Kassenärztliche Bundesvereinigung

Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Richtlinie KV-SafeNet

[KBV_SNK_RLEX_KV-SafeNet]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	3.2
Datum:	31.07.2015
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
3.2	24.07.2015	KBV	QS und Freigabe		
3.2 beta	18.05.2015	KBV	Einarbeitung Kommentare aus dem Kommentierungsverfahren		
3.2 alpha	10.02.2015	KBV	Erweiterung der Richtlinie – Aufnahme weiterer Anforderungen	Anforderungen gemäß Abstimmung im KV-System	
3.1	31.10.2011	KBV	Einarbeitung Kommentare aus dem Kommentierungsverfahren, QS und Freigabe		
3.1 beta	14.02.2011	KBV	Einarbeitung von Maßnahmen zur kontinuierlichen Verbesserung des Datenschutzes Vereinheitlichung der Begriffe und des Dokumentenlayouts	Maßnahmen gemäß Abstimmung mit Leiter des Arbeitskreises Technik der Datenschutzbeauftragten von Bund und Ländern Maßgaben der Dokumentenlenkung	
3.0	06.03.2009	KBV	Version zur Veröffentlichung	Einarbeitung Kommentare aus Providerkommentierungsrunde	
3.0 beta	16.02.2009	KBV	Version Kommentierungsrunde der Provider	Einarbeitung Kommentare aus interner Kommentierungsrunde	
3.0 alpha	05.02.2009	KBV	Initiale Version zur internen Kommentierung		

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.

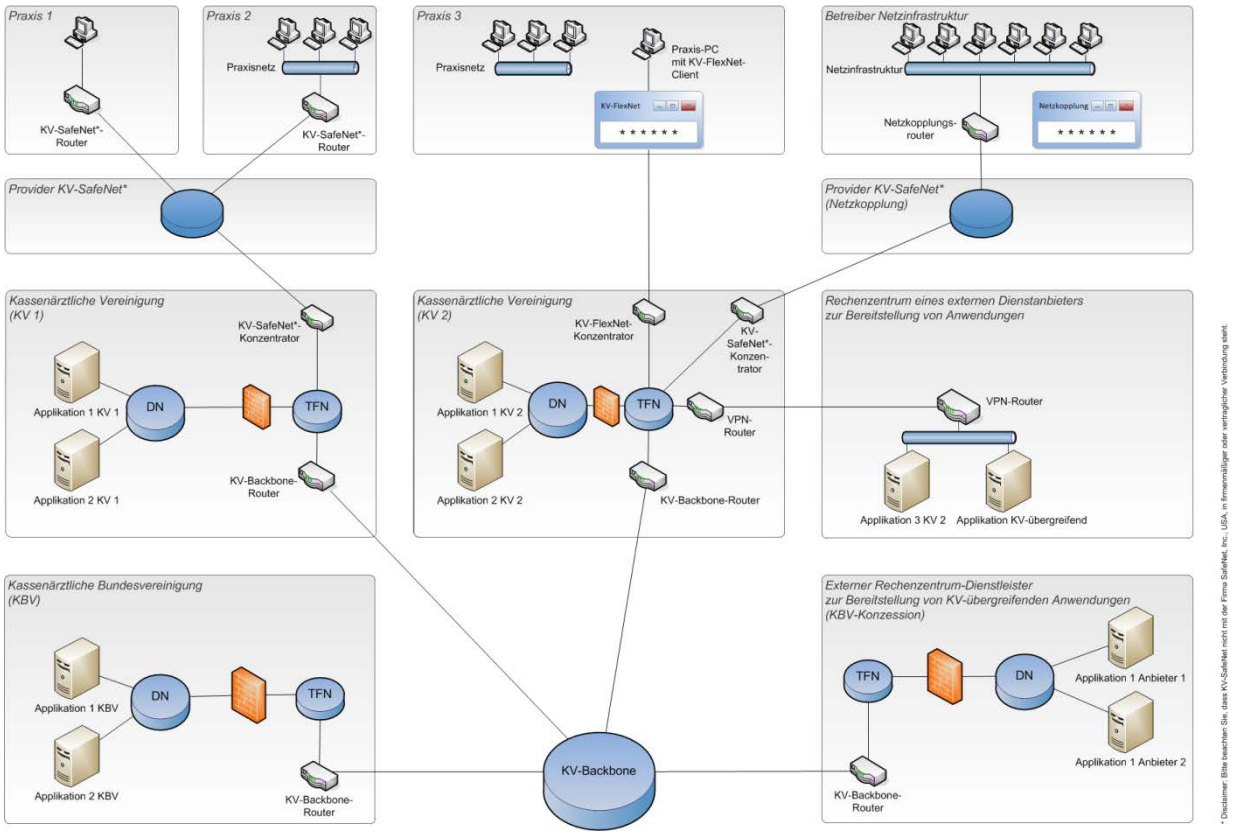

Abbildung 1: Beispielhafte Netztopologie

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

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 sicheren Netz der KVen beteiligten Akteure, insbesondere an Anbieter von KV-SafeNet- und Netzkopplungslösungen.

