Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Konzept IP-Adressvergabe

[KBV_SNK_KNEX_IP-Adressvergabe]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.1
Datum:	31.10.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
V1.1	31.10.2011	KBV	Dokumentenlenkung und Anpassung der Präambel		Alles
V1.0	13.03.2009	KBV	Intiales Dokument		Alles

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 Präambel

1.1 Das *Sichere Netz der KVen*

Die Kassenärztliche Bundesvereinigung und die Kassenärztlichen Vereinigungen haben eine Online-Infrastruktur aufgebaut, die den hohen Anforderungen an Datenschutz und Datensicherheit Rechnung trägt und die u.a. für die Übermittlung von Patienten- und Honorardaten geeignet ist – das *Sichere Netz der KVen*.

Informationssicherheit im *Sicheren Netz der KVen* ist eines der wichtigsten Ziele aller Beteiligten. Von besonderer Bedeutung ist dabei der Schutz der Sozialdaten und weiterer personenbezogener Daten. Für diese und andere Informationen und Werte werden im Rahmen des Sicherheitsmanagements Schutzziele definiert. Im Mittelpunkt dabei stehen die Sicherung der Vertraulichkeit, die Gewährleistung der Integrität und die Aufrechterhaltung der Verfügbarkeit. Zur Einhaltung dieser Ziele trifft die KBV regulatorische Maßgaben in Form von Richtliniendokumenten und Zertifizierungen. Die Umsetzung obliegt allen Beteiligten.

Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind hierzu über den KV-Backbone, einem logisch vom Internet getrennten Netzwerk, miteinander verbunden. Die KBV ist der Betreiber des KV-Backbones.

