Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Leitfaden Zertifizierung Netzkopplungsprovider

[KBV_SNK_LFEX_Zert_Netzkopplung]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version 1.1
Datum: 30.01.2013
Klassifizierung: Öffentlich
Status: In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.1	30.01.2013	KBV	3.2 Punkte zur Vertragslaufzeit, Zertifikatsgültigkeit an Richtlinie angepasst 3.3 Erläuterung zu (7) 3.4 Erweiterung	Korrektur genauere Beschreibung der Anforderungen	10 14 14
1.0	31.10.2011	KBV	Erstellung des Dokuments, QS und Freigabe		

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.

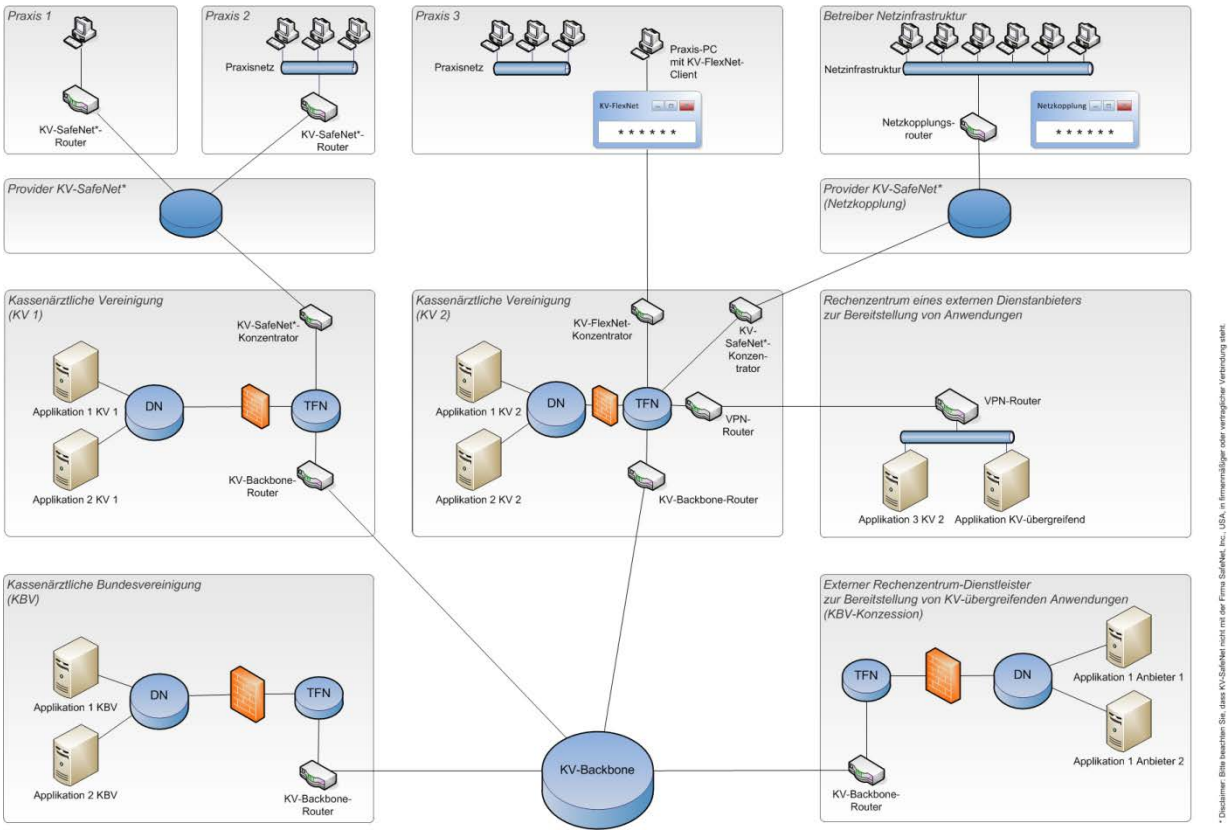

Abbildung 1: Beispielhafte Netztopologie

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

Der Leitfaden beschreibt den prozessualen Ablauf einer Zertifizierung zum Provider zur Durchführung der Netzkopplung, im folgenden Netzkopplungsprovider genannt. Hierfür werden die normativen Vorgaben der Richtlinie [KBV_SNK_RLEX_Netzkopplung] erläutert und spezifiziert. In Kapitel 2 werden die allgemeinen Regelungen zur Zertifizierung aufgeführt und in Kapitel 3 die entsprechenden Unterlagen und deren Inhalte, die ein Unternehmen bzw. Provider einreichen muss, der sich zur Durchführung der Netzkopplung zertifizieren lassen möchte.

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 bereits zertifizierte KV-SafeNet-Provider, die sich zusätzlich für die Durchführung von Netzkopplungen zertifizieren bzw.- rezertifizieren lassen möchten.