* 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

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

Die folgenden Eckpunkte umreißen die Anforderungen an ein standardisiertes Informationssicherheitsmanagement:

- Sicherheitsleitlinie und Organisation der Sicherheit
- Datenschutz, Vertraulichkeit und Zugangskontrolle
- Personalsicherheit
- Gebäude- und Arbeitsplatzsicherheit
- Management der Betriebs- und Kommunikationsprozesse
- Beschaffung, Entwicklung und Wartung
- Management von Informationssicherheitsereignissen (Incident Management)
- Business Continuity Management (BCM)
- Compliance

Es wird dringend empfohlen, diese Maßgaben aus der ISO 27001 bzw. aus dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) abzuleiten und durch unabhängige Dritte überprüfen zu lassen. Die Zertifizierung des Informationssicherheitsmanagementsystems (ISMS) eines Anbieters gemäß ISO 27001 mit einem Anwendungsbereich, der die Leistungen zum sicheren Netz der KVen abdeckt, wird empfohlen. Die Vorlage eines entsprechenden Zertifikats kann zudem den KBV-Zertifizierungsprozess eines Anbieters beschleunigen.

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.

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 der Ergänzenden Erklärung [KBV_SNK_FOEX_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. Die Zertifizierung des Anbieters wird von allen am sicheren Netz der KVen beteiligten KVen anerkannt. Ausschließlich zertifizierte Anbieter erhalten eine Anbindung an das sichere Netz der KVen. Ausschließlich zertifizierte Anbieter können die Anbindung eines Teilnehmers beantragen und die Anbindung an das sichere Netz der KVen 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 durch eine zur Verschwiegenheit verpflichtete und von der KBV zu bestimmende Person überprüfen zu lassen. Diese Person ist von der KBV und dem Anbieter dazu berechtigt und verpflichtet, der KBV Mitteilung über Verstöße gegen die Anforderungen dieser Richtlinie zu machen. Der Anbieter hat die Verstöße innerhalb eines von der KBV zu bestimmenden, angemessenen Zeitraums zu beseitigen. Der Anbieter ist dazu verpflichtet an der Überprüfung mitzuwirken.

Die Kosten der Überprüfungen trägt der Anbieter.

Die folgenden Überprüfungsmaßnahmen werden einmal im Rahmen der Zertifikatslaufzeit, frühestens mit Beginn des zweiten Jahres, nach den Maßgaben der KBV durchgeführt:

- Auditierung
  Es werden Überprüfungen der Einhaltung organisatorischer Maßgaben dieser Richtlinie durchgeführt. Diese Audits beinhalten eine Vor-Ort-Prüfung beim Anbieter sowie eine Prüfung ausgewählter Dokumente.
- Penetrationstest
  Es wird ein durch die KBV ausgewählter KV-SafeNet-Router und ein 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 zu Überprüfungszwecken mindestens ein im Rahmen der Zertifizierung geprüftes Gerät des Anbieters in der KBV. Die Auswahl dieses Gerätes erfolgt durch die KBV. Darüber hinaus ist der Anbieter 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.

2.1.4 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 Konzentrator einzusetzen, so muss jeweils die Konformität durch die Prüfstelle der KBV bestätigt werden. Diese Bestätigung hat keinen Einfluss auf die Laufzeit des Zertifikats.

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 Zertifikats nach der neuen Richtlinie rezertifizieren zu lassen.

2.1.6 Laufzeit

Ein ausgestelltes Zertifikat erlischt nach drei Jahren und muss vom Anbieter neu beantragt werden. 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. Das Zertifikat erlischt mit Einstellung des Rezertifizierungsverfahrens, ohne dass es auf die Bestandkraft dieser Entscheidung ankommt.

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 Zertifikats alle Dokumente und Geräte durch die KBV-Prüfstelle erfolgreich rezertifiziert 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 Ergänzende Erklärung [KBV_SNK_FOEX_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 sichere Netz der KVen angebundenen Teilnehmern mit einer Vorlaufzeit von einem halben Jahr mitteilen. Wird diese Vorlaufzeit nicht eingehalten, so trägt der Anbieter die Kosten für den Wechsel des Teilnehmers zu einem anderen Anbieter, nicht jedoch die laufenden Kosten nach dem Wechsel.