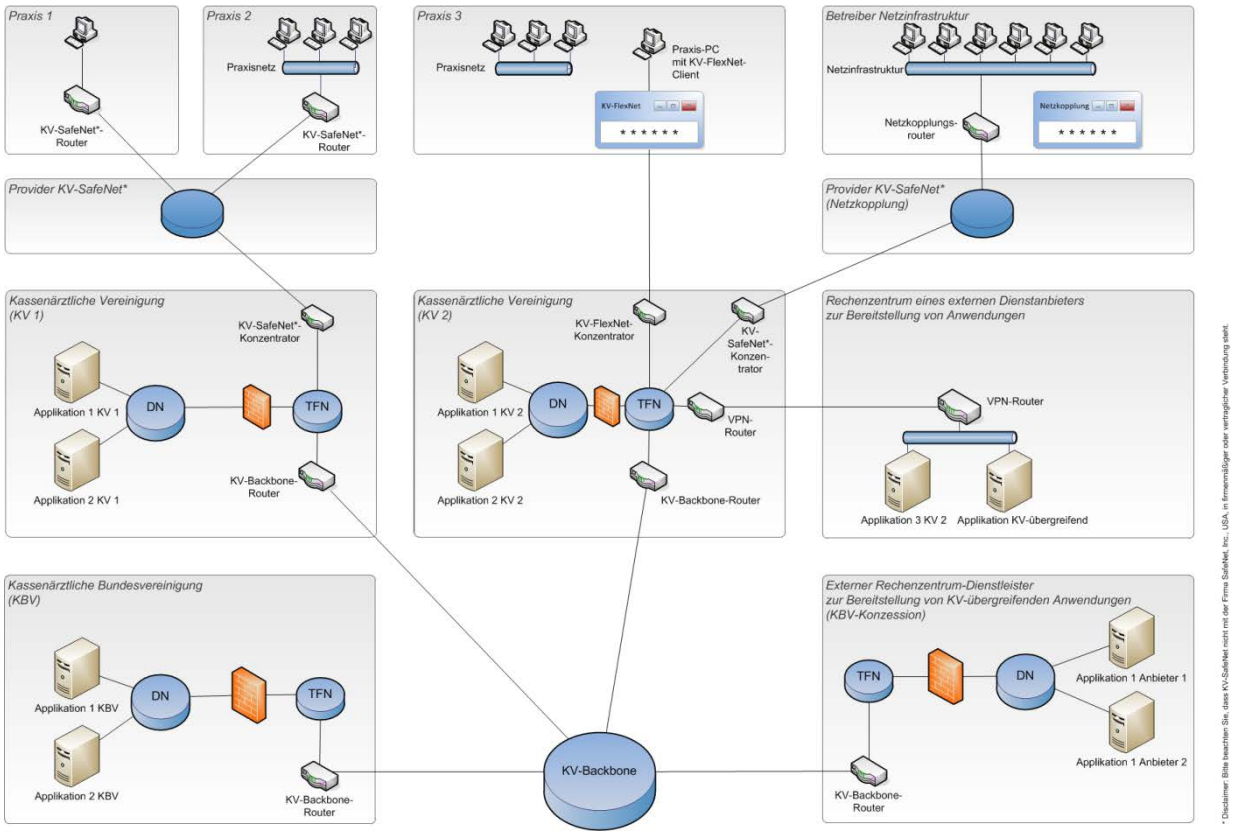

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am *Sicheren Netz der KVen* sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*. Ihnen werden sichere Zugangswege zu den Diensten und Anwendungen bereitgestellt. Die Anbindung der Teilnehmer an das *Sichere Netz der KVen* erfolgt mittels einer VPN-Verbindung. Es gibt hierbei zwei Mög-

lichkeiten der sicheren Anbindung, einerseits über das KV-SafeNet*, einem Hardware-VPN und andererseits über das KV-FlexNet[1] einem Software-VPN. Die Bereitstellung eines Zugangs über die Variante KV-FlexNet liegt in der Hoheit der jeweiligen KV. Beide Zugangsvarianten ermöglichen eine sichere Anbindung an das *Sichere Netz der KVen*.

Der Anschluss von Teilnehmern aus bereits in sich abgesicherten gesundheitsmedizinischen Netzinfrastrukturen an das *Sichere Netz der KVen* erfolgt mittels KV-SafeNet (Netzkopplung). Diese gesicherte Anbindung basiert auf der Zugangsvariante KV-SafeNet und erweitert diese um einen Authentisierungsdienst.

Im *Sicheren Netz der KVen* werden den Teilnehmern von den KVen und der KBV Dienste und Anwendungen zur Verfügung gestellt, die mit dem Begriff Applikationen (oder auch KV-Apps) zusammengefasst werden. Es besteht auch für KV-fremde Dienstanbieter die Möglichkeit, Dienste anzubieten, Voraussetzung hierfür ist eine Zertifizierung der betreffenden Applikation durch die KBV.

Der Anschluss mittels KV-SafeNet erfolgt durch einen von der KBV zertifizierten Provider. Dieser stellt einem Teilnehmer alle technischen Voraussetzungen zur Anbindung an das *Sichere Netz der KVen* mittels einer Hardware-VPN-Lösung zur Verfügung und garantiert für die Sicherheit dieser Verbindung. Der Provider stellt dem Teilnehmer hierzu einen KV-SafeNet-Router zur Verfügung.

Beim Anschluss eines Teilnehmers über KV-FlexNet stellt die jeweilige KV des Teilnehmers eine von der KBV zugelassene Software-VPN-Lösung zur Verfügung und garantiert für die Sicherheit der Verbindung.

1.2 Ziel des Dokuments

Ziel dieses Dokuments ist es, das dem *Sicheren Netz der KVen* zugrundeliegende IP-Adresskonzept einerseits, und andererseits den Prozess der Beantragung von IP-Adressräumen zur Adressierung von Applikationen und Teilnehmern, darzulegen.

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an alle am *Sicheren Netz der KVen* beteiligten Akteure, insbesondere an Provider, KVen und Applikationsanbieter.

* Disclaimer: Bitte beachten Sie, dass KV-SafeNet nicht mit der Firma SafeNet, Inc., USA, in firmenmäßiger oder vertraglicher Verbindung steht.
[1] In der jeweiligen KV kann diese Lösung auch einen anderen Namen haben.

2 IP-Adressvergabe

2.1 IP-Adressen im *Sicheren Netz der KVen*

Die notwendige Adressierung der Teilnehmer des *Sicheren Netzes der KVen* sowie der angebotenen Dienste über die verfügbaren privaten IP-Adressbereiche ist nicht empfehlenswert, da davon auszugehen ist, dass diese Adressbereiche häufig zur Adressierung von LANs der zur Nutzung des *Sicheren Netzes der KVen* berechtigten Institutionen im Einsatz sind und damit die Gefahr auf Netzkollisionen (z.B. bei Nutzung eines Dienstes) gegeben wäre. Diese Gefahr könnte durch eine übergreifende Erfassung und Abstimmung der sich im Einsatz befindlichen privaten Adressbereiche beseitigt werden, allerdings wäre dieser Vorgang unverhältnismäßig arbeits- und kostenintensiv. Daher hat sich die KBV dazu entschlossen, öffentlichen IP-Adressen für das *Sichere Netz der KVen* einzusetzen, welche von der KBV vergeben und organisiert werden. Alle Teilnehmer und Dienste des *Sicheren Netzes der KVen* müssen mit öffentlichen IP-Adressen des für den KV-Backbone zu Verfügung stehenden Adressraums adressiert werden. Die Verwendung von privaten IP-Adressen zur Adressierung von Teilnehmern und Diensten ist ausgeschlossen.

