KBV

KASSENÄRZTLICHE
BUNDESVEREINIGUNG

RICHTLINIE KV-SAFENET

[KBV_SNK_RLEX_KV-SAFENET]

KASSENÄRZTLICHE BUNDESVEREINIGUNG

DEZERNAT DIGITALISIERUNG UND IT

15. MAI 2020

VERSION: 3.3

INHALT

DOKUMENTENHISTORIE UND KENNZEICHNUNG

KENNZEICHNUNG: **ÖFFENTLICH**

STATUS: **IN KRAFT**

GÜLTIG AB: **12. JUNI 2020**

Version	Datum	Autor	Änderung	Begründung	Seite
3.3	15.05.2020	KBV	Aktualisierung der Richtlinie	Anwendung neues Corporate Design der KBV, Entfernung der monatlichen Berichtspflicht, Entfernung Anhänge sowie Notwendigkeit der Vertragsprüfung, Anpassungen aufgrund TI-Verfügbarkeit sowie BSI-Vorgaben	Alle

1 PRÄAMBEL

1.1 DAS SICHERE NETZ DER KVEN

Die Kassenärztliche Bundesvereinigung (KBV) und die Kassenärztlichen Vereinigungen (KVen) 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 (SNK).

Informationssicherheit im SNK 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 KVen und der KBV sind hierzu über den KV-Backbone, einem logisch vom Internet getrennten Netzwerk, miteinander verbunden. Die KBV ist der Betreiber des KV-Backbones.

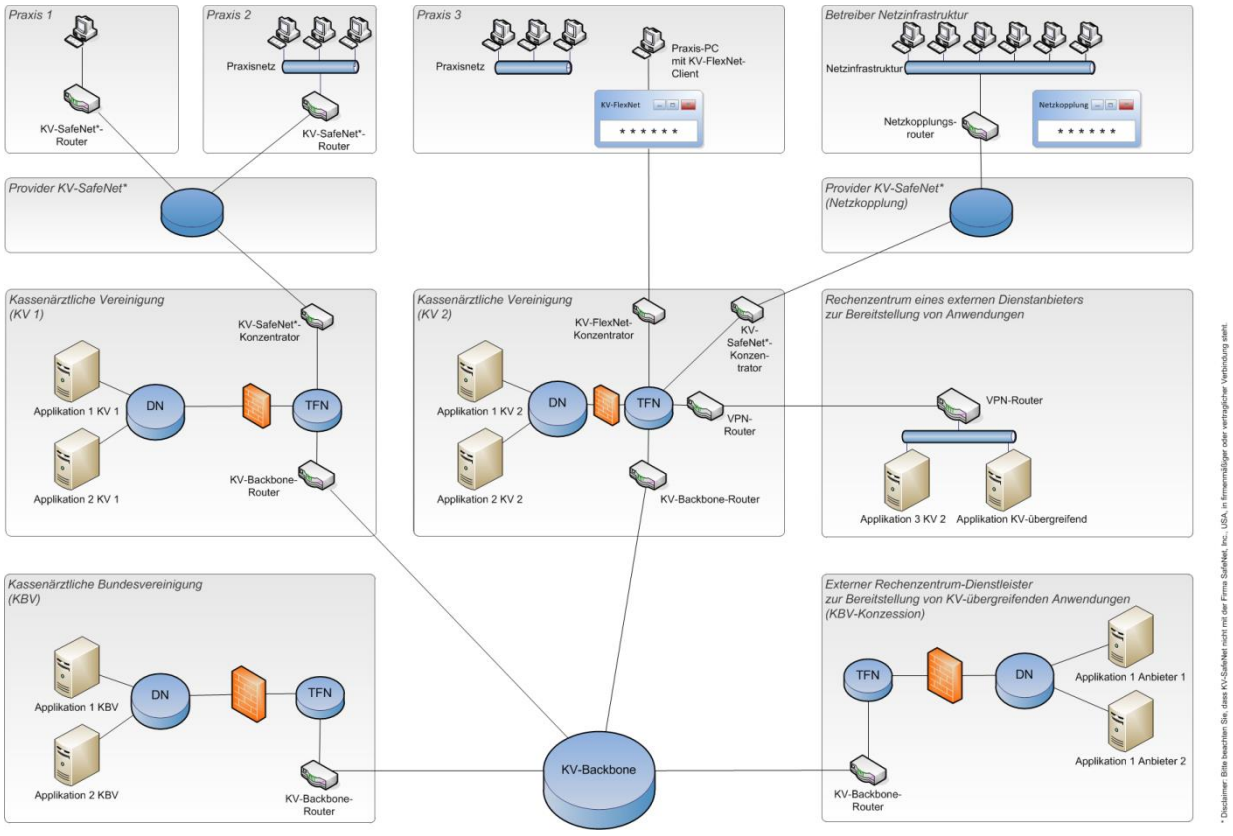

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am SNK sind die Mitglieder der KVen, also Vertragsärzte und -psychotherapeuten oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des SNK. Ihnen werden sichere Zugangswege zu den Diensten und Anwendungen bereitgestellt. Die Anbindung der Teilnehmer an das SNK erfolgt mittels einer VPN-Verbindung. Es gibt hierbei zwei Möglichkeiten der sicheren Anbindung: einerseits über das KV-SafeNet*, einem Hardware-VPN, und andererseits über das KV-FlexNet[1], einem Software-VPN. Die

---

* 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.

