Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Konzept Routing

[KBV_SNK_KNEX_Routing]

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
1.1	31.10.2011	KBV	Dokumentenlenkung und Anpassung der Präambel		alles
1.0	23.03.2009	KBV	Initiales 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.

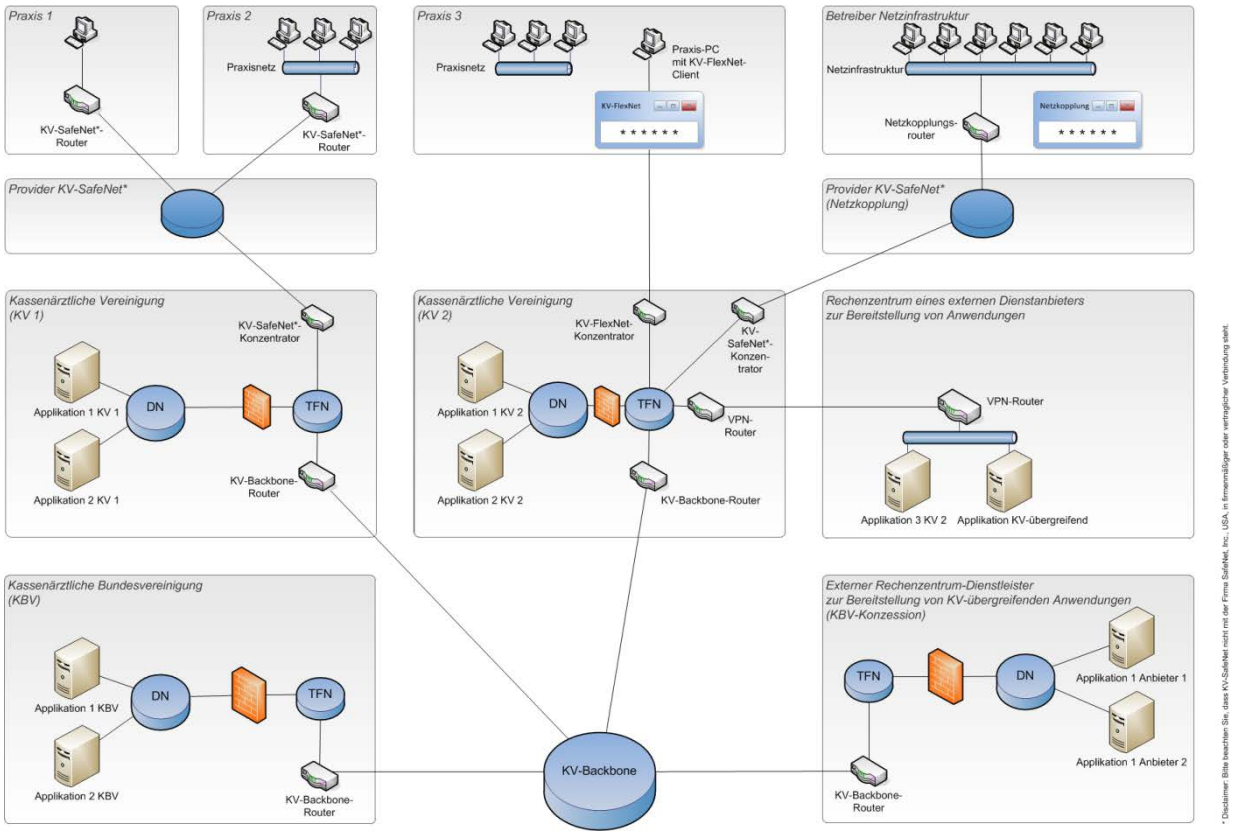

Abbildung 1: Beispielhafte Netztopologie

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, die dem *Sicheren Netz der KVen* zugrundeliegende Routingstrategie 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 Regelungen

2.1 Grundsätzliche Annahmen

2.1.1 IP-Adressen: Dienste, Teilnehmer NAT

Grundsätzlich sind alle Dienste und Teilnehmer des *Sicheren Netzes der KVen* mit dem für den KV-Backbone zur Verfügung stehenden, öffentlichen IP-Adressraum adressiert. Die Verwendung von privaten IP-Adressen ist ausgeschlossen.