2.1.1 Einsatz der IP-Adressen

Die zur Adressierung von Teilnehmern und Diensten zugeteilten IP-Adressbereiche sind exklusiv für das *Sichere Netz der KVen* und dürfen ausschließlich in diesem Kontext verwendet werden. Eine Nutzung dieser Adressbereiche zu anderen als dem vorgegebenen Zweck ist untersagt. Die KBV behält sich das Recht einer Überprüfung dieser Anforderung vor.

2.1.2 Teilnehmeranschluss-IP-Adressen

Teilnehmeranschluss-IP-Adressen werden zur Adressierung der Teilnehmeranschlüsse benötigt. Dabei handelt es sich um die VPN-seitige Adressierung der Zugangskomponente im Teilnehmer LAN.

2.1.3 Service-IP-Adressen

Diese IP-Adressen werden zur Adressierung der Applikationsserver benötigt, auf den die Clients zugreifen. Da hier die Kommunikation eingehend geschieht, ist für jeden Applikationsserver eine eigene IP-Adresse notwendig. Um das Problem von IP-Adress-Konflikten mit den Praxen lösen, müssen hier öffentliche IP-Adressen verwendet werden.

Hinweis: Bei Webservern kann je nach Sicherheitsanforderung die Anzahl der benötigten IP-Adressen durch die Verwendung von anderen TCP-Ports, dem Einsatz von NAT oder reverse-Proxies erheblich reduziert werden. Hierzu muss jedoch die Struktur und Konzeption der Server betrachtet und ggf. angepasst werden, weshalb diese Methoden hier nicht berücksichtig werden. Für die Zukunft sollten die KVen dies für die Applikationen jedoch berücksichtigen.

2.1.4 Transfer-IP-Adressen

Um IP-Netze miteinander zu koppeln, werden Router benötigt. Diese wiederum werden über Transfernetze miteinander verbunden. In diesen Netzen benötigen die Router entsprechend IP-Adressen. Transfernetze existieren in jeder teilnehmenden KV. Über dieses Netz wird der Router des Servicenetzes mit dem KV-Backbone-Router verbunden. Bei Knotenbetreibern sind darüber hinaus die Konzentratoren der Zugangsprovider an das Transfernetz angeschlossen.