Bereitstellung eines Zugangs über die Variante KV-FlexNet liegt in der Hoheit der jeweiligen KV. Beide Zugangsvarianten ermöglichen eine sichere Anbindung an das SNK.

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

Im SNK 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.

Der Anschluss mittels KV-SafeNet erfolgt durch einen von der KBV zertifizierten Provider. Dieser stellt einem Teilnehmer alle technischen Voraussetzungen zur Anbindung an das SNK 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

Die Richtlinie KV-SafeNet beschreibt die Bedingungen für eine gesicherte Verbindung zwischen dem Teilnehmer und der KV auf der Basis einer hardwarebasierten VPN-Lösung, dem KV-SafeNet, und zudem die Bedingungen für die Zertifizierung eines Anbieters. Diese Richtlinie bildet zusammen mit dem Leitfaden [KBV_SNK_LFEX_Zert_KV-SafeNet] die Grundlage für die Zertifizierung von Anbietern.

1.3 KLASSIFIZIERUNG UND ADRESSATEN DES DOKUMENTS

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an alle am SNK beteiligten Akteure, insbesondere an Anbieter von KV-SafeNet- und Netzkopplungslösungen.

2 REGELUNGEN

Der Anbieter verpflichtet sich, Leistungen im Zusammenhang mit dem SNK nach Maßgaben und Best Practices eines standardisierten Informationssicherheitsmanagements zu erbringen.

Die folgenden Eckpunkte umreißen die Anforderungen an ein standardisiertes Informationssicherheitsmanagement:

- Informationssicherheitsrichtlinien
- Organisation der Informationssicherheit
- Personalsicherheit
- Verwaltung der Werte
- Zugangssteuerung
- Kryptographie
- Physische und umgebungsbezogene Sicherheit
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhalten von Systemen
- Lieferantenbeziehungen
- Handhabung von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte beim Business Continuity Management
- Compliance

Der Anbieter soll die Maßgaben aus ISO/IEC 27001 in der jeweils gültigen Fassung bzw. aus den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ableiten und durch unabhängige Dritte überprüfen lassen.

Der Anbieter soll den Anwendungsbereich, der die Leistungen zum SNK abdeckt, durch einen unabhängigen Dritten nach ISO/IEC 27001 zertifizieren lassen.

Die nachfolgenden Abschnitte regeln den Prozess der Zertifizierung sowie die konkreten Anforderungen, die ein Anbieter zu erfüllen hat, um eine Zertifizierung zu erlangen und aufrechtzuerhalten. Die weitere Detaillierung dieser Anforderungen sowie die einzureichenden Dokumente sind dem Leitfaden [KBV_SNK_LFEX_Zert_KV-SafeNet] zu entnehmen.

Grundsätzlich gelten alle Regelungen und damit alle Abschnitte der zum Zeitpunkt der Zertifizierung gültigen Fassung der Zertifizierungsrichtlinie der KBV [KBV_ITA_RLEX_Zert] für die Richtlinie KV-SafeNet und sind entsprechend umzusetzen. Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich zum KV-SafeNet werden in dieser Richtlinie definiert.

2.1 ZERTIFIKAT

Das Zertifikat bescheinigt dem Anbieter, dass seine Anbindung den Bestimmungen dieser Richtlinie genügt.

2.1.1 Zertifizierung

Der Antrag auf Zertifizierung erfolgt durch das Einreichen des Formulars [KBV_SNK_FOEX_AAZ_KV-SafeNet]. Mit dem Antrag auf eine Zertifizierung verpflichtet sich der Anbieter zur Einhaltung dieser Richtlinie. Die Zertifizierung erfolgt durch die KBV anhand des Dokuments [KBV_SNK_LFEX_Zert_KV-SafeNet]. Die Kosten der Zertifizierung trägt der Anbieter. Ausschließlich zertifizierte Anbieter erhalten eine

Anbindung an das SNK. Ausschließlich zertifizierte Anbieter können die Anbindung eines Teilnehmers beantragen und die Anbindung an das SNK dem Teilnehmer in Rechnung stellen.

2.1.2 Überprüfung

Die KBV behält sich das Recht vor, die Einhaltung aller Maßgaben dieser Richtlinie durch den Anbieter, in regelmäßigen Abständen oder anlassbezogen, durch einen Dritten zu überprüfen. Der Anbieter hat die Verstöße innerhalb eines von der KBV zu bestimmenden, angemessenen Zeitraumes zu beseitigen. Der Anbieter ist dazu verpflichtet an der Überprüfung mitzuwirken. Die Gebühren der Überprüfungen trägt der Anbieter.

Die folgenden Überprüfungsmaßnahmen können im Rahmen der Zertifikatslaufzeit nach den Maßgaben der KBV durchgeführt werden:

- Auditierung
  Es wird die Einhaltung der organisatorischen Maßgaben dieser Richtlinie geprüft. Diese Auditierung kann im Rahmen von Vor-Ort-Prüfungen oder der Prüfung ausgewählter Dokumente erfolgen.
- Penetrationstest
  Es wird ein durch die KBV ausgewählter KV-SafeNet-Router und ein VPN-Konzentrator einer sicherheitstechnischen Überprüfung unterzogen.

Die weitere Detaillierung der Maßnahmen zur Überprüfung sind dem Leitfaden [KBV_SNK_LFEX_Überprüfung_Provider] zu entnehmen.

2.1.3 Bereitstellung der Hardware

Der Anbieter stellt der KBV zu Zertifizierungszwecken je einen als KV-SafeNet-Router einzusetzenden Gerätetyp zur Verfügung.