2.1.8 Kostentragung

Für Zertifizierungen und Rezertifizierungen werden nach dem Leitfaden Kosten (Gebühren und Auslagen, siehe [KBV_SNK_LFEX_Zert_KV-SafeNet]) erhoben, wenn ein Anbieter eine Zertifizierung oder Rezertifizierung nach Abschnitt 2.1.1 beantragt hat. Kosten werden auch erhoben, wenn ein auf Vornahme einer Zertifizierung oder Rezertifizierung gerichteter Antrag abgelehnt oder zurückgenommen wird. Die Gebührenschuld entsteht mit der Beendigung der Zertifizierung oder Rezertifizierung oder mit der Rücknahme des Antrages. Kosten werden mit der Bekanntgabe der Kostenentscheidung an den Kostenschuldner fällig, wenn nicht die KBV einen späteren Zeitpunkt bestimmt.

Die Zertifizierungen und Rezertifizierungen können von der vorherigen Zahlung eines angemessenen Kostenvorschusses abhängig gemacht werden.

2.1.9 Entzug des Zertifikats

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.

Verweigert der Anbieter im Fall der Überprüfung der Einhaltung der vorgeschriebenen Voraussetzungen, bei deren Wegfall ein Grund zur Rücknahme oder zum Widerruf einer Erlaubnis gegeben wäre, seine Mitwirkung, so kann die KBV deren Wegfall vermuten.

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 Kassenärztlichen Vereinigungen 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.

2.2 Anbindung

2.2.1 Anzahl Einwahlknoten

Der Anbieter installiert in zwei unterschiedlichen KVen 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.

Für die Installation der Konzentratoren stehen die folgenden KVen bereit:

- KV Bayerns, Elsenheimerstraße 39, 80687 München
- KV Hessen, Georg-Voigt-Straße 15, 60325 Frankfurt
- KV Niedersachsen, Berliner Allee 22, 30175 Hannover
- KV Nordrhein, Tersteegenstraße 9, 40474 Düsseldorf
- KV Westfalen-Lippe, Robert-Schimrigk-Straße 4-6, 44141 Dortmund

Es steht der KBV frei, weitere Knoten zu benennen.

2.2.2 Nutzung des KV-Backbones

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

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

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 sicheren Netz der KVen 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. Diese Vorschrift ist für den Anbieter bindend. Die Nachweispflicht für die Überlastung liegt auf Seiten der KBV.

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 Konzentratoren übernimmt der Anbieter.

Die KV oder deren Dienstleister werden die tatsächlich anfallenden Kosten für Infrastrukturerweiterungen, die durch die Aufstellung und den Anschluss des Konzentrators des Anbieters entstehen, dem Anbieter in Rechnung stellen.

Die geeigneten Räumlichkeiten stellt die KV bereit, die Mietkosten trägt der Anbieter. Die KV gewährt dem Anbieter entsprechend den jeweils gültigen Sicherheitsvorschriften für Servicearbeiten an seinem 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. Die KVen benennen einen Ansprechpartner für organisatorische und verwaltungstechnische Fragen des Anbieters.

2.2.8 Teststellungen der angebotenen Anbindungsvarianten

Es ist dem zertifizierten Zugangsprovider erlaubt, eine Teststellung der Anbindung der angebotenen KV-SafeNet-Router an den Konzentrator pro Anbindungsvariante zu Analyse- und Supportzwecken vorzuhalten.

2.2.9 Ausschluss des Supports durch die KV/KBV

Die KV/KBV übernimmt keinerlei Supportanfragen seitens der Teilnehmer, die im Zusammenhang mit der Anbindung an das sichere Netz der KVen durch den Anbieter entstehen.

2.3 Schutz der Anbindung

Zugriffe auf das sichere Netz der KVen 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 (siehe BSI-Maßnahme M 2.11)[2]
- Benutzung aller relevanten und rechtmäßigen Protokollmechanismen, um Störfälle und Angriffsversuche analysieren zu können

[2] BSI-Maßnahme M 2.11 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

- Regelung und Dokumentation der Benutzerrechte (siehe BSI-Maßnahmen M 2.30, M 2.31)[3]
- Einsatz von geeigneter Sicherheits-Software

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

2.4.1 Technische Berichte

Der Anbieter hat die in dieser Richtlinie geforderte Verfügbarkeit[4] in Form eines monatlichen Reports nachzuweisen. Dieser Report beinhaltet auch alle Formen von sicherheitsrelevanten Stör- bzw. Vorfällen (Incidents). Eine Kategorisierung der Incidents erfolgt auf Basis der BSI Gefährdungskataloge[5]. Der Report ist der KBV zu übermitteln und muss die folgenden Mindestangaben beinhalten:

- Art und Anzahl der Störfälle / sicherheitsrelevante Vorfälle (Incidents[6])
- Anzahl geplanter Ausfälle und Changes

Diese Angaben erfolgen jeweils mit

- Datum,
- Beginn,
- Ende,
- Dauer sowie
- durchgeführten und geplanten Maßnahmen.