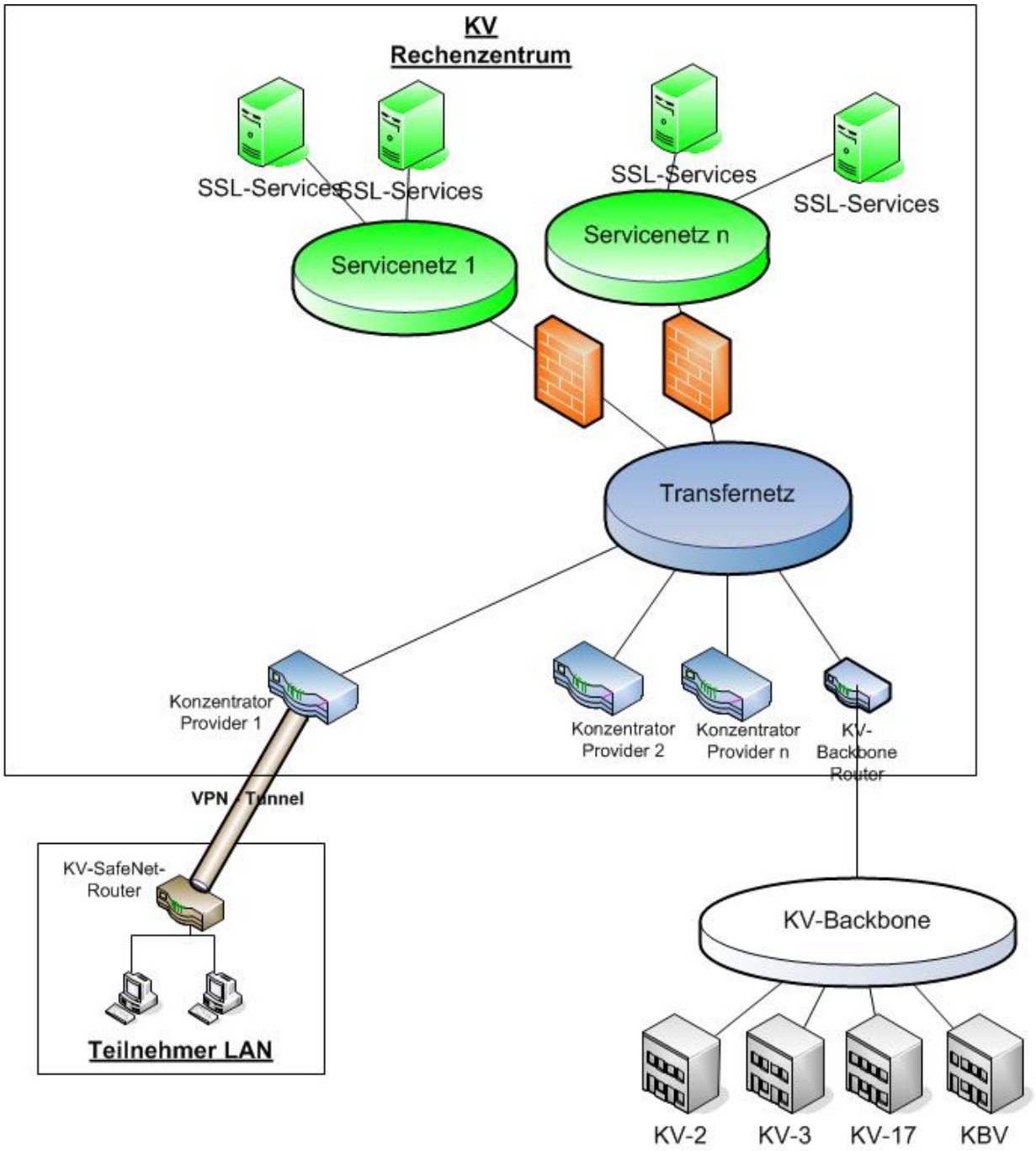

Abbildung 2: Darstellung der verschiedenen Teilnetze im *Sicheren Netz der KVen*

2.2 Dimensionierung

Ziel des *Sicheren Netzes der KVen* ist die Anbindung aller Vertragsärzte und Vertragspsychotherapeuten an die Rechenzentren der KVen sowie die Vernetzung aller KV-Rechenzentren. Um alle Teilnehmern und Dienste adressieren zu können wird ein Netzblock entsprechender Größe benötigt. Dieser Netzblock wird in passend große Subnetze zerlegt und KVen und Zugangsprovidern seitens der KBV entsprechend ihrer Angaben zugeteilt.

2.2.1 Teilnehmer-IP-Adressen

Um bundesweit alle Vertragsärzte und Vertragspsychotherapeuten anzubinden, werden bis zu 130.000 öffentliche IP-Adressen benötigt.

2.2.2 Service IP-Adressen

Zur Adressierung der im sicheren Netz der KVen angebotenen Dienste werden bis zu 1024 öffentliche IP-Adressen benötigt.

2.2.3 Transfer-IP-Adressen

Für die vorhandenen Transfernetze der KV-Rechenzentren werden ebenfalls bis zu 1024 öffentliche IP-Adressen benötigt.

2.3 Beschaffung von IP-Adressen

Aufgrund der Größe des benötigten öffentlichen IP-Adressraums ist die KBV der Organisation RIPE NCC als LIR (Local Internet Registrar) beigetreten. Als LIR erhält die KBV die Möglichkeit einen PA (Provider Aggregatable) IP-Adressraum zu beantragen, um diesen selbstständig zu verwalten. Die Vergabe der IP-Bereiche sowie die Auslastung dieser müssen sowohl bei RIPE NCC als auch bei der KBV genau dokumentiert werden. Die Bedarfsschätzung ergibt sich aus der Übermittlung der aktuell benötigten IP-Adressen in Kombination mit der geschätzten Bedarfsentwicklung für die nächsten zwei Jahre. Die folgende Abbildung stellt den Prozess der Beantragung bzw. Erweiterung des IP-Adressraums für alle Beteiligten dar. Beide grundsätzlichen Möglichkeiten der Erweiterung und Vergabe, werden in den folgenden Abschnitten detaillierter beschrieben.