1.4 Anwendung des Leitfadens Zertifizierung KV-SafeNet

Grundsätzlich gelten alle Regelungen und damit alle Abschnitte der zum Zeitpunkt der Zertifizierung geltenden Fassung des Leitfaden Zertifizierung KV-SafeNet-Provider [KBV_SNK_LFEX_Zert_KV-SafeNet] für den Leitfaden zur Zertifizierung der Netzkopplung und sind entsprechend umzusetzen. Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in diesem Leitfaden definiert.

* 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 zur Zertifizierung

Im Folgenden werden die allgemeinen Regelungen der Zertifizierung zum Netzkopplungsprovider erläutert.

Die in der aktuell gültigen Version des Leitfadens [KBV_SNK_LFEX_Zert_KV-SafeNet] definierten Regelungen betreffend KV-SafeNet-Zertifizierung, insbesondere

- Reihenfolge
- Fristen
- Vorbehalt
- Rezertifizierung

sind auch entsprechend für die Zertifizierung zur Durchführung der Netzkopplung gültig und anzuwenden.

Die Gültigkeit des Zertifikates ist in der Richtlinie [KBV_SNK_RLEX_Netzkopplung] geregelt.

2.1 Prüfstelle

Das Formular Ergänzende Erklärung [KBV_SNK_FOEX_Netzkopplung] ist der offizielle Antrag auf Zertifizierung bzw. Rezertifizierung zum Netzkopplungsprovider. Dieses ist – ebenso wie die Datenschutzerklärung – ausgefüllt und unterschrieben auf dem Postweg über folgende Adresse einzureichen:

Kassenärztliche Bundesvereinigung K.d.ö.R.
KBV–Prüfstelle
Herbert-Lewin-Platz 2
10623 Berlin

Alle weiteren Unterlagen bzgl. der Zertifizierung zum Netzkopplungsprovider – ausgenommen das Formular Ergänzende Erklärung [KBV_SNK_FOEX_Netzkopplung] und die Datenschutzerklärung – können per E-Mail an die Prüfstelle der KBV (pruefstelle@kbv.de) gesandt werden.

Betreffzeile: „Antrag auf Zertifizierung zum Netzkopplungsprovider“.

Die Prüfstelle der KBV versendet ein Protokoll, welches den Verlauf der Prüfung wiedergibt, sobald diese als Teil oder im Ganzen abgeschlossen ist.

2.2 Kosten der Zertifizierung (Pauschale)

Art der Prüfung	Kosten in €
Erstzertifizierung	**1.560,00**
Rezertifizierung	**1.100,00**
Neues Lösungskonzept	**845,00**
Zertifizierung eines neuen Zugangsgeräts	**338,00**
Beratungsgespräch[2]	**338,00**
Verwaltungskosten	
Die Verwaltungskostenpauschale bezieht sich auf die Ausstellung von Konformitätsbescheinigungen und das Umschreiben von Prüfergebnissen (z.B. bei Wechsel der Produktverantwortlichkeit).	**120,00**

Anmerkungen

1. Die genannten Zertifizierungspauschalen verstehen sich immer zuzüglich der Verwaltungskostenpauschale pro Prüfung sowie zuzüglich der gesetzlich vorgeschriebenen Mehrwertsteuer.
2. Sofern gleichzeitig die Zertifizierung zum KV-SafeNet-Provider durchgeführt wird, verstehen sich die hier genannten Zertifizierungspauschalen grundsätzlich zuzüglich der jeweiligen Kosten für die Zertifizierung zum KV-SafeNet-Provider gemäß dem Leitfaden [KBV_SNK_LFEX_Zert_KV-SafeNet]. In diesem Fall wird die Verwaltungskostenpauschale nur einmal erhoben.

Weiterhin gelten die entsprechenden Regelungen und Anmerkungen des Leitfadens [KBV_SNK_LFEX_Zert_KV-SafeNet].

2.3 Erstzertifizierung

Grundlegend gelten die Regelungen des Leitfadens [KBV_SNK_LFEX_Zert_KV-SafeNet].

Abweichend hiervon verbleibt nach erfolgter Zertifizierung kein Gerät bei der KBV. Der Provider ist verpflichtet, die notwendigen Maßnahmen zu ergreifen, um ebenfalls zu Überprüfungszwecken innerhalb von zehn Werktagen jeden zertifizierten und im Einsatz befindlichen Gerätetyp der KBV im vollständig konfigurierten Zustand zur Verfügung zu stellen.

2.4 Zulassungsfähige Lösungen

In Abhängigkeit von den zu nutzenden Anwendungen und von der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur sind verschiedene Lösungskonzepte jeweils separat zulassungsfähig.