2.4.2 Teilnehmerstatistiken

Der Anbieter hat den für die jeweiligen Mitglieder zuständigen KVen eine monatliche Teilnehmerstatistik spätestens innerhalb der ersten Woche des Folgemonats bereitzustellen. Folgende Informationen sind dabei zu übermitteln:

- Neuanmeldungen
- Vertragskündigungen
- Anzahl der Teilnehmer
- Anzahl der Sperrungen von Teilnehmern

Das Datenformat zur Übermittlung der Statistiken ist in Anhang B.2 verbindlich definiert.

[3] BSI-Maßnahmen M 2.30 und M 2.31 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.
[4] Unter Verfügbarkeit wird die Eigenschaft von Ressourcen verstanden, auf Verlangen zugänglich und nutzbar zu sein.
[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/inhalt_node.html
[6] Ein Störfall / sicherheitsrelevanter Vorfall ist ein einzelnes oder eine Reihe von unerwünschten oder unerwarteten Ereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert oder bedroht werden.

2.4.3 Statistiken über KV-SafeNet-Anschlüsse

Der Anbieter hat der KBV monatlich eine Übersicht über KV-SafeNet-Anschlüsse bereitzustellen. Folgende Informationen sind dabei zu berücksichtigen:

- Eingesetzte Typen von KV-SafeNet-Routern
- Anzahl der KV-SafeNet-Router je Router-Typ
- Anzahl der angeschlossenen Teilnehmer je Router-Typ

Das Datenformat zur Übermittlung der Statistiken ist in Anhang B.3 verbindlich definiert.

2.4.4 Vertragsstatistiken

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

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

Der Anbieter stellt der KBV die aktuellen Preise und Leistungen zur Verfügung und erklärt sich mit der Veröffentlichung der Daten einverstanden. Der KBV steht es frei, die regulären Preislisten aller Anbieter zu veröffentlichen.

Bei Änderungen der Preise oder Leistungen stellt der Anbieter der KBV die neuen Preise oder geänderten Leistungen unaufgefordert und unverzüglich zur Verfügung.

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 sichere Netz der KVen zu gewähren.

Der Anbieter verpflichtet sich, ausschließlich das im Rahmen der Zertifizierung eingereichte Muster als Teilnehmervertrag zu verwenden. Er ist verpflichtet den jeweils zertifizierten Teilnehmervertrag gegenüber dem Teilnehmer zu verwenden. Bestehende Verträge sind durch den Anbieter anzupassen.

Sofern der Anbieter ein Kombi-Angebot anbietet, hat er für die Zertifizierung nur den KV-SafeNet-Teilnehmervertrag einzureichen.

Die folgenden Anforderungen müssen im Teilnehmervertrag berücksichtigt sein.

2.5.1 Vertragspartner

Vertragspartner des Anbieters bei der Leistungserbringung ist ausschließlich der Teilnehmer.

2.5.2 Vertragsvoraussetzung

Voraussetzung für die Wirksamkeit des Vertrags zwischen Teilnehmer und Anbieter ist die Zulassung des Teilnehmers zum sicheren Netz der KVen durch die jeweils zuständige KV. Im Speziellen kann die Zulassung eines Teilnehmers auch durch die KBV in Abstimmung mit den KVen erfolgen, falls dieser von bundesweiter Bedeutung ist.

Der Anbieter muss im Rahmen des Vertrages den Teilnehmer über sein Zertifikat und die entsprechende Zertifikatslaufzeit informieren.

2.5.3 Vertragsverlängerung

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

2.5.4 Kontrollrecht des Teilnehmers

Der Vertrag zwischen Teilnehmer und Anbieter beinhaltet ein Kontrollrecht des Teilnehmers hinsichtlich der fortlaufenden Einhaltung aller Vorgaben dieser Richtlinie, welches die KBV für ihn ausüben kann.

2.5.5 Ordentliche Kündigung

Der Vertrag zwischen Anbieter und Teilnehmer muss ordentlich kündbar sein. Als ordentlicher Kündigungsgrund gilt die Verfügbarkeit der von der Bundesregierung geplanten Telematikinfrastruktur (TI). Diese ist verfügbar, wenn die Betreibergesellschaft gematik GmbH den Produktivstart der TI erklärt und der TI-Konnektor für den Teilnehmer verfügbar ist. Ab diesem Zeitpunkt müssen die bestehenden KV-SafeNet-Verträge mit einer Frist von sechs Monaten kündbar sein. Durch die Ausübung des ordentlichen Kündigungsrechts dürfen dem Teilnehmer keine Kosten entstehen.