1. Initiale Adressvergabe und
2. Erweiterung des vorhandenen Adressraums.

2.3.1 Initiale Adressvergabe

1. Initiale Bestellung des Bedarfs an KBV
2. Übermittlung des Bedarfs an KBV
    a. Plausibilitätsprüfung KBV
        i. Bedarf i.O.
        ii. Fehler in Bedarfsübermittlung → Korrektur durch Provider
3. Genehmigung des Adressraums KBV
        i. Zuweisung der Adressen durch KBV
4. Information des Providers

Der initiale Bedarf an IP-Adressen wird mittels einer Excel-Tabelle (siehe Tabelle 1) an die KBV (snk-services@kbv.de) übermittelt (Schritt 2).

Dabei muss eine Schätzung des Bedarfs an IP-Adressen innerhalb der nächsten sechs Monate, innerhalb des nächsten Jahres und innerhalb der nächsten zwei Jahre angegeben werden. Die folgende Tabelle gibt die Struktur der Exceldatei beispielhaft wieder:

Standort der KV	Auslastung des Netzblocks	Aktuelle Netzblockgröße	Benötigte IP-Adressen	Schätzung zusätzliche benötigte IP Adressen für die kommenden 6 Monate	Schätzung zusätzliche benötigte IP Adressen für die kommenden 12 Monate	Schätzung zusätzliche benötigte IP Adressen für die kommenden 24 Monate
KV X	80%	/24[2]	/24[2]	/24[2]	/23[2]	/23[2]

Tabelle 1: IP-Bedarfstabelle inklusive Bedarfsschätzung für die nächsten zwei Jahre

Nach der Übermittlung des Bedarfs an IP-Adressen erfolgt eine Plausibilitätsprüfung (Schritt 2(a)) des übermittelten Bedarfs durch die KBV. Im Fall einer fehlerfreien Übermittlung wird die Bedarfsmeldung bei der KBV intern dokumentiert und im Anschluss dem beantragenden Provider mitgeteilt.

2.3.2 Erweiterung des vorhandenen IP-Adressraums

1. Erweiterung des IP-Adressraums
    a. Auslastung IP-Adressraum 80% oder höher?
        i. Ja
        ii. Nein → Information des Providers. Keine Erweiterung.
2. Übermittlung des Bedarfs an KBV
    a. Plausibilitätsprüfung KBV
        i. Bedarf i.O.
        ii. Fehler in Bedarfsübermittlung → Korrektur durch Provider
3. Genehmigung des Adressraums (KBV)
        i. Zuweisung der Adressen durch KBV
4. Information des Providers

Die Erweiterung des vorhandenen IP-Adressraums verläuft analog zum Prozess der initialen Bestellung von Adressräumen. Es gibt im Vergleich zum bereits beschriebenen Vorgehen nur eine Anpassungen. Der Provider muss nachweisen, dass der von ihm verwendete Adressraum zu mindestens 80% ausgelastet ist. Ist das der Fall, steht der Beantragung einer Erweiterung des bestehenden IP-Adressraums nichts mehr im Weg.

2.3.3 Freigabe von IP-Adressen

Für den Fall, dass ein Provider sein Angebot einstellt und keine gültigen, laufenden Verträge mehr hat besteht die Verpflichtung zur Freigabe der von der KBV bezogenen IP-Adressbereiche. Die Freigabe dieser Adressbereiche wird in den Datenbanken von KBV und RIPE NCC dokumentiert und können danach einem anderen Provider zur Verfügung gestellt werden.

[2] Angabe der Netzgröße mit Hilfe der sogenannten „Slash Notation“ (http://de.wikipedia.org/wiki/Netzmaske)