Zur Sicherstellung der Interoperabilität sollten KV-SafeNet-Provider, mit einer gültigen Zertifizierung vor der Version 3.0 der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet], dringend die Migration in den öffentlichen IP-Adressraum durchführen.

2.1.2 Verfügbarkeit bzw. Integration der Knoten

Für das Routing von Teilnehmern eines Knotens zu Diensten eines anderen Knotens, darf die Infrastruktur des jeweiligen Knotens (z.B. lokale Firewalls und Router, die nicht vom KV-SafeNet- bzw. KV-FlexNet-Provider gestellt werden) keinerlei Rolle spielen. Sie ist ausdrücklich aus dem übergreifenden Datentransfer auszuschließen, d.h. konkret, dass der Betreiber eines Knotens nicht in den Datenverkehr, der nicht für ihn bestimmt ist, eingreifen (manipulieren, filtern oder überwachen) darf. Somit ist gewährleistet, dass im Fehlerfall ausschließlich der Betreiber des KV-Backbone und die an den jeweiligen Knoten angeschlossenen Provider verantwortlich sind. Des Weiteren ist sichergestellt, dass ein Knoten den Datenfluss zu einem anderen Knoten nicht manipuliert, filtert, überwacht oder in irgendeiner Form beeinflusst. Grundsätzlich ist somit festzuhalten, dass die Kommunikation zwischen einem Teilnehmer und einem beliebigen Dienst im *Sicheren Netz der KVen* in keinerlei Form durch einen Knoten beeinträchtigt bzw. überwacht wird.

2.2 Routingkonzept

Basierend auf die Ermittlung der möglichen Routingmechanismen in den einzelnen KVen ist es nicht möglich grundsätzlich von dynamischen Routing zur Anbindung der Dienstenetze der KVen auszugehen. Es wird allerdings sichergestellt, dass in den KV-Rechenzentren mit KV-SafeNet- und / oder KV-FlexNet-Provideranbindungen dynamische Routingprotokolle unterstützt werden. Da im *Sicheren Netz der KVen* ausschließlich öffentliche Adressen zur Anbindung von Diensten und Teilnehmer genutzt werden, ist statisches Routing bei den Anbietern von Diensten und in den KV-Rechenzentren mit geringem Aufwand zu realisieren.

Im Weiteren wird zwischen KV-SafeNet- und KV-FlexNet-Providern bzgl. der einzusetzenden Routingstrategie unterschieden. Dynamisches Routing ist für KV-SafeNet-Provider verpflichtend und für KV-FlexNet-Provider optional.

2.2.1 Routingstrategie: Statisch vs. Dynamisch

Im Sinne eines störungsfreien, einfach geregelten Routingprozesses ist das Routingprotokoll BGPv4 eingeführt worden. Das Border Gateway Protocol (BGP) beschreibt, wie Router untereinander die Verfügbarkeit von Verbindungswegen zwischen den Netzen autonomer Systeme („AS“) propagieren.

Die KV-Knoten können sich individuell am dynamischen Routing beteiligen. Der Zugangsprovider hat dafür zu sorgen, dass der Teilnehmer das Routing und die damit erreichbar gemachten Dienste / KV-Rechenzentren ohne Einschränkungen nutzen kann.

2.2.2 Routingstrategie für das *Sichere Netz der KVen*

Die zur Umsetzung des Routingprotokolls benötigte BGP AS Nummer für den Adressraum des *Sicheren Netzes der KVen* wird zentral von der KBV bei der RIPE NCC beantragt. KV-SafeNet-Provider benötigen eigene BGP AS Nummern zur Umsetzung des geplanten Routings auf Basis des Protokolls BGPv4. Sollte es KV-SafeNet-Provider ohne eine eigene öffentliche BGP AS Nummer geben, so wird diesen Providern eine Nummer aus dem Raum der privaten BGP AS Nummern von der KBV zugewiesen. Die KBV fungiert somit als zentrale Koordinierungsstelle der am System beteiligten BGP AS Nummern und kann die doppelte Vergabe aus dem Raum der privaten Nummern vermeiden.