2.5.6 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, ist dem Teilnehmer ein Sonderkündigungsrecht mit Wirksamkeit zum Ende der Laufzeit des derzeitig gültigen Zertifikates einzuräumen. Der Anbieter hat zudem die Pflicht und die entsprechende KV das Recht, den Teilnehmer vier Monate vor Ende der Gültigkeit des Zertifikats entsprechend zu informieren.

Hinweis: KV-SafeNet-Anbietern steht es frei, die Zulassung als TI-Provider anzustreben, um für die eigenen Kunden einen leichten Übergang in die TI zu ermöglichen.

2.5.7 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 sicheren Netz der KVen mehr möglich ist.

Werden KV-SafeNet-Router dem Teilnehmer im Rahmen eines Mietverhältnisses überlassen, ist bei Vertragsende durch den Anbieter die unverzügliche Rückgabe des Gerätes einzufordern. Erwirbt der Teilnehmer Eigentum am KV-SafeNet-Router, so ist bei Vertragsende durch den Anbieter das Gerät so zurückzusetzen, dass keine Konfigurationsmerkmale mit Bezug auf das sichere Netz der KVen verbleiben.

2.5.8 Haftungsausschluss

Die KV/KBV übernimmt keine Haftung bezüglich der Verfügbarkeit des Zugangsnetzes des Anbieters.

Die KV/KBV übernimmt keine Gewährleistung bezüglich der IT-Sicherheit des Zugangsnetzes des Anbieters.

Die KV/KBV übernimmt keine Haftung bezüglich der Sicherheit des Teilnehmernetzwerks.

2.5.9 Transparenz des Angebotes

Sämtliche Kosten des Teilnehmervertrages müssen im Angebot vollständig und nachvollziehbar aufgelistet werden.

Es muss aus dem Angebot klar ersichtlich sein, ob dem Teilnehmer durch den Anschluss an das sichere Netz der KVen weitere, nicht in der Verantwortung des Anbieters liegende Kosten entstehen. Diese müssen namentlich aufgelistet sein.

Sämtliche technischen Voraussetzungen auf Seiten des Teilnehmers für eine Anbindung an das sichere Netz der KVen müssen im Angebot beschrieben sein.

2.5.10 Bereitstellungszeitraum des Zugangs

Der Anbieter garantiert dem Teilnehmer die Bereitstellung eines Zugangs zum sicheren Netz der KVen mindestens für die Dauer der Vertragslaufzeit.

2.5.11 Teilnehmersupport des Anbieters

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

Der Anbieter stellt dem Teilnehmer einen kostengünstigen telefonischen Zugang zu seinem Support zur Verfügung.

Die telefonische Support-Hotline muss den direkten Kontakt mit dem internen 1st-Level-Support des Anbieters gewährleisten. Ein Anschluss an den Support über einen Drittanbieter ist ausgeschlossen.

2.5.12 Servicezeiten

Der Anwendersupport 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:

- Von Montag bis Freitag: zwei Stunden
- an Wochenenden und Feiertagen: Nächster Arbeitstag 8:00 Uhr + zwei Stunden

Die Wiederherstellungszeit bei durch den Anbieter verursachten technischen Problemen beträgt:

- Von Montag bis Freitag: 24 Stunden ab Eingang der Störungsmeldung
- an Wochenenden und Feiertagen: Nächster Arbeitstag 8:00 Uhr + 24 Stunden

2.5.13 Vertragsstrafe

Der Teilnehmervertrag muss eine Vertragsstrafe im Falle der Überschreitung der Wiederherstellungszeit durch den Anbieter enthalten. Die Vertragsstrafe beträgt für jeden weiteren angefangenen Kalendertag mindestens 100,00 €. Eine Begrenzung auf 1.000,00 € pro Jahr ist dem Anbieter freigestellt.

Diese Vertragsstrafe befreit den Anbieter nicht von Regressansprüchen seitens des Teilnehmers für Schäden, die diesem durch einen Verstoß des Anbieters gegen diese Richtlinie entstanden sind.

2.5.14 Vorbehalt der KV/KBV

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

2.5.15 Mindestumfang des Angebotes

Mindestumfang des Angebotes ist die exklusive Anbindung an das sichere Netz der KVen über die Zugangsvariante KV-SafeNet.

2.5.16 Mehrwertdienste

Darüber hinausgehende Angebote von Diensten des Anbieters müssen

- gesondert gekennzeichnet sein,
- explizit mit Unterschrift beauftragt werden und
- den Sicherheitsmaßnahmen in Abschnitt 2.6.16 gerecht werden.

2.5.17 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. Dieser Router baut ein virtuelles privates Netzwerk (VPN) zu einem Konzentrator in einer KV auf, welches die Verbindung vom normalen Internet abschottet und so einen abgesicherten Datenaustausch mit dem sicheren Netz der KVen ermöglicht.