Der Provider erhält die Zertifizierung ausschließlich für das eingereichte Konzept und die darin spezifizierte Lösung.

[2] Das Beratungsgespräch ist eine optionale Leistung der Prüfstelle, die im Vorfeld der Zertifizierung vom Antragsteller in Anspruch genommen werden kann.

3 Einzureichende Unterlagen

Die in der aktuell gültigen Version des Leitfadens [KBV_SNK_LFEX_Zert_KV-SafeNet] definierten Regelungen betreffend KV-SafeNet-Zertifizierung, insbesondere

- Konformitätserklärung über Einhaltung des Datenschutzes
- Mustervertrag bei Einbeziehung von Erfüllungsgehilfen
- Angebot des Providers
- Dokumente zur Informationssicherheit
- Supportkonzepte
- Optionale Angaben
- Dokumentation des VPN-Konzentrators

sind auch entsprechend für die Zertifizierung zur Durchführung der Netzkopplung anzuwenden.

Ergänzende oder abweichende Regelungen werden in diesem Anschnitt definiert.

3.1 Ergänzende Erklärung

Anforderung

Einreichung des vollständig ausgefüllten Formulares Ergänzenden Erklärung [KBV_SNK_FOEX_Netzkopplung]

Erläuterung

Das Formular Ergänzende Erklärung [KBV_SNK_FOEX_Netzkopplung] ist der offizielle Antrag auf Zertifizierung bzw. Rezertifizierung zum Netzkopplungsprovider. Dieses ist ausgefüllt und unterschrieben per Post oder Fax an die Prüfstelle zu schicken (siehe 2.1).

Mit dem Formular Ergänzende Erklärung [KBV_SNK_FOEX_Netzkopplung] stimmt der Antragsteller zu, dass er die aktuell gültige Richtlinie [KBV_SNK_RLEX_Netzkopplung] ohne Einschränkungen anerkennt, sowie jegliche Änderungen, die KV-SafeNet und/oder Netzkopplungs-relevant sind, an die Prüfstelle zu melden. Dies betrifft insbesondere Änderungen an der vom Provider auf Seiten des Teilnehmers verwendeten Hardware (Netzkopplungsrouter).

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_Netzkopplung] in Abschnitt 5 (Zertifikat)

3.2 Muster des Netzkopplungsvertrags

Anforderung

Einreichung des Mustervertrags zur Netzkopplung, der folgende Mindestanforderungen erfüllt:

(1) Allein durch den Vertrag zwischen dem Provider und dem Betreiber der anzuschließenden Netzinfrastruktur entsteht dem Betreiber oder Teilnehmern aus dem Netz des Betreibers kein Anspruch gegenüber den KVen oder der KBV auf Zulassung

zum *Sicheren Netz der KVen*.

(2) Der Vertrag erhält erst mit Zulassung bzw. Zustimmung der zuständigen KV seine Gültigkeit.

(3) Der Vertrag muss die Regelungen zur Benennung und Zulassung der berechtigten Teilnehmer enthalten. Der Betreiber der anzuschließenden Netzinfrastruktur benennt die Teilnehmer. Der Provider ermöglicht den Teilnehmern den Zugang zum *Sicheren Netz der KVen*. Insbesondere muss der Vertrag berücksichtigen, dass KVen und KBV ein Recht zur Kontrolle und nachträgliche Ablehnung von Teilnehmern haben.

(4) Der Vertrag muss die Regelungen zum Kontrollrecht und Vorbehalt der KVen/der KBV bezüglich der Teilnehmer enthalten.

(5) Der Vertrag muss die Regelungen zur Authentisierung der Teilnehmer für den Zugriff zum *Sicheren Netz der KVen* enthalten. Insbesondere muss darauf hingewiesen werden, dass nur erfolgreich authentisierte Teilnehmer Zugang zum *Sicheren Netz der KVen* erhalten und dass jeder berechtigte Teilnehmer eine persönliche Kennung erhält, die nicht an eine andere Person weitergegeben werden darf.

(6) Der Vertrag muss die Regelungen zur Protokollierung der Teilnehmerzugriffe im rechtmäßigen Rahmen enthalten.

(7) Der Betreiber der anzuschließenden Netzinfrastruktur muss darauf hingewiesen werden, dass der Provider vor einer Vertragsverlängerung bei der jeweils zuständigen KV die Rechtmäßigkeit der Zulassung des Betreibers zum *Sicheren Netz der KVen* bestätigen lassen muss.

(8) Der Provider muss im Rahmen des Vertrages den Betreiber der anzuschließenden Netzinfrastruktur über die Laufzeit seines Zertifikates als Netzkopplungsprovider informieren.