Für die Laufzeit des Zertifikates verbleibt kein KV-SafeNet-Router bei der KBV.

2.1.4 Änderungen der Zugangskomponenten

Die Zertifizierung gilt ausschließlich für das zur Prüfung eingereichte Konzept und die vorgestellten Zugangskomponenten. Plant der Anbieter für eine zertifizierte Zugangsvariante ein anderes Zugangsgerät oder einen anderen VPN-Konzentrator einzusetzen, so muss jeweils die Konformität durch die Prüfstelle der KBV bestätigt werden. Diese Bestätigung hat keinen Einfluss auf die Laufzeit des Zertifikates.

2.1.5 Änderungen der Richtlinie

Bei Änderungen dieser Richtlinie stellt die KBV die jeweils aktuelle Fassung zeitnah zur Verfügung und informiert die Anbieter. Dem zertifizierten Anbieter steht es frei, sich schon vor Ablauf seines gültigen Zertifikates nach der neuen Richtlinie rezertifizieren zu lassen.

2.1.6 Laufzeit

Ein ausgestelltes Zertifikat ist auf einen Zeitraum von drei Jahren befristet. Sofern der Anbieter fristgerecht einen Antrag auf Rezertifizierung gestellt hat, gilt das Zertifikat bis zum Zeitpunkt der Einstellung des Rezertifizierungsverfahrens durch die KBV-Prüfstelle als nicht erloschen.

2.1.7 Rezertifizierung

Eine Rezertifizierung erfolgt entsprechend den Bedingungen der zum Zeitpunkt der Rezertifizierung aktuellen Richtlinie KV-SafeNet. Im Rahmen der Rezertifizierung müssen bis spätestens vier Monate vor Ablauf des derzeit gültigen Zertifikates alle Dokumente und Geräte bei der KBV-Prüfstelle eingereicht sein, ansonsten kann die Rezertifizierung verweigert werden.

Strebt der Anbieter keine Rezertifizierung an bzw. hat er die Rezertifizierung durch die Einreichung des vollständig ausgefüllten Formulars Antrag auf Zertifizierung [KBV_SNK_FOEX_AAZ_KV-SafeNet] bei der Prüfstelle der KBV nicht mindestens sechs Monate vor Ablauf des Zertifikates beantragt, so muss er dies den über sein Netz an das SNK angebundenen Teilnehmern mit einer Vorlaufzeit von einem halben Jahr mitteilen.

2.1.8 Gebühren

Für Zertifizierungen und Rezertifizierungen werden nach dem Leitfaden [KBV_SNK_LFEX_Zert_KV-SafeNet] Gebühren und Auslagen erhoben, wenn ein Anbieter eine Zertifizierung oder Rezertifizierung nach Abschnitt 2.1.1 beantragt hat. Es gilt § 9 der Zertifizierungsrichtlinie der KBV [KBV_ITA_RLEX_ZERT].

2.1.9 Entzug des Zertifikates

Eine Zertifizierung ist zurückzunehmen, wenn nachträglich bekannt wird, dass die Zertifizierung hätte versagt werden müssen. Eine Zertifizierung ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Versagung hätten führen müssen. Eine Zertifizierung kann auch widerrufen werden, wenn inhaltliche Beschränkungen nicht beachtet werden. In diesem Falle trägt der Anbieter die Kosten für den Wechsel des Teilnehmers zu einem anderen Anbieter, nicht jedoch die laufenden Kosten nach dem Wechsel.

2.1.10 Information der KVen

Die KBV kann die KVen über die Einstellung von Zertifizierungsverfahren und den Entzug eines Zertifikates informieren, ohne dass die Entscheidung bestandskräftig sein muss. Die KBV informiert die KVen durch Vorinformationen über auslaufende Zertifikate, geplante Einstellungen von Zertifizierungsverfahren und den Entzug eines Zertifikates.

2.1.11 Haftungsausschluss

Die KBV und die KVen übernehmen gegenüber dem Anbieter keine Haftung aus Anlass der Vorgaben technischer und/oder wirtschaftlicher sowie damit im Zusammenhang stehender Art und/oder aus der Umsetzung dieser Vorgaben.

Für Kapazitätsprobleme durch die Nutzung des KV-Backbones für die Anbindung von Teilnehmern übernimmt die KBV keine Haftung.

2.2 ANBINDUNG

2.2.1 Anzahl Einwahlknoten

Der Anbieter installiert in zwei unterschiedlichen KVen VPN-Konzentratoren zur Realisierung von insgesamt zwei anbieterspezifischen Einwahlpunkten. Pro Einwahlpunkt ist mindestens ein Konzentratorpaar vorzusehen, welches im Hot-Standby- oder Active-Active-Modus betrieben wird. Die Standorte der VPN-

Konzentratoren können dem Leitfaden Zertifizierung KV-SafeNet-Provider [KBV_SNK_LFEX_Zert_KV-SafeNet] entnommen werden.

2.2.2 Nutzung des KV-Backbones

Der KV-Backbone steht für die Anbindung der Teilnehmer einer KV über die Einwahlknoten in einer KV zur Verfügung.

2.2.3 Einschränkung der Nutzung

Anbieterseitiger Management-Traffic darf nicht über den KV-Backbone geleitet werden.

Der Anbieter darf den KV-Backbone nicht zur Vernetzung von fremden bzw. nicht zum SNK gehörigen Standorten oder Diensten missbrauchen.