Es wird empfohlen, nach Common Criteria (Evaluation Assurance Level 4+) zertifizierte Geräte einzusetzen.

2.6.2 VPN-Konzentratoren

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

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

Es wird empfohlen, nach Common Criteria (Evaluation Assurance Level 4+) zertifizierte Geräte einzusetzen.

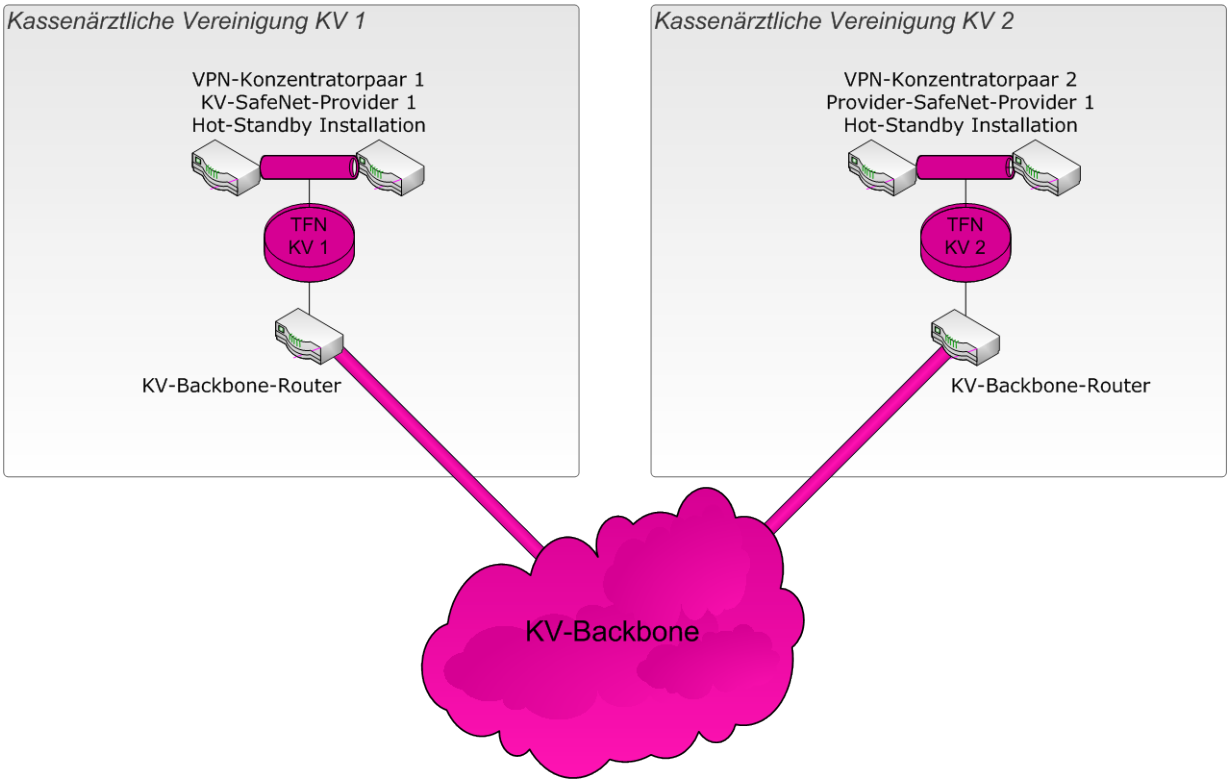

Abbildung 2: Hot-Standby Betrieb der VPN-Konzentratoren

2.6.3 VPN Verbindungsart

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

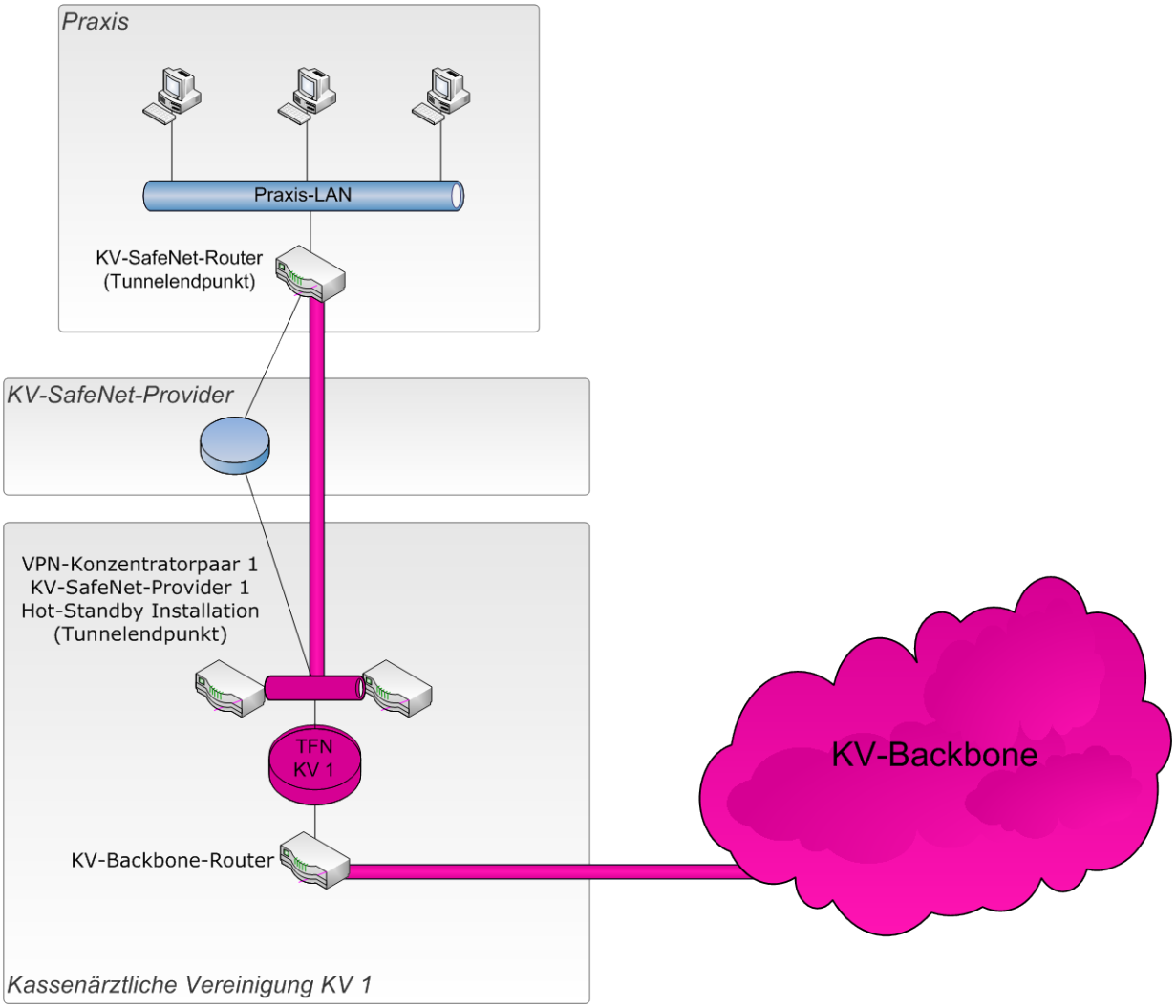

Abbildung 3: Site-to-Site Tunnelendpunkte

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 Konzentrator muss durch geeignete Sicherheitsmaßnahmen sicherstellen, dass jegliche unbefugte Zugriffe auf das sichere Netz der KVen, den KV-SafeNet-Router, den 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 sichere Netz der KVen für den KV-SafeNet-Router und den Konzentrator Zugriffslisten (sogenannte ACL, Access Control Lists) umzusetzen.

2.6.5 Adressierung

Die zur Adressierung der Teilnehmer am sicheren Netz der KVen benötigten IP-Adressräume werden zentral von der Kassenärztlichen Bundesvereinigung 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 sichere Netz der KVen [KBV_SNK_KNEX_Routing] einzuhalten.

2.6.8 DNS