(9) Dem Betreiber der anzuschließenden Netzinfrastruktur steht ein außerordentliches Kündigungsrecht aus wichtigem Grund zu, beispielsweise bei nicht erfolgter Aufklärung hinsichtlich der technischen Voraussetzungen, welche notwendig für den Netzkopplungsanschluss sind.

(10) Dem Betreiber der anzuschließenden Netzinfrastruktur muss vier Monate vor Ablauf der Zertifikatsgültigkeit des Providers ein außerordentliches Kündigungsrecht entsprechend der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] zum Ende der Zertifikatsgültigkeit eingeräumt werden. Der Provider hat zudem die Pflicht und die entsprechende KV das Recht, den Teilnehmer vier Monate vor Ende der Gültigkeit des Zertifikats entsprechend zu informieren, falls sich der Provider nicht entsprechend der Richtlinie [KBV_SNK_RLEX_Netzkopplung] rezertifizieren lassen hat.

(11) Falls eine Rezertifizierung nicht angestrebt wird, so muss der Provider mindestens sechs Monate vor Ablauf der Zertifikatsgültigkeit eine Information an die Betreiber der angeschlossenen Netzinfrastruktur versenden. Bei einem Verstoß gegen diese Regelung übernimmt der Provider die Wechselkosten des Betreibers.

(12) Der Provider sichert dem Betreiber der anzuschließenden Netzinfrastruktur die Erreichbarkeit des *Sicheren Netzes der KVen* mindestens für den Zeitraum der Vertragslaufzeit zu.

(13) Der Vertrag muss eine für den Betreiber der anzuschließenden Netzinfrastruktur verständliche Übersicht der Kosten enthalten. Dazu gehört die Angabe aller Voraussetzungen und zusätzlich anfallender Kosten.

(14) Der Provider stellt dem Betreiber der anzuschließenden Netzinfrastruktur die Kontaktdaten für den Support zur Verfügung, inklusive Servicezeiten und -kosten für Serviceanfragen des Betreibers.

(15) Der Vertrag muss Regelungen über Zugriffe auf die Komponenten des Netzkopplungsrouters für Fälle von Störungen, Wartungen und Updates etc. enthalten, inkl. Angabe eines Ansprechpartners oder einer Supporthotline. Diese Regelungen müssen gewährleisten, dass der Betreiber der anzuschließenden Netzinfrastruktur den Wartungsarbeiten zustimmen muss und dass die Teilnehmer der angeschlossenen Netzinfrastruktur über Wartungsaktivitäten informiert werden.

(16) Der Vertrag muss eine Klausel über die Vertragsstrafe aufgrund nicht eingehaltener Wiederherstellungszeiten der Anbindung an das *Sichere Netz der KVen* enthalten.

(17) Der Vertrag muss einen Abschnitt enthalten, indem die Pflichten des Betreibers der anzuschließenden Netzinfrastruktur entsprechend Richtlinie Netzkopplung aufgeführt sind. Insbesondere müssen die Vorgaben zu PC-Arbeitsplatz, Netzinfrastruktur und organisatorischen Maßnahmen im Vertrag geregelt werden.

(18) Der Vertrag muss eine Regelung enthalten, die die physikalische Absicherung der Komponenten des Netzkopplungsrouters regelt, die in den Räumlichkeiten des Betreibers der anzuschließenden Netzinfrastruktur betrieben werden.

(19) Der Betreiber der anzuschließenden Netzinfrastruktur muss darauf hingewiesen werden, dass die Weitergabe des Netzkopplungsrouters bzw. einzelner Komponenten an Dritte verboten ist.

(20) Der Provider muss bei Beendigung seines Vertragsverhältnisses mit einem Betreiber der angeschlossenen Netzinfrastruktur sicherstellen, dass mit dem Tag des Vertragsendes kein Zugriff von Teilnehmern aus der angeschlossenen Netzinfrastruktur zum *Sicheren Netz der KVen* mehr möglich ist.

(21) Es muss eine Regelung enthalten sein über die Rückgabe des Netzkopplungs-Routers bei Vertragsende bzw. die vollständige Zurücksetzung des Gerätes, wenn dieses Eigentum des Betreibers der angeschlossenen Netzinfrastruktur ist.

(22) Der Betreiber der anzuschließenden Netzinfrastruktur erhält ein Kontrollrecht über die fortlaufende Einhaltung der Richtlinie [KBV_SNK_RLEX_Netzkopplung], welches die KBV für ihn ausüben kann.

(23) Der Betreiber der anzuschließenden Netzinfrastruktur ist im Vertrag darauf hinzuweisen, dass der KV/KBV das Recht eingeräumt wird, den Netzkopplungsanschluss insgesamt oder einzelne Teilnehmer aus der angeschlossenen Netzinfrastruktur im Falle eines Missbrauches zu sperren.

(24) Der Provider muss den Betreiber der anzuschließenden Netzinfrastruktur darauf hinweisen, dass die KBV / KV keinerlei Haftung sowohl bzgl. der Verfügbarkeit und der IT-Sicherheit des Zugangsnetzes des Providers, als auch bzgl. der Sicherheit der angeschlossenen Netzinfrastruktur übernimmt.

Zusätzliche Angaben bei der Einbeziehung von Erfüllungsgehilfen

(25) Der Provider muss dem Betreiber der anzuschließenden Netzinfrastruktur benennen, welche Erfüllungsgehilfen er für welchen Aufgabenbereich zur Erfüllung des Vertrages einsetzt.

Erläuterung

Alle in der Richtlinie [KBV_SNK_RLEX_Netzkopplung] aufgezählten Inhalte des Netzkopplungsvertrages müssen im Muster des Vertrages vorhanden sein.

Die detaillierten Erläuterungen sind in der Richtlinie [KBV_SNK_RLEX_Netzkopplung] zu finden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_Netzkopplung] in Abschnitt 6 (Anforderungen an den Netzkopplungsvertrag)

3.3 Diagramme der Betriebsprozesse

Grundlegend gelten die Regelungen des Leitfadens [KBV_SNK_LFEX_Zert_KV-SafeNet].

Diese sind entsprechend der Richtlinie [KBV_SNK_RLEX_Netzkopplung] zu adaptieren und die entsprechenden Betriebsprozesse zu beschrieben.

Anforderung

Beschreibung der folgenden Betriebsprozesse

(1) Prozess der Zulassung eines Betreibers einer anzuschließenden Netzinfrastruktur

(2) Prozess der Zulassung von Teilnehmern aus der angeschlossenen Netzinfrastruktur

(3) Prozess der Zustellung der Kennungen an Teilnehmer

(4) Prozess der Änderung von Kennungen durch Teilnehmer und/oder Provider

(5) Prozess der temporären Sperrung der Kennung eines Teilnehmers und Sperrung des Zugangs

(6) Prozess der Entsperrung der Kennung eines Teilnehmers und Entsperrung des Zugangs

(7) Prozess der endgültigen Sperrung und Deaktivierung eines Zugangs

(8) Prozess der Wartungsaktivitäten

(9) Monitoring (Überwachen) des laufenden Netzbetriebes

(10) Erkennen, Abwehr und Meldung von Angriffen mit der Angabe der dafür verwendeten Tools (Firewall, Intrusion Detection System, Monitoring Systeme etc.)

(11) Integration des techn. Berichtswesens inkl. Ausfälle und der Teilnahmestatistiken in den Diagrammen

Erläuterung

Die Betriebsprozesse sind unter Einbeziehung des technischen Berichtswesens (ggf. Benachrichtigung der KV und/oder KBV) ausführlich zu beschreiben.

Die Betriebsprozesse sind übersichtlich und verständlich in Diagrammform einzureichen. Dabei ist die Verwendung einer Legende umzusetzen.

Es wird empfohlen für die Darstellung BPMN (Business Process Modeling Notation) zu verwenden.

Die folgende Abbildung zeigt den grundlegenden Prozess der Zulassung eines Betreibers einer anzuschließenden Netzinfrastruktur und den Prozess der Benennung der berechtigten Teilnehmer aus der anzuschließenden Netzinfrastruktur. Die einzelnen Schritte werden in der Richtlinie [KBV_SNK_RLEX_Netzkopplung] erläutert, die Grafik dient der näheren Erläuterung.