2.2.3 Routingvorgaben für Transfernetze von KBV und KVen

Das Transfernetz wird durch den KV-Backbone-Router aufgespannt und in das Routing des KV-Backbones integriert. Alle im Transfernetz befindliche Hardware ist damit im *Sicheren Netz der KVen* zu erreichen. Im Transfernetz werden VPN-Konzentratoren der Zugangsprovider (KV-SafeNet und KV-FlexNet) sowie die Tunnelendpunkte eventuell angeschlossener externer Rechenzentren betrieben.

Die Zugangsknotenbetreiber stellen für Installation und Betrieb der VPN-Konzentratoren der Provider die notwendigen Räumlichkeiten zur Verfügung. Das Routing zur Anbindung dieser VPN-Konzentratoren an den KV-Backbone soll auf Basis des Routingprotokolls BGPv4 erfolgen.

2.2.4 Routingvorgaben für Dienstenetze von KBV und KVen

Das Dienstenetz ist ein vom Transfernetz getrenntes Teilnetz zur Platzierung von Applikationen. Dieses Netz ist über einen Netzübergang (Firewall oder Router) mit dem Transfernetz verbunden ist. Zwischen Netzübergang und KV-Backbone-Router wird statisch geroutet.

2.2.5 Routingvorgaben für KV-SafeNet-Provider

Das Routing für die von KV-SafeNet-Providern angebundenen Teilnehmer am *Sicheren Netz der KVen* soll durch Einsatz des Routingprotokolls BGPv4 erfolgen. Statisches Routing ist für KV-SafeNet-Provider nicht zulässig.

2.2.6 Routingvorgaben für KV-FlexNet-Provider

Das Routing für die von KV-FlexNet-Providern angebundenen Teilnehmer am *Sicheren Netz der KVen* erfolgt statisch. Der Einsatz des Routingprotokolls BGPv4 ist optional.

2.2.7 Routingvorgaben für externe Applikationsanbieter

Applikationen externer Applikationsanbieter, welche im Rechenzentrum des Anbieters betrieben werden, werden mittels statischen Routen an ein beliebiges Transfernetz, und damit an den KV-Backbone angebunden.

2.2.8 Routingvorgaben für externe Rechenzentren

Der Rechenzentrum-Dienstleister wird mittels eines KV-Backbone-Routers an das Sichere Netz der KVen angeschlossen. Der KV-Backbone-Router spannt das Transfernetz auf. Gesonderte Routingvorgaben für das Transfernetz sind nicht notwendig, da das Routing direkt vom KV-Backbone-Router realisiert wird.