Zur Adressierung der im sicheren Netz der KVen 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 sicheren Netz der KVen betrieben. Der Anbieter hat dafür zu sorgen, dass die Teilnehmer am sicheren Netz der KVen 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 sichere Netz der KVen 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 der vom BSI herausgegebenen „Technischen Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102)[7] sowie den BSI-Maßnahmen M 5.76 und M 2.164[8] entnommen werden.

Im Speziellen ist auf den Einsatz von Pre-Shared-Keys im Rahmen der Kryptografie zu verzichten. Der Einsatz von Zertifikaten (z. B. X.509) ist verbindlich.

[7] BSI TR-02102 siehe: https://www.bsi.bund.de.
[8] BSI-Maßnahmen M 5.76 und M 2.164 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

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 (siehe BSI-Maßnahmen M 4.201 und M 4.202)[9].

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 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 bei Bedarf in Absprache mit dem Teilnehmer unter Einhaltung der Datenschutzbestimmungen zulässig. Entsprechende Regelungen sind in den Verträgen mit den Teilnehmern festzuhalten.

Insbesondere bei der Fernwartung ist durch den Anbieter zu gewährleisten, dass der Teilnehmer die aktive Möglichkeit hat, den Wartungszugang zu steuern. Dieses ist dann gegeben, wenn der Teilnehmer zum einen im Grundsatz der Fernwartung zustimmen und zum anderen den jeweiligen Wartungszugriff überwachen kann.