2.2.4 Vorbehalt

Die KBV behält sich das Recht vor, bei übermäßiger Belastung des KV-Backbones durch Anbindung von Teilnehmern, dem Anbieter die Errichtung zusätzlicher Einwahlknotenpunkte zur Entlastung des KV-Backbones vorzuschreiben.

2.2.5 Missbrauch der Anbindung durch den Anbieter

Die KBV behält sich das Recht vor, bei Missbrauch der Anbindung des Anbieters diese jederzeit zu unterbrechen, um Schaden an Daten, Anwendungen oder angeschlossenen Systemen zu vermeiden.

2.2.6 Installation und Betrieb

Anfallende Arbeiten und Kosten für die Installation der VPN-Konzentratoren übernimmt der Anbieter.

Die geeigneten Räumlichkeiten stellt die KV bereit. Die KV gewährt dem Anbieter, entsprechend den jeweils gültigen Sicherheitsvorschriften, für Servicearbeiten an seinem VPN-Konzentrator Zugang zu den entsprechenden Räumen. Der Anbieter schließt mit der jeweiligen KV einen entsprechenden Vertrag ab. Die Erhebung von Nutzungsgebühren liegt im Ermessen der jeweiligen KV.

2.2.7 Support und Wartung

Für Meldungen von technischen Störungen stellen die KVen und der Anbieter einander einen direkten Zugang zum jeweiligen 2nd-Level-Support zur Verfügung. Die Verfügbarkeitszeiten sind in den jeweiligen Verträgen zwischen Anbieter und KV festzulegen. Der Anbieter benennt einen verantwortlichen Ansprechpartner für organisatorische und verwaltungstechnische Fragen. Die KVen benennen einen technischen Ansprechpartner für den Anbieter sowie einen Ansprechpartner für organisatorische und verwaltungstechnische Fragen des Anbieters.

2.2.8 Teststellungen der angebotenen Anbindungsvarianten

Der zertifizierte Zugangsprovider kann eine Teststellung der Anbindung der angebotenen KV-SafeNet-Router an den VPN-Konzentrator pro Anbindungsvariante zu Analyse- und Supportzwecken vorhalten.

2.2.9 Ausschluss des Supports durch die KV/KBV

Die KV/KBV übernimmt keine Supportanfragen seitens der Teilnehmer, die im Zusammenhang mit der Anbindung an das SNK durch den Anbieter entstehen.

2.3 SCHUTZ DER ANBINDUNG

Zugriffe auf das SNK müssen eindeutig identifizierbar sein. Der Anbieter verpflichtet sich, eventuell auftretende Schwachstellen seiner Lösung unverzüglich der KBV zu melden und unverzüglich zu beheben und zu dokumentieren.

Die folgenden Maßnahmen sind bei aktiver KV-SafeNet-Verbindung umzusetzen:

- Regelmäßiger Einsatz von Werkzeugen, die Integritätsverletzungen an Programmen und Dateien feststellen können
- Einsatz aller vom Hersteller empfohlenen Sicherheitsmaßnahmen für das im Einsatz befindliche Betriebssystem
- Benutzung starker Passwörter
- Benutzung aller relevanten und rechtmäßigen Protokollmechanismen, um Störfälle und Angriffsversuche analysieren zu können
- Regelung und Dokumentation der Benutzerrechte
- Einsatz von geeigneter Sicherheitssoftware

Bei Angriffsversuchen oder sonstigen Sicherheitsvorfällen, die durch den Teilnehmer, die KBV oder eine KV festgestellt und gemeldet werden, ist der Anbieter im Rahmen seiner Möglichkeiten verpflichtet, durch geeignete Maßnahmen den Angreifer ausfindig zu machen und angemessene Gegenmaßnahmen einzuleiten.

Bei durch den Anbieter festgestellten Angriffsversuchen oder sonstigen Sicherheitsvorfällen ist der Anbieter im Rahmen seiner Möglichkeiten verpflichtet, durch geeignete Maßnahmen den Angreifer ausfindig zu machen und unverzüglich angemessene Gegenmaßnahmen einzuleiten. Angriffsversuche oder sonstige Sicherheitsvorfälle und die eingeleiteten Maßnahmen sind den Betroffenen und der KBV unverzüglich zu melden.

2.4 BERICHTSWESEN

Auf Anfrage der KBV muss der Anbieter der KBV Berichte zur Verfügung stellen. Aus diesen Berichten sollen sich Informationen über die geforderte Verfügbarkeit, die Anzahl und den Umfang von sicherheitsrelevanten Störungen, Teilnehmerstatistiken sowie Anschlussdetails ableiten lassen. Dabei ist die von der KBV zur Verfügung gestellte Berichtsvorlage zu nutzen.

Der Anbieter hat der für die Teilnehmer zuständigen KV folgende Informationen zur Verfügung zu stellen:

- eine Kopie des wirksamen Vertrages (innerhalb von fünf Werktagen nach Vertragswirksamkeit)
- das Datum des Anschlusses
- ggf. das Datum der Kündigung
- ggf. Vertragsänderungen

2.5 ANFORDERUNGEN AN DEN TEILNEHMERVERTRAG

Diese Richtlinie ist Vertragsgrundlage zwischen Anbieter und Teilnehmer. Der Anbieter verpflichtet sich, ausschließlich von den KVen zugelassenen Teilnehmern Zugriff auf das SNK zu gewähren.

Der Teilnehmervertrag muss Folgendes enthalten:

2.5.1 Vertragspartner

Vertragspartner des Anbieters bei der Leistungserbringung ist ausschließlich der Teilnehmer.

2.5.2 Vertragsvoraussetzung und Bereitstellungszeitraum des Zugangs

Vor Bereitstellung des Zugangs bestätigt die jeweils zuständige KV gegenüber dem Anbieter, dass der Teilnehmer an das SNK angeschlossen werden kann. Die Zulassung eines Teilnehmers kann auch durch die KBV erfolgen.

Der Anbieter informiert den Teilnehmer über das Zertifikat und die entsprechende Zertifikatslaufzeit. Der Anbieter garantiert dem Teilnehmer die Bereitstellung eines Zugangs zum SNK mindestens für die Dauer der Vertragslaufzeit.

2.5.3 Vertragsverlängerung

Vor einer Vertragsverlängerung muss sich der Anbieter bei der jeweils zuständigen KV die Rechtmäßigkeit der Zulassung des Teilnehmers zum SNK bestätigen lassen.

2.5.4 Außerordentliche Kündigung

Der Vertrag zwischen Teilnehmer und Anbieter muss aus wichtigem Grund kündbar sein.

Hat sich der Anbieter nicht entsprechend Abschnitt 2.1.7 dieser Richtlinie rezertifizieren lassen, kann der Teilnehmer den Vertrag zum Ende der Laufzeit des derzeitig gültigen Zertifikates kündigen. Der Anbieter hat zudem die Pflicht und die entsprechende KV das Recht, den Teilnehmer drei Monate vor Ende der Gültigkeit des Zertifikates entsprechend zu informieren.

2.5.5 Beendigung des Vertragsverhältnisses

Der Anbieter muss bei Beendigung seines Vertragsverhältnisses mit einem Teilnehmer sicherstellen, dass mit dem Tag des Vertragsendes kein Zugriff des Teilnehmers zum SNK mehr möglich ist. Auch muss sichergestellt werden, dass bei Teilnehmern oder zurückgegebenen Geräten keine Konfigurationsmerkmale mit Bezug auf das SNK verbleiben.

2.5.6 Transparenz des Angebotes

Der Anbieter muss sämtliche Kosten des Teilnehmervertrages im Angebot vollständig und nachvollziehbar aufführen. Dieses gilt auch für sämtliche technischen Voraussetzungen auf Seiten des Teilnehmers für eine Anbindung an das SNK.

2.5.7 Teilnehmersupport des Anbieters

Der Anbieter muss über einen Teilnehmersupport für die KV-SafeNet-Anbindung verfügen.

Der Anbieter stellt dem Teilnehmer telefonischen Zugang zu seinem Support zur Verfügung, dessen Kosten marktüblich sind.

Die telefonische Support-Hotline muss den direkten Kontakt mit dem internen 1st-Level-Support des Anbieters gewährleisten.

2.5.8 Servicezeiten

Der Teilnehmersupport steht dem Teilnehmer von Montag bis Freitag mindestens in der Zeit von 8:00 bis 18:00 Uhr zur Verfügung.

Die Reaktionszeit bei Anfragen der Teilnehmer beträgt:

- Innerhalb der Servicezeiten von Montag bis Freitag: zwei Stunden
- Außerhalb der Servicezeiten, an Wochenenden und Feiertagen: Nächster Arbeitstag 8:00 Uhr + zwei Stunden

Die Wiederherstellungszeit bei durch den Anbieter verursachten technischen Problemen beträgt:

- Innerhalb der Servicezeiten von Montag bis Freitag: 24 Stunden ab Eingang der Störungsmeldung
- Außerhalb der Servicezeiten, an Wochenenden und Feiertagen: Nächster Arbeitstag 8:00 Uhr + 24 Stunden

2.5.9 Vertragsstrafe

Der Anbieter verpflichtet sich gegenüber dem Teilnehmer, für die Fälle der Überschreitung der Wiederherstellungszeit durch den Anbieter, zur Zahlung einer Vertragsstrafe. Die Vertragsstrafe beträgt für jeden weiteren angefangenen Kalendertag mindestens 100,00 €. Eine Begrenzung auf 1.000,00 € pro Jahr ist dem Anbieter freigestellt.

2.5.10 Vorbehalt der KV/KBV

Die KV/KBV behält sich das Recht vor, bei Missbrauch der Anbindung des Teilnehmers, diese zu unterbrechen oder durch den Anbieter unterbrechen zu lassen, um Schaden an Daten, Anwendungen oder angeschlossenen Systemen zu vermeiden.

2.5.11 Nutzung von Mehrwertdiensten durch den Teilnehmer

Ein Angebot zur Nutzung von Mehrwertdiensten muss immer als frei wählbare Option im Vertrag aufgeführt werden. Es muss einen Hinweis auf den Datenschutz und eine Beschreibung der notwendigen Sicherheitsmaßnahmen im Teilnehmernetz und den angeschlossenen Rechnern für den Fall beinhalten, dass der Teilnehmer parallel zum KV-SafeNet auch einen Zugang zum Internet oder anderen Diensten des Anbieters nutzen will.

Bei dem Angebot zur Nutzung von Mehrwertdiensten ist gesondert darauf hinzuweisen, wie der Zugang vom Teilnehmernetz zum Mehrwertdienst erfolgt:

- geschützt über den KV-SafeNet-Router
- geschützt über den KV-SafeNet-Router und ein gesondertes Netz des Anbieters

2.6 TECHNISCHE ANFORDERUNGEN

Die in den nachfolgenden Abschnitten beschriebenen technischen Anforderungen sind durch den Anbieter sicherzustellen.

2.6.1 KV-SafeNet-Router

Der KV-SafeNet-Router muss zwischen Internetanschluss und Praxisnetzwerk installiert werden.

Der Anbieter soll nach Common Criteria (Evaluation Assurance Level 4+) zertifizierte Geräte einsetzen.

2.6.2 VPN-Konzentratoren

Der Anbieter installiert in zwei unterschiedlichen KVen VPN-Konzentratoren (redundante Aufstellung) zur Realisierung von insgesamt zwei anbieterspezifischen Einwahlpunkten. Pro Einwahlpunkt ist mindestens ein Konzentratorpaar vorzusehen, welches im Hot-Standby- oder Active-Active-Modus betrieben wird. Zusatzaufwände bezüglich der Dienste „Routing“ und „DNS“ für KVen und Teilnehmer müssen dabei vermieden werden. Aufstellort des VPN-Konzentrators ist jeweils das gesicherte Rechenzentrum der KV.

Bei steigender Anzahl über sein Netz angebundener Teilnehmer passt der Anbieter die Kapazität seiner VPN-Konzentratoren entsprechend an.

Der Anbieter soll nach Common Criteria (Evaluation Assurance Level 4+) zertifizierte Geräte einsetzen.

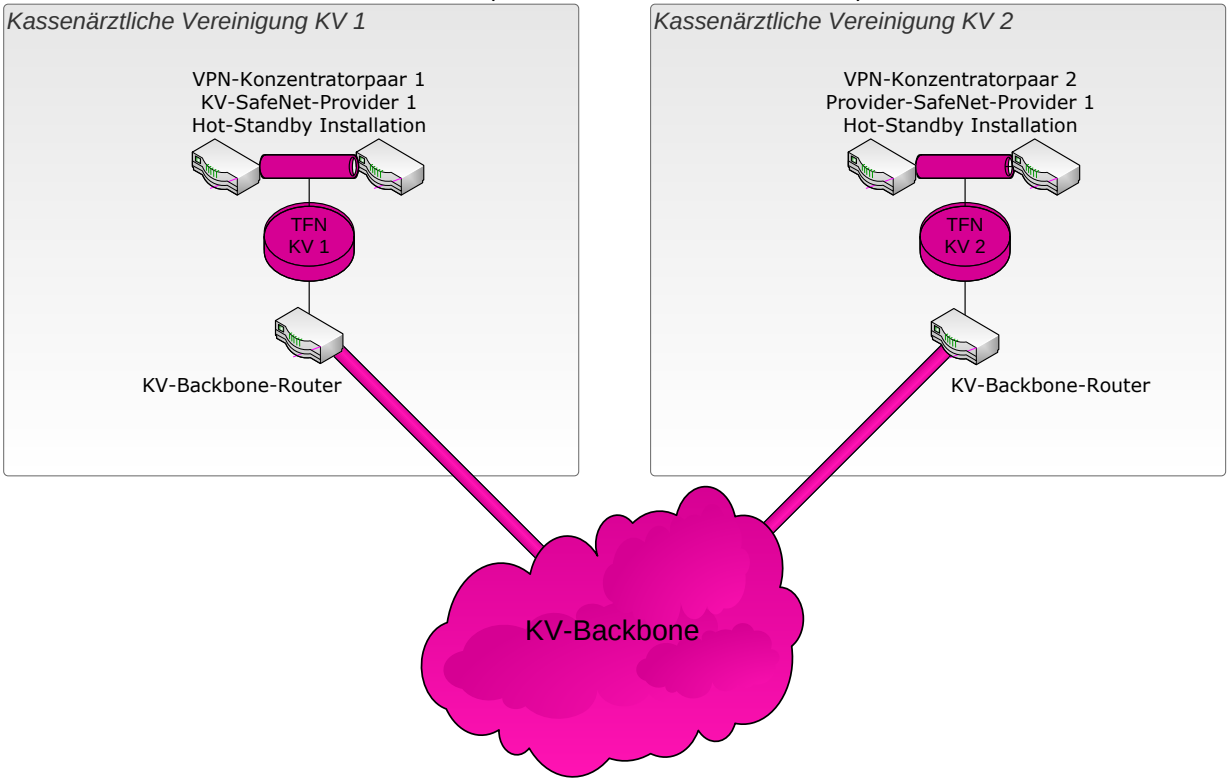

Abbildung 2: Hot-Standby Betrieb der VPN-Konzentratoren

2.6.3 VPN Verbindungsart

Der zwischen KV-SafeNet-Router und VPN-Konzentrator aufgebaute VPN-Tunnel ist als sogenanntes Site-to-Site-VPN (Site 1 = KV-SafeNet-Router, Site 2 = Konzentrator) zu realisieren.

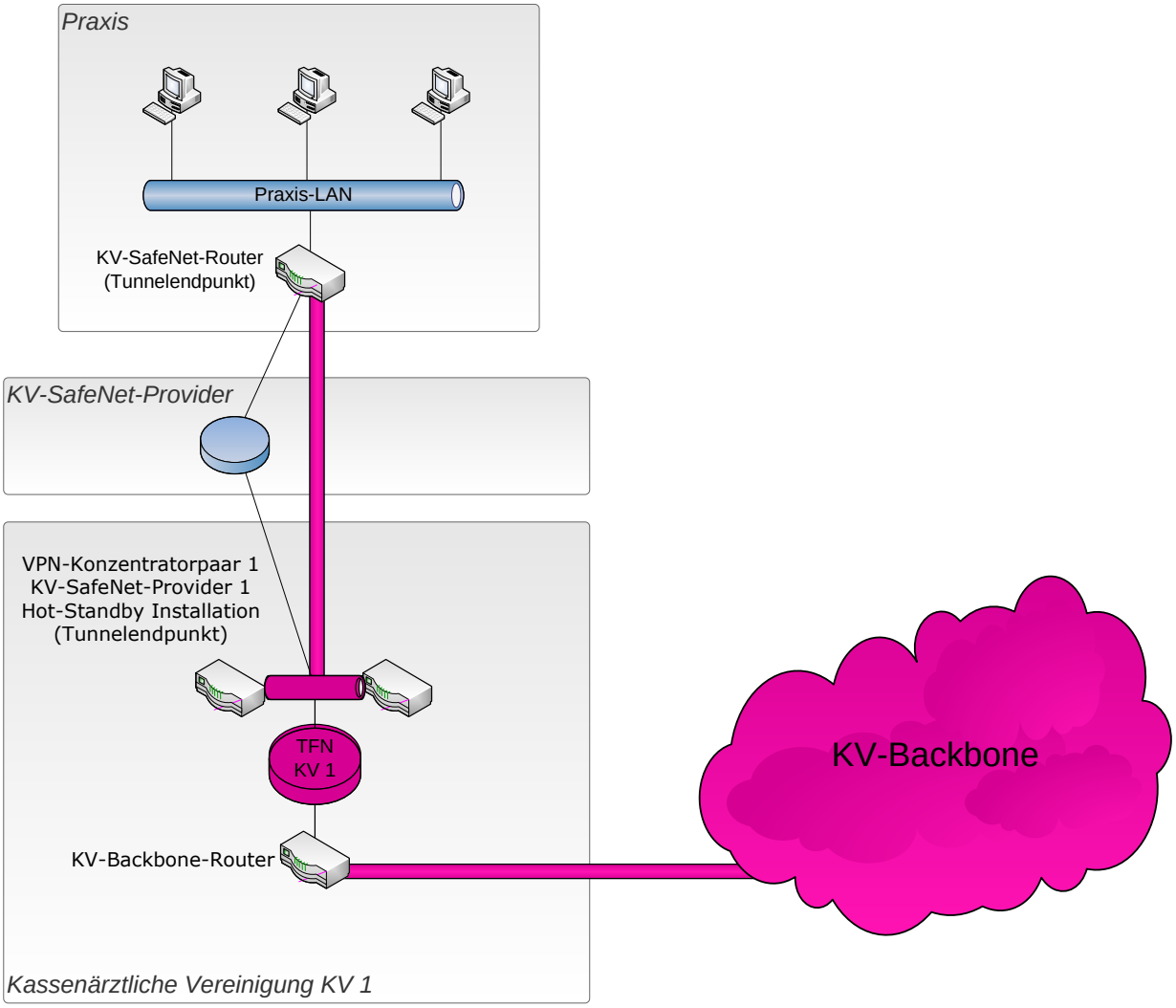

Abbildung 3: Site-to-Site Tunnelendpunkte

2.6.4 Unbefugter Zugriff

Unbefugte Administrationszugriffe auf die KV-SafeNet-Komponenten über das Netz des Anbieters wie auch über das Netz des Teilnehmers müssen ausgeschlossen sein. Zugriffe erfolgen ausschließlich über ein alleinstehendes Administrationsnetz des Anbieters.

Die Konfiguration von KV-SafeNet-Router und VPN-Konzentrator muss durch geeignete Sicherheitsmaßnahmen sicherstellen, dass jegliche unbefugten Zugriffe auf das SNK, den KV-SafeNet-Router, den VPN-Konzentrator, das Teilnehmernetzwerk und den darin befindlichen Rechnern jederzeit ausgeschlossen sind. Insbesondere sind für administrative Zugänge, aber auch für den Aufbau des VPN zur Anbindung an das SNK für den KV-SafeNet-Router und den VPN-Konzentrator Zugriffslisten (sogenannte ACL, Access Control Lists) umzusetzen.

2.6.5 Adressierung

Die zur Adressierung der Teilnehmer am SNK benötigten IP-Adressräume werden zentral von der KBV vergeben. Das Vorgehen zur Beantragung der IP-Adressräume sowie die seitens der KBV verantwortlichen Ansprechpartner sind Gegenstand des Konzeptes [KBV_SNK_KNEX_IP-Adressvergabe]. Der Anbieter ist verpflichtet, das jeweils gültige Konzept zur IP-Adressvergabe [KBV_SNK_KNEX_IP-Adressvergabe] einzuhalten.

2.6.6 VPN-Datenübertragung

Die Mehrwertdienstkommunikation (z. B. Übermittlung von Daten aus dem Internet) darf nicht im KV-SafeNet-VPN (Nutzdatentunnel) erfolgen, sondern hiervon separiert und außerhalb des Nutzdatentunnels.

2.6.7 Routing

Der Anbieter ist verpflichtet, das jeweils gültige Konzept zu den Routingvorgaben für das SNK [KBV_SNK_KNEX_Routing] einzuhalten.

2.6.8 DNS

Zur Adressierung der im SNK angebotenen Dienste werden IP-Adressen verwendet. Da die Handhabung dieser mit steigender Anzahl der Dienste unkomfortabel wird, soll mit Namensauflösung gearbeitet werden. Dazu wird ein Dienst DNS im SNK betrieben. Der Anbieter hat dafür zu sorgen, dass die Teilnehmer am SNK den installierten Dienst erreichen können. Genaue Angaben zur Realisierung des Dienstes DNS sind Gegenstand des Konzeptes [KBV_SNK_KNEX_DNS].

2.6.9 Sichtbarkeit

Die Teilnehmercomputer und deren IP-Adressen dürfen durch die Anbindung an das SNK mittels KV-SafeNet-Router nicht über das Internet oder sonstige Netze sichtbar sein.

2.6.10 Verschlüsselung

Die von den Teilnehmern übermittelten und/oder empfangenen Daten müssen vor einem Zugriff Dritter durch einen verschlüsselten VPN-Tunnel geschützt sein.

Der Tunnelaufbau über das Internet darf erst nach einer gegenseitigen Authentifikation der Tunnelendpunkte erfolgen.

Die eingesetzten Verfahren zur Authentifizierung, Verschlüsselung und Signierung müssen dem Stand der Technik entsprechen und können den vom BSI veröffentlichten Vorgaben entnommen werden.

Es ist auf den Einsatz von Pre-Shared-Keys im Rahmen der Kryptografie zu verzichten. Es sind Zertifikate (z. B. X.509) einzusetzen.

2.6.11 Sicherheit der Zugangsdaten

Die im KV-SafeNet-Router vorgehaltenen Daten zur Authentifikation sind geheim zu halten. Der Anbieter beschränkt den Zugriff auf diese Daten ausschließlich auf autorisiertes Personal seines Unternehmens oder entsprechende Erfüllungsgehilfen.

2.6.12 Deaktivierung ungenutzter Router-Ports

Der KV-SafeNet-Router muss entsprechend der Maßgaben des BSI so konfiguriert werden, dass ungenutzte Ports des Routers und damit nicht benutzte Dienste des Routers deaktiviert sind.

2.6.13 Überwachungsmaßnahmen - Anbieter

Zum Schutz der internetseitigen und SNK-seitigen (von „außen“) Anbindung der Konzentratoren muss ein Intrusion Detection System / Intrusion Prevention System (IDS / IPS) installiert sein. Die Protokolldateien müssen im Einklang der datenschutzrechtlichen Vorgaben vorgehalten werden.

2.6.14 Betriebszeit und Verfügbarkeit

Die Betriebszeit der Konzentratoren beträgt 7 x 24 Stunden pro Woche.

Die Verfügbarkeit der KV-SafeNet-Einwahl muss 99,5 % per annum betragen. Ausgenommen hiervon ist die Betriebsumgebung und die Anbindung der VPN-Konzentratoren, solange der Anbieter hierfür nicht in der Betriebsverantwortung ist. Die hierfür notwendigen Zugriffsmöglichkeiten für den Anbieter sind zwischen dem Anbieter und der jeweiligen KV vertraglich zu regeln.

2.6.15 Wartungsarbeiten

Zu Wartungs- und Störungsbehebungszwecken ist ein Zugriff auf den KV-SafeNet-Router durch den Anbieter unter Einhaltung der Datenschutzbestimmungen zulässig.

Für die Fernwartung der VPN-Konzentratoren sollen eigene MPLS-Anbindungen oder gesicherte Internetanbindungen genutzt werden. Management-Ports an KV-SafeNet-Routern und VPN-Konzentratoren dürfen jedoch nicht aus dem SNK erreichbar sein.

2.6.16 Besondere Sicherheitsmaßnahmen bei Nutzung von Mehrwertdiensten

Bei Mehrwertdiensten müssen sowohl dem Anbieter als auch dem Teilnehmer neben den Funktionen auch die Risiken bewusst sein. Hier liegt besonders bei den Anbietern eine große Verantwortung. Für die parallele Nutzung von Mehrwertdiensten, neben dem Zugang zum SNK, gelten die vom BSI aufgestellten Anforderungen.

Eine wichtige und daher empfehlenswerte Standardmaßnahme zum Schutz des Teilnehmers und des SNK beim Anschluss des Teilnehmers an das Internet als Mehrwertdienst ist die Einrichtung einer DMZ seitens des Anbieters.

Es wird empfohlen, folgende Maßnahmen umzusetzen und den Teilnehmer hierüber zu informieren:

- Regelmäßiger Einsatz von Programmen, die Integritätsverletzungen an Programmen und Dateien feststellen können

- Einsatz von Programmen zur Erkennung von Angriffen auf ein IT-System, z. B. ein Intrusion Detection System (IDS) oder ein anderes zur Frühwarnung taugliches Netzüberwachungssystem
- Einsatz aller vom Hersteller empfohlenen Sicherheitsmaßnahmen, für das im Einsatz befindliche Betriebssystem
- Benutzung starker Passwörter
- Benutzung aller relevanten und rechtmäßigen Protokollmechanismen um Störfälle und Angriffsversuche analysieren zu können
- Regelung und Dokumentation der Benutzerrechte
- Einsatz von geeigneter Sicherheitssoftware

Die aufgezeigten Maßnahmen können sowohl im Netz des Anbieters zwischen dem Teilnehmer und dem Internet als auch beim Teilnehmer installiert werden.