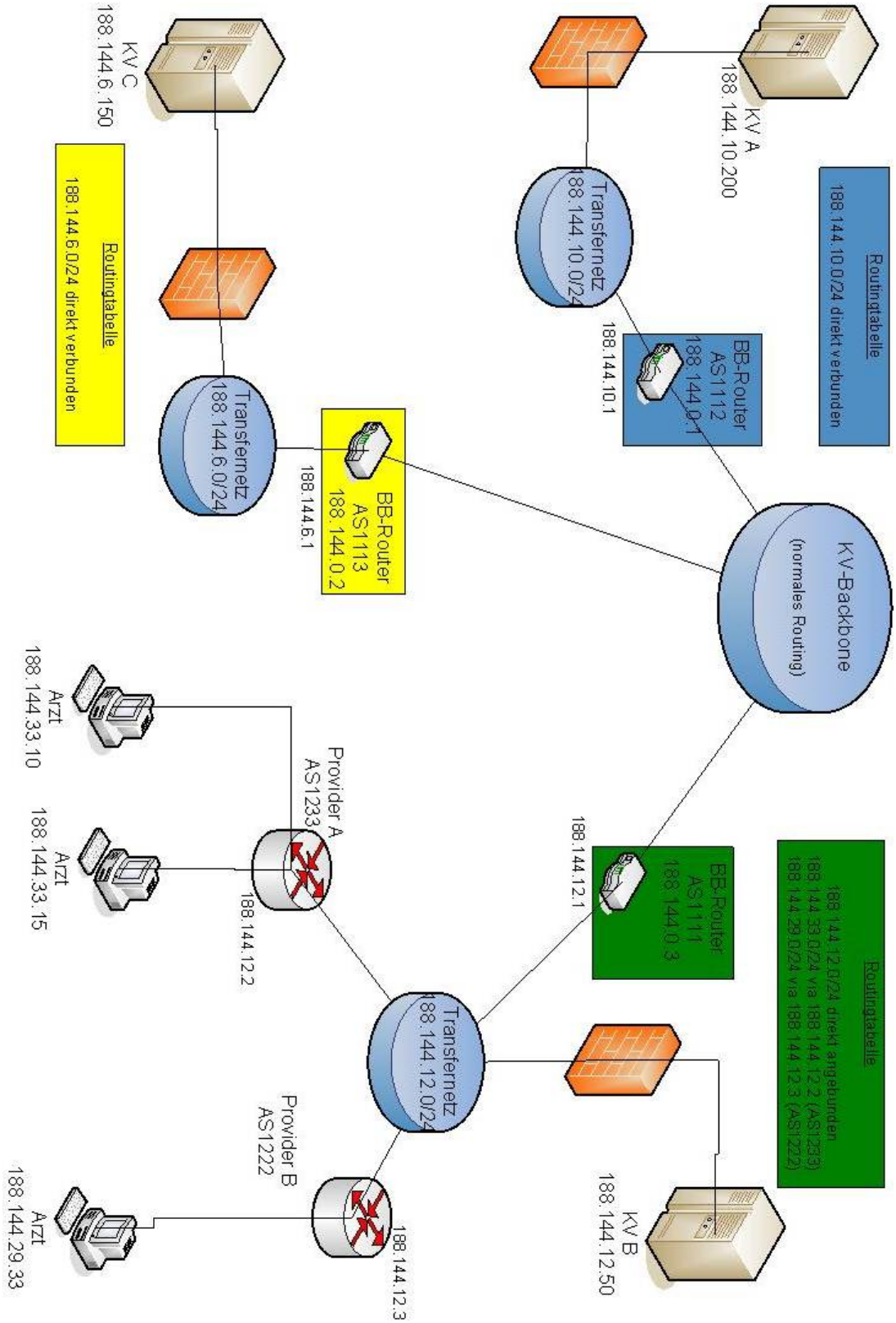

Abbildung 2: Routing im *Sicheren Netz der KVen* mit beispielhaften IP-Adressen und Routingtabellen

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.
Dienst	Services und Anwendungen der KVen und der KBV.
Dienstanbieter	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.
Fault-, bzw. Anti-Fraud Systeme	Diese Managementsysteme dienen der Vorbeugung, Entdeckung und adäquaten Reaktion von Computer- bzw. Wirtschaftskriminalität. Dazu gehören u. a. Ausspähen von vertraulichen Informationen, unerlaubtes Modifizieren der Daten oder der Verlust von Daten.
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 Dienst.
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 zum *Sicheren Netz der KVen* ermöglicht.

Begriff	Erklärung
KV-SafeNet-Router	Ein KV-SafeNet-Router ist ein nicht manipulierbarer Router. Dieser wird zwischen Telefonanschluss 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 den Rechenzentren der jeweiligen KV und der KBV 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.
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 Patienten- und Honorardaten geeignet.
Teilnehmer	Ein Teilnehmer ist eine Arztpraxis oder ein anderes nach den Maßgaben der KBV zugelassenes Mitglied des Sicheren Netzes der KVen.
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. 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 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.

4 Referenzierte Dokumente

Referenz	Dokument
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet