung, eDMP oder eArztbrief, wurden unterschiedliche KV-Connect Anwendungen von der KV Telematik GmbH spezifiziert. Diese werden kostenfrei zur Implementierung im Primärsystem bereitgestellt. KV-Connect und die Anwendungen werden insbesondere über das Primärsystem (Praxisverwaltungs-, Laborinformations- oder Krankenhausinformationssystem) zur Verfügung gestellt.

In diesem Zusammenhang werden folgende Dienste angeboten:

- Betrieb der KV-Connect Server
- Integration KV-Connect in das Primärsystem
    - Integration mittels KV-Connect Client über Standard E-Mail-Schnittstellen (smtp/pop3)
    - Integration mittels KV-Connect Serverschnittstelle (REST) und native Anbindung
- Bereitstellen von Spezifikationen für KV-Connect Anwendungen
- Bereitstellen von Audits für KV-Connect Anwendungen
- Datenschutz- und Datensicherheitsmechanismen

2 Voraussetzungen für KV-Connect

2.1 SNK-Anbindung

Da KV-Connect ausschließlich im "sicheren Netz der KVen" (SNK) zur Verfügung steht, muss ein Zugang zum SNK vorhanden sein. Das SNK stellt zwei Zugangsvarianten - KV-SafeNet und KV-FlexNet - zur Verfügung, welche durch unterschiedliche technische Lösungen abgestufte Sicherheitsanforderungen realisieren.

2.1.1 KV-SafeNet

Das KV-SafeNet bietet einen sicheren Zugang zu den Online-Diensten der KVen. Hinter dem KV-SafeNet verbirgt sich eine IT-Struktur, die es ermöglicht, Dienste der KVen über ein privates virtuelles Netz (VPN) zu nutzen.

KV-SafeNet ist durch geprüfte Sicherheitsmechanismen vom öffentlichen Internet getrennt. Der Zugang ist nur mit Berechtigung und speziell konfigurierten Geräten (KV-SafeNet-Router) möglich. Durch die Abschottung vom unsicheren Internet und die Datenübertragung über ein geschlossenes sicheres Netz werden die Anforderungen zum Datenschutz gewährleistet und sensible Daten können auf sicherem Weg an andere Mitglieder des Netzwerkes übertragen werden.

Für die Anbindung über KV-SafeNet ist ein geeigneter KV-SafeNet-Anbieter auszuwählen, der einen vorkonfigurierten KV-SafeNet-Router zur Verfügung stellt. Weitere Informationen zu KV-SafeNet sowie die Checkliste und Konditionen für die Einrichtung eines KV-SafeNet-Anschlusses sind bei der KBV unter www.kbv.de/html/7145.php zu finden.

2.1.2 KV-FlexNet

Als Alternative zu KV-SafeNet, bieten einige KVen KV-FlexNet als Zugangsmöglichkeit zum SNK und zu ihrem Mitgliederportal an. KV-FlexNet funktioniert ähnlich wie das KV-SafeNet, nur wird der sichere Tunnel zur Datenübertragung hier nicht über den KV-SafeNet-Router, sondern mittels einer Software aufgebaut (sogenannte Software-VPN-Lösung). Im Unterschied zu KV-SafeNet sind nicht alle Arbeitsplätze der Praxis, sondern nur der Rechner, auf dem die Software installiert ist, angebunden. Eine permanente Nutzung der Online-Dienste ist im Unterschied zu KV-SafeNet nicht möglich.

Der SNK-Zugang über KV-FlexNet zur Nutzung von KV-Connect ist grundsätzlich auch möglich, in den meisten KV-Bereichen wird diese Methode jedoch aus datenschutzrechtlichen Gründen nicht unterstützt. KVen, die FlexNet anbieten, ermöglichen in der Regel auch den Betrieb von KV-Connect darüber.

2.2 Ein Primärsystem, das KV-Connect integriet hat

Die Kassenärztliche Bundesvereinigung (KBV) verpflichtet alle PVS-Hersteller, KV-Connect für die Anwendung 1-ClickAbrechnung bereitzustellen (vgl. http://www.kbv.de/html/5614.php). Einem Großteil der niedergelassenen Ärzte und Psychotherapeuten steht somit KV-Connect in ihrem Praxisverwaltungssystem zur Verfügung.Sollte KV-Connect in Ihrem System nicht verfügbar sein, kann auch eine herstellerunabhängige Software eingesetzt werden.

2.3 Registrierung für KV-Connect

Um an KV-Connect teilnehmen zu können, ist eine Registrierung erforderlich. Die Registrierung für KV-Connect läuft über die zuständige KV.
Die zuständige KV prüft die erhaltenen Informationen auf ihre Richtigkeit und Vollständigkeit. Falls die Informationen richtig und vollständig sind, registriert die KV den Arzt in der Benutzerverwaltung für KV-Connect und sendet die Zugangsdaten auf dem Postweg zu. Die Zugangsdaten bestehen aus einem Benutzernamen und einem Passwort. Nach Erhalt der KV-Connect Zugangsdaten müssen diese in das Primärsystem eingepflegt werden.
Eine Übersicht über die Ansprechpartner der jeweiligen KV sind auf der Homepage der KV-Telematik GmbH unter folgendem Link https://www.kv-telematik.de/aerzte-und-pschotherapeuten/kv-connect/teilnahme-registrierung/ zu finden.

3 KV-Connect Anwendungen

3.1 1-Click-Abrechnung

Mit der 1-Click- Abrechnung via KV-Connect können niedergelassene Ärzte und Psychotherapeuten ihre Quartalsabrechnung direkt aus dem PVS an die Kassenärztliche Vereinigung (KV) senden. Seit dem Sommer 2014 steht eine erweiterte Variante der 1-Click-Abrechnung 2.0 zur Verfügung. Damit ist auch der Versand von Testabrechnungen und signierten Sammelerklärungen möglich, sofern die KV dies anbietet.

3.2 eArztbrief

Der herkömmliche Arztbrief auf Papier ist im Transport langsam und zieht mehrere Medienbrüche nach sich. Das heute gerne verwendete Fax, bzw. eFax oder E-Mail ist zwar schneller, aber haftungs- und datenschutzrechtlich sehr kritisch. Beide Varianten sind in ihrer Aussagefähigkeit begrenzt. Demgegenüber erlaubt der eArztbrief über KV-Connect eine schnelle, sichere und weitergehende Übermittlung qualitativ aussagekräftiger Informationen bis hin zu bewegten Bildsequenzen. Neben der Sicherheit kann durch die Nutzung des eArztbriefes auch die Wirtschaftlichkeit in der medizinischen Versorgung erhöht werden.

3.3 Weitere Anwendungen

- eDMP
- DALE-UV
- eHKS
- eKoloskopieDoku
- eDialyseDoku
- eDoku
- eNachricht

eTerminservice, ePVS, und die Befundübermittlung bei LDT 3.0 sowie sQS sind als weitere Anwendungen in Planung, und werden im Laufe des Jahres 2016 zur Verfügung stehen.

3.4 KV-Connect Anwendungen im PVS

Die Kassenärztliche Bundesvereinigung (KBV) verpflichtet alle PVS-Hersteller, KV-Connect für die 1-Click-Abrechnung bereitzustellen. Ob auch weitere KV-Connect-Anwendungen in Ihrem Softwaresystem umgesetzt werden, ist optional und hängt vom jeweiligen Anbieter ab.

Aus diesem Grund kann keine allgemeingültige Anleitung gegeben werden, welche KV-Connect Anwendungen von Ihrem Softwaresystem unterstützt werden.

4 Kosten

Die KV Telematik GmbH stellt KV-Connect allen Softwareanbietern kostenlos zur Verfügung. Für die Integration von KV-Connect im Allgemeinen und die Implementierung der einzelnen Anwendungen im Speziellen haben die verschiedenen Anbieter sehr unterschiedliche Preismodelle entwickelt, die auf Grund Ihrer Komplexität und Vielfalt hier nicht dargestellt werden können.

Des Weiteren entstehen Kosten für die Anbindung an das SNK. Je nach Anbieter und Anschlussvariante können die Kosten variieren.

5 Nutzungsbedingungen

Die Nutzungsbedingungen von KV-Connect sind auf der Homepage der KV Telematik GmbH unter dem nachfolgendem Link zu finden:

https://www.kv-telematik.de/aerzte-und-psychotherapeuten/kv-connect/nutzungs-bedingungen/

6 KV-Connect Integration in das Primärsystem

Zur Integration in das Primärsystem (PVS, KIS etc.) ist KV-Connect flexibel konzipiert und bietet je nach Anforderung grundsätzlich zwei unterschiedliche Schnittstellen an:

1. Integration KV-Connect Client über Standard E-Mail-Schnittstellen (smtp/pop3) → Anbindung des Clients über POP3 und SMTP
2. Integration KV-Connect Serverschnittstelle (REST) und native Anbindung → Anbindung an KVConnect über die REST-Serverschnittstelle

6.1 Anbindung des Clients über POP3 und SMTP

Der KV-Connect Client versendet bzw. empfängt über SMTP (RFC 5321) und POP3 (RFC 1939) MIME-Nachrichten. Hierzu fungiert der KV-Connect Client als E-Mail-Server auf dem lokalen System. Er übernimmt hierbei auch die Ver- und Entschlüsselung sowie die Signatur. Der KV-Connect Client kommuniziert über MIME-Nachrichten nach RFC 2048 mit dem Primärsystem. Im Rahmen des Versands werden die vom Primärsystem erzeugten MIME-Nachrichten über SMTP angenommen. Anschließend signiert der KV-Connect Client die Nachricht inkl. der vorhandenen Anlagen mittels X.509v3-Zertifikaten, verschlüsselt und versendet die so entstandene S/MIME-Nachricht. Der Empfang der Nachrichten verläuft entsprechend. Für Signatur und Entschlüsselung ist ein privater Keystore notwendig, der bei der ersten Verwendung des KV-Connect Client über eine lokale Konfigurationswebseite angelegt werden muss. Der private Keystore ist über eine PIN geschützt, die beim Abrufen und Senden von E-Mails mit dem Kennwort übermittelt werden muss.

Die Verbindung zwischen Primärsystem und KV-Connect Client ist mittels TLS/SSL abgesichert. Hierbei kommt SMTP Auth nach RFC 4954 mit Plain oder Login Authentisierung für SMTP nach RFC 4616 zum Einsatz. Aus diesem Grund wird SMTP über Port 465 und POP3 über Port 995 angesprochen. Diese Ports sind konfigurierbar.

6.1.1 Ablauf

Versand über SMTP

Das Primärsystem generiert eine MIME-Nachricht, die auch Anlagen enthalten kann. Diese MIME-Nachricht wird mittels SMTP an den KV-Connect Client übergeben. Der KV-Connect Client behandelt die MIME-Nachricht kryptographisch. Hierzu ist es erforderlich, den Keystore des Benutzers über eine PIN zu entsperren. Die PIN wird mit dem SMTP-Kennwort übermittelt. Sofern die Kryptographie fehlerfrei durchgeführt werden konnte, wird die S/MIME-Nachricht versendet. Ein Auftreten von Fehlern bei der Kryptographie führt zum Abbruch des Versandvorgangs. Fehlermeldungen werden über SMTP-Statuscodes abgebildet.

Empfang über POP3

Das Primärsystem fragt mittels POP3-Kommandos am KV-Connect Client an, ob neue S/MIME-Nachrichten zum Abruf bereit stehen. Der KV-Connect-Client seinerseits sorgt in diesem Fall dafür, dass eventuell auf dem Server vorhandene Nachrichten gesucht werden. Sofern neue Nachrichten vorhanden sind, werden diese mithilfe der entsprechenden POP3-Befehle abgeholt. Die dazu notwendige PIN des privaten Keystores wird mit dem POP3-Kennwort übermittelt. Wurde die PIN korrekt angegeben, wird die S/MIME-Nachricht kryptographisch behandelt. Im Anschluss prüft der KV-Connect Client die Signatur der S/MIME-Nachricht und erzeugt im Fall einer fehlerhaften Signatur eine entsprechende Fehlermeldung, die als „synthetische" Mail (Originalnachricht wird angehängt) dem Empfänger zur Verfügung gestellt wird. Nach erfolgreicher Entschlüsselung wird die MIME/Nachricht dem Primärsystem zur Verfügung gestellt. Hat das Primärsystem die MIME-Nachricht erfolgreich empfangen, so übermittelt es die POP3-Befehle zum Löschen der Nachricht auf dem Server an den KV-Connect Client.