3 Glossar

Begriff	Erklärung
Anbieternetz	Zum Netz des Anbieters zählen alle notwendigen Dienste und Infrastrukturelemente, die zur Einrichtung, Aufrechterhaltung und Wartung der KV-SafeNet Anbindung zwischen Teilnehmer und KV notwendig sind.
Applikation	Services und Anwendungen im *Sicheren Netz der KVen*
Applikationsanbieter	Anbieter eines Dienstes
Dienstenetz (DN)	Das Dienstenetz ist das Netz der Services und Anwendungen. Hier werden alle Anwendungsserver des *Sicheren Netzes der KVen* installiert und verfügbar gemacht. Die Organisation des Dienstenetzes liegt in der Verantwortung der Applikationsanbieter bzw. des Rechenzentrumsdienstleisters.
Einwahlknoten / Konzentrator	Der Einwahlknoten ist der Endpunkt des Anbieternetzes, der in der KV installiert ist und den Übergang vom Anbieternetz zum *Sicheren Netz der KVen* darstellt.
Firewall	Eine Firewall dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall unerlaubte Netzwerkzugriffe zu unterbinden.
Firmware	Firmware bezeichnet Software, die in elektronische Geräte fest eingebettet und somit mit dem Gerät untrennbar verbunden ist. Eine Firmware benötigt u.U. in regelmäßigen Abständen ein Update.
Fremdprovider / VPN-Provider	Ein VPN-Provider stellt im Gegensatz zum ISDN, DSL oder UMTS Provider nicht die technischen Voraussetzungen bzgl. der Übertragungstechnik zur Verfügung, sondern nutzt eine bereits bestehende Internetverbindung.
KV-App	Siehe Applikation.
KV-Backbone	Der KV-Backbone ist ein geschütztes, logisch vom Internet getrenntes, vollvermaschtes VPN-Netzwerk auf Basis eines von der KBV definierten Konzeptes. Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind über den KV-Backbone miteinander vernetzt. Die KBV ist der Betreiber des KV-Backbones.
KV-FlexNet	Anbindungsmöglichkeit eines Teilnehmers an das *Sichere Netz der KVen* mittels einer Software-VPN-Lösung. Der Anschluss erfolgt über die KV des Teilnehmers.
KV-SafeNet	Anbindungsmöglichkeit eines Teilnehmers an das *Sichere Netz der KVen* mittels einer Hardware-VPN-Lösung, dem KV-SafeNet-Router. Der Anschluss erfolgt über einen KV-SafeNet-Provider.
KV-SafeNet-Provider	Von der KBV nach der KV-SafeNet-Richtlinie zertifizierter Provider, der Teilnehmern einen Zugang über die Anschlussvariante „KV-SafeNet“ zum *Sicheren Netz der KVen* ermöglicht.
KV-SafeNet-Router	Ein KV-SafeNet-Router ist ein nicht manipulierbarer Router. Dieser wird zwischen Internetanschluss und Praxisnetzwerk geschaltet. Dieser Router baut ein virtuelles privates Netzwerk (VPN) zu einem Einwahlknoten in der KV auf, welches die Verbindung vom normalen Internet abschottet und so einen abgesicherten Datenaustausch mit dem *Sicheren Netz der KVen* ermöglicht. Gleichzeitig blockiert der Router den Zugriff von außen auf das Praxis-Netzwerk und die dortigen Daten, da er den Zugriff aus dem Anbieternetz in das Teilnehmernetz verhindert. Die Verantwortung für den KV-SafeNet-Router trägt der KV-SafeNet-Provider.

Begriff	Erklärung
Servicenetz	Siehe Dienstenetz
Sicheres Netz der KVen	Das *Sichere Netz der KVen* ist eine von der KBV und den KVen bereitgestellte Infrastruktur, bestehend aus einem vollvermaschten VPN-Netzwerk (KV-Backbone), im Netzwerk befindlichen Diensten und Anwendungen (KV-Apps) und den definierten Anbindungsmöglichkeiten an das Netzwerk (KV-SafeNet und KV-FlexNet). Diese Infrastruktur trägt den Anforderungen an Datenschutz und Datensicherheit Rechnung und ist für die Übermittlung von Sozialdaten geeignet.
Teilnehmer	Ein Teilnehmer ist ein Vertragsarzt, -psychotherapeut oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*. Grundsätzlich bestimmen die KVen den Teilnehmerkreis.
Teilnehmernetz	Die untereinander lokal vernetzten Teilnehmercomputer bilden das Netzwerk des Teilnehmers. Hier können sich weitere vernetzte Endsysteme (z.B. Server, Drucker, Kartenleser) befinden.
Transfernetz (TFN)	Das Transfernetz dient der Weiterleitung der Datenpakete vom Teilnehmer zu den Applikationsservern und zurück. Es wird durch den KV-Backbone-Router realisiert. Die Organisation des Transfernetzes liegt in Verantwortung des KV-Backbone-Betreibers.
Tunnel / VPN-Tunnel	Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt. Daher spricht man bei VPN vom Tunnel.
Zertifizierung	Prozess in dem explizit nachgewiesen wird, wie der Antragsteller die in der Richtlinie geregelten Anforderungen umsetzt. Wird dieses Verfahren erfolgreich abgeschlossen, erhält der Antragsteller eine Konformitätserklärung.
Zugangsnetz	Dazu gehören Netzelemente und Vermittlungsstellen, die Grundlagen der techn. Infrastruktur zwischen Anbieter- und Teilnehmeranschluss schaffen.