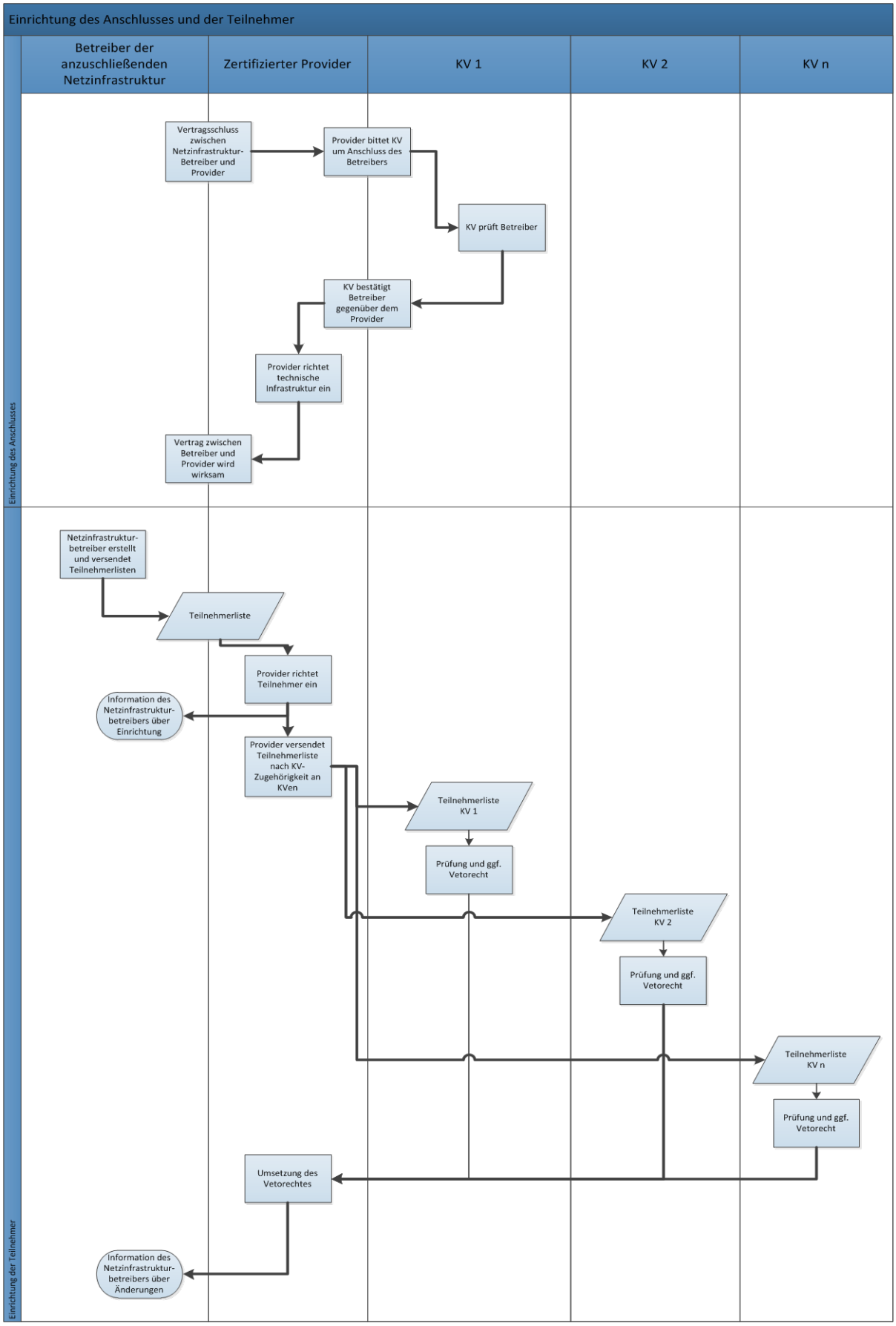

Abbildung 2: Prozess der Zulassung eines Betreibers und der Benennung der berechtigten Teilnehmer

Ausgewählte Anforderungen an die Dokumentation werden im Folgenden genauer beschrieben.

zu (7): Bei der endgültigen Sperrung des Zugangs ist das Löschen der Konfiguration des Netzkopplungsrouters (Werkszustand wiederherstellen) dringend erforderlich und muss durch den Anbieter erfolgen. Ein aktives Einbinden des Kunden ist nicht gestattet.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_Netzkopplung] in den Abschnitten 4 (Grundlegendes Vorgehen und Verantwortlichkeiten), 6 (Anforderungen an den Netzkopplungsvertrag), 8 (Organisatorische Anforderungen an den Provider), 9 (Berichtswesen), sowie die entsprechenden Abschnitte der Richtlinie [KBV_SNK_RLEX_KV-SafeNet].

3.4 Beschreibung der Anbindung

Anforderung

Vollständige Beschreibung des technischen Konzeptes der Anbindung an das Sichere Netz der KVen, die folgende Mindestanforderungen erfüllt:

(1) Grafische Darstellung der Anbindung an das *Sichere Netz der KVen* inkl. Abgrenzung der Verantwortlichkeitsbereiche und Beschreibung der Netztopologie

(2) Beschreibung des Vorgangs der Authentisierung und des Verbindungsaufbaus zum *Sicheren Netz der* KVen, einerseits aus Sicht des Teilnehmers und andererseits aus technischer Sicht.

(3) Erläuterung und Darstellung der eingesetzten Schutzmaßnahmen vor unbefugten Zugriffen

   a. aus dem oder den lokalen Netzen des Providers auf Komponenten des *Sicheren Netzes der KVen*

   b. der anzubindenden Netzinfrastruktur aus dem *Sicheren Netz der KVen* heraus

   c. auf die Konfigurationsschnittstelle der einzelnen Komponenten des Netzkopplungsrouters

(4) Erläuterung zur Sicherstellung der Unsichtbarkeit der Teilnehmercomputer in der angeschlossenen Netzinfrastruktur

(5) Erläuterung und Nennung der Konfiguration des bzw. der VPN-Tunnel

(6) Beschreibung der verwendeten Verschlüsselungsverfahren

(7) Beschreibung der Dienstneutralität[3] des Zugangsnetzes

(8) Bestätigung, dass der „Nutzdatentunnel“ nicht unterbrochen wird, sondern eine Ende-zu-Ende-Sicherheit des VPN-Tunnels zwischen Netzkopplungsrouter (beim Betreiber) und dem VPN-Konzentrator (in der jeweiligen KV) gegeben ist.

[3] Um Dienstneutralität eines Zugangsnetzes zu erlangen, muss die Verkabelung eines Objektes so ausgelegt werden, dass alle Übertragungsdienste eingesetzt werden können.

Erläuterung

Es muss eine Dokumentation aller angebotenen Anbindungsvarianten an das *Sichere Netz der KVen* eingereicht werden. Ausgewählte Anforderungen an die Dokumentation werden im Folgenden genauer beschrieben.

zu (1): Die angeforderte grafische Darstellung der Anbindungsvarianten kann bspw. in Form eines technischen Schaubildes eingereicht werden, welches zudem die Visualisierung oben genannten Punkte (2) bis (8) enthält.

zu (3a): Die Erläuterung und Darstellung der eingesetzten Schutzmaßnahmen vor unbefugten Zugriffen aus dem oder den lokalen Netzen des Providers auf Komponenten des *Sicheren Netzes der KVen* fokussiert u.a. auf die Trennung von Office- und Management-Netzen.

zu (5): Es soll dargelegt werden, welches Verfahren für den Aufbau des VPN-Tunnels verwendet wird (SSL/TLS oder IPSEC).

zu (6): Die geforderte Beschreibung der verwendeten Verschlüsselungsverfahren soll insbesondere unter Angabe der verwendeten Algorithmen zum Schlüsselaustausch und der Schlüssellängen der verwendeten symmetrischen Verfahren erfolgen.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.3 (Schutz der Anbindung) und 2.6 (Technische Anforderungen), sowie Richtlinie [KBV_SNK_RLEX_Netzkopplung] in den Abschnitten 7.1 (Basisanforderungen), 7.2.1 (Datendurchleitung und zu unterstützende Protokolle), 8.2 (Schutz der Anbindung)

3.5 Dokumentation des Netzkopplungsrouters

Anforderung

Dokumentation des Gesamtkonzeptes und aller Komponenten des Netzkopplungsrouters mit folgenden Mindestangaben:

(1) Gesamtkonzeption des Netzkopplungsrouters inkl. der ggf. benötigten Einzelkomponenten, unter besonderer Beachtung der Basis-Anforderungen:
   a. Identifizierbarkeit der Zugriffe von Teilnehmern am Netzkopplungsrouter
   b. Authentisierung der Teilnehmer vor dem Zugang zum *Sicheren Netz der KVen*
   c. Protokollierung der Teilnehmerzugänge
   d. Verschlüsselung innerhalb der Komponenten des Netzkopplungsrouters und extern
   e. Sicherstellung der Trennung der Authentisierungsdaten im Falle eines zentralen Authentisierungsdienstes

(2) Ggf. die Berücksichtigung der optionalen und spezifischen Anforderungen

(3) Technische Unterlagen oder Produktbeschreibungen

(4) Erläuterung der realisierten Sicherungsmaßnahmen

(5) Vollständige Liste der verwendeten Hardware und Software, Produkte und Dienste / Ports

(6) Erläuterung zu Schutzmaßnahmen der Konfigurationsschnittstelle(n) der einzelnen

Komponenten vor unbefugtem Zugriff

(7) Beschreibung der Gerätekonfiguration(en)

(8) Verwendete Routingtabelle(n)

(9) Beschreibung der verwendeten Verschlüsselungsverfahren

(10) Vorgehen bei notwendigen Firmware-Updates

Optionale Angaben (sofern zutreffend bzw. vorhanden)

(11) Benutzerhandbuch/Installationshandbuch für den Teilnehmer und/oder den Betreiber der anzuschließenden Netzinfrastruktur

(12) Beschreibung der individuellen Anpassung(en) - sofern ein OTS (of the shelf) Produkt verwendet und für den Einsatz als Komponente des Netzkopplungsrouters modifiziert wurde

Erläuterung

Es muss für jede Komponente des Netzkopplungsrouters eine Dokumentation eingereicht werden. Ausgewählte Anforderungen an die einzureichenden Unterlagen werden im Folgenden genauer beschrieben.

zu (2): Aussage, ob und wenn ja welche optionalen bzw. spezifischen Anforderungen mit der dargestellten Lösung umgesetzt werden können und eine detaillierte Beschreibung, wie das erfolgt.

zu (3): Die technischen Unterlagen können bspw. in Form von Datenblättern oder Produktbeschreibungen (Handbücher) eingereicht werden.

zu (4): Die Erläuterung zu den Sicherungsmaßnahmen umfasst bspw. das Deaktivieren nicht benötigter Dienste (dies betrifft insbesondere Dienste, wie telnet oder ftp) bzw. die Deaktivierung ungenutzter Ports des Routers.

zu (7): Die Beschreibung der Gerätekonfiguration (bspw. durch zusätzliche Konfigurationsdatei) soll mindestens Angaben zu folgenden Eigenschaften/Parametern enthalten:

a. Externes Interface
b. Internes Interface
c. VPN
d. Firewall
e. weitere sicherheitsrelevante Parameter

zu (9): Die Beschreibung der verwendeten Verschlüsselungsverfahren soll insbesondere unter Angabe der verwendeten Algorithmen zum Schlüsselaustausch und der Schlüssellängen der verwendeten symmetrischen Verfahren erfolgen.

Hinweis: Im Anschluss an die erfolgreiche Prüfung der eingereichten Dokumente, wird eine hardwareseitige Prüfung des jeweiligen Netzkopplungsrouters bzw. der einzelnen Komponenten durchgeführt (siehe Kapitel 4).

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_Netzkopplung] in den Abschnitten 7.1 (Basisanforderungen), 7.2 (Spezifische Anforderungen) und Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.3 (Schutz der Anbindung) und 2.6 (Technische Anforderungen)

4 Praktische Prüfung des Netzkopplungsrouters

Anforderung

Erfolgreiche Prüfung der verwendeten Hardwarekomponenten

Erläuterung

Entsprechen die Unterlagen den Anforderungen der Richtlinie, so hat der Antragsteller die Komponente, die als Netzkopplungsrouter eingesetzt werden sollen, ein Testgerät einzureichen.

Diese Tests umfassen u.a. eine Prüfung der Konfiguration auf Korrektheit (Verbindungsaufbau zum VPN-Konzentrator) sowie ein Test des Netzkopplungsrouters auf offene interne und externe Schnittstellen (Ports).

Da bei einer Erstzertifizierung zu diesem Zeitpunkt noch kein VPN-Konzentrator des Providers in einer KV stehen kann, ist es nur möglich die Schnittstellen des (Betriebs-) Systems des Netzkopplungsrouters zu prüfen (gehärtetes OS).

Sollte die praktische Prüfung nicht erfolgreich sein, so wird der Provider über die zu korrigierenden Mängel informiert. Der Provider hat dann die Möglichkeit diese Mängel innerhalb von vier Wochen zu beheben und einen Netzkopplungsrouter mit korrigierter Konfiguration einzureichen.

Die Prüfstelle behält sich vor, den Anschluss und die Wartung eines Netzkopplungsrouters praktisch vorführen zu lassen.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_Netzkopplung] in den Abschnitten 5.3 (Bereitstellung der Hardware).

5 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
Betreiber der anzuschließenden Netzinfrastruktur	Institution, die die im Rahmen der Netzkopplung anzuschließende Netzinfrastruktur verantwortet.
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.

Begriff	Erklärung
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.
Netzkopplungsprovider	Von der KBV nach der Richtlinie KV-SafeNet (Netzkopplung) zertifizierter Anbieter, der die Netzkopplung durchführt und damit Teilnehmern aus angeschlossenen Netzinfrastrukturen einen Zugang zum *Sicheren Netz der KVen* ermöglicht. Siehe auch KV-SafeNet-Provider.
Netzkopplungsrouter	Ein Netzkopplungsrouter dient dem Anschluss größerer Netzinfrastrukturen an das *Sichere Netz der KVen*. Er wird von einem Netzkopplungsprovider bereitgestellt. Ein Netzkopplungsrouter ist ein nicht manipulierbarer Router. 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. Teilnehmer aus der angeschlossenen Netzinfrastruktur müssen sich vor einem Zugriff auf *Das Sichere Netz der KVen* am Netzkopplungsrouter mit sicheren Verfahren authentifizieren. Die Zugriffe auf das *Sichere Netz der KVen* werden protokolliert. Die Verantwortung für den Netzkopplungsrouter trägt der 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 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.

6 Referenzierte Dokumente

Alle im Folgenden aufgelisteten Dokumente sind unter http://www.kbv.de/25362.html beziehbar.

Referenz	Dokument
[KBV_SNK_RLEX_Netzkopplung]	Richtlinie KV-SafeNet (Netzkopplung)
[KBV_SNK_FOEX_Netzkopplung]	Formular Ergänzende Erklärung zur Zertifizierung zum Netzkopplungsprovider
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_LFEX_Zert_KV-SafeNet]	Leitfaden Zertifizierung KV-SafeNet-Provider