6.2 Anbindung an KV-Connect über die REST-Serverschnittstelle

Mittels der REST-Serverschnittstelle besteht die Möglichkeit, das Primärsystem direkt an den KV-Connect-Server anzubinden. In diesem Fall entfällt eine lokale Installation des KV-Connect Client. Die Funktionen des KV-Connect Client müssen durch das Primärsystem realisiert werden. Neben der

Kommunikation über die REST-Serverschnittstelle muss das Primärsystem die kryptographische Behandlung der ein- und ausgehenden Nachrichten übernehmen. Die Kommunikation mit der REST-Serverschnittstelle erfolgt über eine SSL-geschützte Verbindung. Zur Authentifizierung beim Zugriff auf die Ressourcen wird BASIC Authentification verwendet. Details hierzu sind, ebenso wie die Kryptographie sowie die Schnittstelle, im KV-Connect Partnerportal beschrieben.

6.2.1 Ablauf

Versand

Das Primärsystem generiert eine MIME-Nachricht, die auch Anlagen enthalten kann. Im Anschluss müssen die Zertifikate der Empfänger abgerufen werden. Sollte ein Zertifikat nicht vorhanden sein, so ist eine Fehlermeldung auszugeben und der Versandvorgang ist abzubrechen. Sofern alle Zertifikate vorhanden sind, ist die MIME-Nachricht entsprechend der beschriebenen Verfahren (s. KV-Connect Partnerportal) zu signieren und zu verschlüsseln. Anschließend wird die S/MIME-Nachricht versendet. Sollte der Versand nicht erfolgreich sein, so ist eine Fehlermeldung auszugeben und der Versand abzubrechen.

Empfang

Das Primärsystem fragt mittels entsprechender REST-Befehle am KV-Connect Server an, ob neue S /MIME-Nachrichten für den Nutzer vorliegen. Wenn dies der Fall ist, wird die neue S/MIME-Nachricht über ihre Message-ID abgerufen. Im Anschluss wird die Nachricht entschlüsselt und die Signatur der Nachricht geprüft. Sollte die Signatur nicht in Ordnung sein, so ist eine Warnmeldung auszugeben. Die S /MIME-Nachricht wird anschließend lokal als MIME-Nachricht gespeichert und über die jeweiligen REST-Befehle vom KV-Connect Server gelöscht. Für den Fall, dass der Löschvorgang nicht erfolgreich abgeschlossen werden kann, ist eine Fehlermeldung auszugeben. Sollte die Entschlüsselung nicht erfolgreich sein, so muss eine Fehlermeldung ausgegeben werden und der Empfangsvorgang ist abzubrechen. In diesem Fehlerfall bleibt die S/MIME-Nachricht auf dem KV-Connect Server gespeichert.

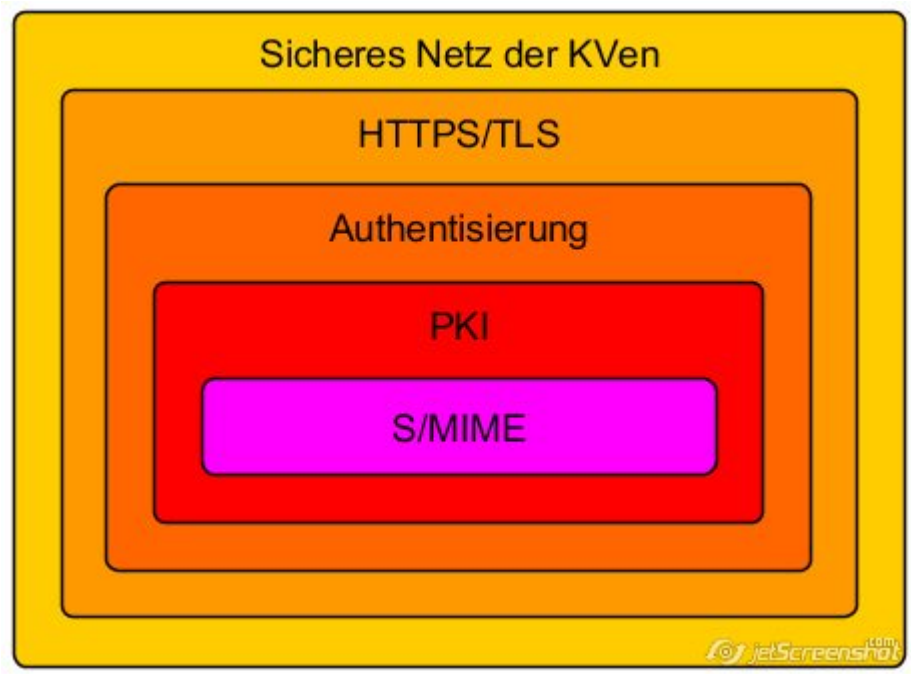
6.2.2 Ablaufdiagramme

Die Ablaufdiagramme, die den Empfang und den Versand mithilfe der REST-Serverschnittstelle aufzeigen, liegen als eigenständige PDF-Dokumente vor.

7 Datenschutz und Datensicherheit

Es sind technische und organisatorische Maßnahmen in KV-Connect ergriffen worden, um die Integrität und Vertraulichkeit des Nachrichtenaustausches zwischen Teilnehmern im Gesundheitssystem zu erreichen. So gibt es in der Kommunikation zwischen *KV-CONNECT*-Client und *KV-CONNECT*-Server mehrere Ebenen zur Gewährleistung des Datenschutzes und der Datensicherheit. Jede Ebene enthält mindestens eine Maßnahme zum Datenschutz und zur Datensicherheit.

Abb. 1: Ebenen-Übersicht



- Authentisierung: Relevante Aktionen erfordern eine Benutzerauthentisierung und -autorisierung, Ausnahmen sind z.B. der Abruf der Serverversion
- PKI: Voraussetzung für die Benutzung von S/MIME.
- S/MIME: der technische Standard für die Verschlüsselung und Signatur von Nachrichten.

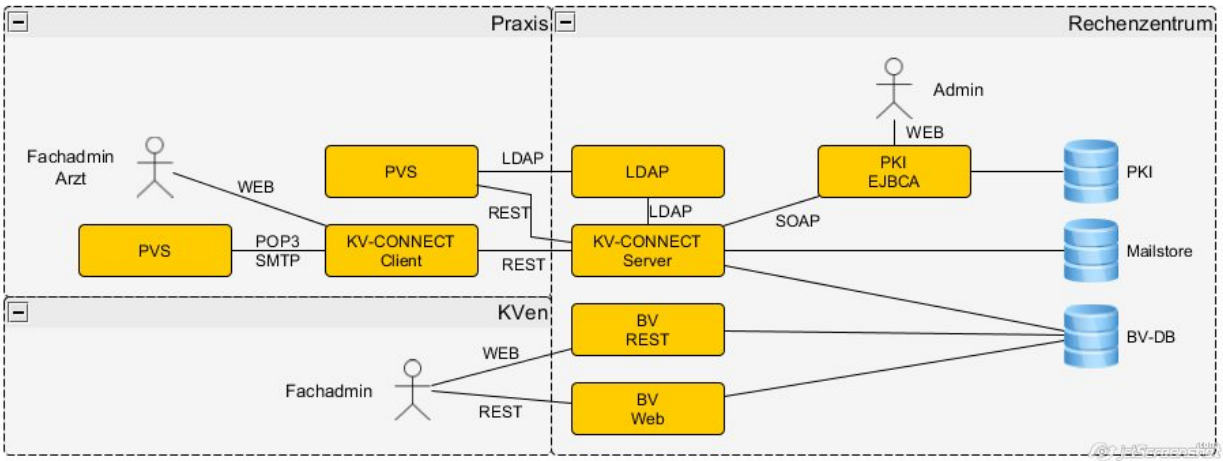
7.1 sicheres Netz der KVen (SNK)

Grundsätzlich ist KV-Connect nur im SNK verfügbar, so dass hier ein erster Schutz vor äußeren Angriffen vorliegt. Die Verbindung findet für alle Beteiligten innerhalb eines virtuellen privaten Netzwerks (VPN) statt. Dabei kommt entweder das KV-SafeNet mit einem VPN auf IPSec-Basis oder das KV-FlexNet mit einem VPN auf HTTPS-Basis zum Einsatz. Diese logische Trennung vom Internet verhindert den Zugriff von außen auf die Verbindung zwischen Client und Server.

Des Weiteren erhalten ausschließlich berechtigte Nutzer Zugang zum SNK. Das sind in erster Linie Vertragsärzte und Vertragspsychotherapeuten. Andere Teilnehmer wie Apotheker können nach besonderer Prüfung durch die KVen einen Zugang erhalten.

7.2 HTTPS/TLS

Im KV-Connect Gesamtsystem sind viele verschiedene Systeme beteiligt, die miteinander kommunizieren. Sämtliche Kommunikation zwischen Systemen findet grundsätzlich verschlüsselt statt. Das dabei verwendete Zertifikat verschlüsselt die Daten und stellt sicher, dass sich der Client mit einem bekannten Server verbindet.



7.3 Authentisierung

Der Datenaustausch zwischen Client und Server geschieht über REST-Webservices. Dabei findet eine Token-basierte Authentifizierung statt, die dafür sorgt, dass nur bekannte Benutzer Nachrichten verschicken oder empfangen können. Das Token wird von einem Secure Token Server (STS) erstellt, gegen den sich der Benutzer mit Login und Kennwort authentifizieren muss.

7.4 PKI

Die existierende PKI stellt für angemeldete Benutzer Zertifikate aus und veröffentlicht diese in einem Verzeichnisdienst (LDAP). Dies geschieht ohne manuelle Prüfung in einem automatischen Prozess. Vom KV-Connect Client wird ein üblicher Certificate Signing Request (CSR) erwartet, der vom KV-Connect Server mit Stammdaten aus der Benutzerverwaltung angereichert wird. Dazu muss lokal ein privater RSA Schlüssel erzeugt und sicher gespeichert werden. Die Verwaltung und Sicherung dieses Schlüssels obliegt dem KV-Connect Client. Die Vertrauenswürdigkeit der signierten Zertifikate ist allein von der Güte der von den KVen übertragenen Stammdaten und der Sicherheit der Authentisierung am Server abhängig.

Der Zertifikats-Request kann auch über die REST-Schnittstelle direkt aus dem Primärsystem heraus erfolgen. In diesem Fall muss das Primäsystem selbst die benötigten Funktionen zur Schlüssel-Generierung und -Verwaltung bereitstellen.

7.5 S/MIME

Alle Nachrichten werden als S/MIME signiert und verschlüsselt. Zum Einsatz kommt ein Private-Public-Key-Verfahren auf Basis von X.509-Zertifikaten. Diese Zertifikate müssen bei der ersten Anmeldung am System angefordert werden. Das Zertifkat wird von einer PKI erstellt (bzw. signiert), sofern der KV-Connect Server die darin enthaltenen Stammdaten geprüft hat. Somit ist sichergestellt, dass nur der Empfänger einer E-Mail diese mit seinem privaten Schlüssel entschlüsseln und lesen kann. Ferner ist der Absender sicher, den richtigen Empfäger anhand der Stammdaten ausgewählt zu haben.

8 Who is who bei KV-Connect

Jeder Teilnehmer ist anhand des KV-CONNECT Adressverzeichnis (wegen seiner technischen Realisierung häufig einfach als „LDAP" angesprochen) identifizierbar. In diesem kann anhand des Namens und weiterer Attribute des Teilnehmers gesucht werden.

Bisher haben noch nicht alle Praxisverwaltungssysteme einen Zugriff auf dieses Verzeichnis implementiert. Aus diesem Grund stellt die KV Telematik eine Anwendersuche im KV-SafeNet zur Verfügung, welche mit einem herkömmlichen Web-Browser aufgerufen werden kann. Der Link dazu heißt https://suche.kv-connect.kv-safenet.de/webvzd/.

Es sind nur diejenigen Teilnehmer im LDAP und in der Anwendersuche auffindbar, die sich mindestens einmal an ihrem Konto angemeldet und ein Zertifikat erzeugt haben.

Die Existenz einer KV-CONNECT Adresse sagt alleine noch nichts darüber aus, dass die damit verbundene Praxis bzw. verbundende Arzt auch tatsächlich bereit ist, über diesen „Briefkasten" Nachrichten entgegen zu nehmen. Sowohl die technischen Möglichkeiten (Implementierung im PVS) als auch die persönliche Bereitschaft des Arztes bzw. der Praxis können dem entgegenstehen. Deshalb darf sich der sendende Teilnehmer *a priori* nicht auf die Zustellung einer Nachricht verlassen; er muss bei Bedarf selber sicherstellen, dass der Empfänger über seine KV-CONNECT Adresse Nachrichten empfangen möchte und auch technisch dazu in der Lage ist.