Der Anbieter hat des Weiteren die Pflicht, alle Wartungsaktivitäten umfassend zu protokollieren und die Protokolle dem Teilnehmer auf Anforderung zur Einsicht zu überlassen. Auf Wunsch des Teilnehmers sind auch von ihm beauftragte Personen berechtigt, diese Protokolle zu prüfen.

Der Anbieter hat die Pflicht, den Teilnehmer über Zeitpunkt und Inhalt aller durchgeführten Wartungs- und Administrationsaktivitäten auf Verlangen schriftlich zu informieren.

Der Anbieter hat sicherzustellen, dass eine Gefährdung des KV-SafeNet-Routers, des Teilnehmernetzwerks oder des sicheren Netzes der KVen durch einen Fernzugriff im Rahmen von Wartungsarbeiten ausgeschlossen ist.

Das Vorgenannte gilt auch, wenn die Wartungsaktivitäten vom KV-SafeNet-Router initiiert werden. Dabei ist unerheblich, ob diese Aktivitäten automatisch oder manuell erfolgen.

[9] BSI-Maßnahmen M 4.201 und M 4.202 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de.

Für die Fernwartung der Konzentratoren sollen nach Möglichkeit separate ISDN-Anschlüsse, eigene MPLS-Anbindungen oder gesicherte Internetanbindungen genutzt werden. Management-Ports an KV-SafeNet-Routern und Konzentratoren dürfen jedoch nicht aus dem sicheren Netz der KVen 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 sicheren Netz der KVen gelten die vom BSI aufgestellten Anforderungen für die „Sichere Anbindung von lokalen Netzen an das Internet (ISi-Lana)“[10] sowie die von der KBV und der Bundesärztekammer herausgegebenen Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis[11].

Eine wichtige und daher empfehlenswerte Standardmaßnahme zum Schutz des Teilnehmers und des sicheren Netzes der KVen 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 (siehe BSI-Maßnahme M 2.11)
- Benutzung aller relevanten und rechtmäßigen Protokollmechanismen um Störfälle und Angriffsversuche analysieren zu können
- Regelung und Dokumentation der Benutzerrechte (siehe BSI-Maßnahmen M 2.30, M 2.31)[12]
- Einsatz von geeigneter Sicherheits-Software

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

[10] ISi-Lana siehe: https://www.bsi.bund.de.
[11] Siehe: http://www.baek.de/page.asp?his=0.7.47.6188
[12] BSI-Maßnahmen M 2.30 und M 2.31 im Rahmen der Grundschutzkataloge siehe: https://www.bsi.bund.de

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 Netz 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.
Kombi-Angebot	Der Telekommunikationsanschluss (bspw. Internetanbindung) wird neben dem KV-SafeNet-Anschluss ebenfalls durch den Antragssteller realisiert.
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.
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 der 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.

4 Referenzierte Dokumente

Referenz	Dokument
[KBV_SNK_KNEX_DNS]	Konzept DNS
[KBV_SNK_KNEX_Routing]	Konzept Routing
[KBV_SNK_KNEX_IP-Adressvergabe]	Konzept IP-Adressvergabe
[KBV_SNK_LFEX_Zert_KV-SafeNet]	Leitfaden Zertifizierung KV-SafeNet-Provider
[KBV_SNK_LFEX_Überprüfung_Provider]	Leitfaden Überprüfung Provider
[KBV_SNK_FOEX_KV-SafeNet]	Formular Ergänzende Erklärung zur Zertifizierung zum KV-SafeNet-Provider

ANHANG

A Ansprechpartner der KBV und der KVen

Kassenärztliche Bundesvereinigung
KBV Service Desk, Tel: 030 4005-2121
E-Mail: snk-services@kbv.de

KV Bayerns
Online-Dienste, Tel: 089 57093-4004-0
E-Mail: online-dienste@kvb.de

KV Westfalen-Lippe
Herr Frank Winkler, Tel: 0231 9432-3226
E-Mail: Frank.Winkler@kvwl.de

KV Nordrhein
Herr Dirk Gohe, Tel: 0211 5970-8311
E-Mail: it@kvno.de

KV Sachsen
Herr Peter Heilmann, Tel. 0351 8290-700
E-Mail: snk@kvsachsen.de

KV Baden-Württemberg
Herr Jens Sommer, Tel 0711 7875-3503
E-Mail: jens.sommer@kvbawue.de

KV Hessen
info.line, Tel. 069 79502-602
E-Mail: info.line@kvhessen.de

KV Thüringen
Herr Wilfried Schmidt, Tel. 03643 559-110
E-Mail: wschmidt@kvt.de

KV Mecklenburg-Vorpommern
Herr Christian Ecklebe, Tel. 0385 743-1257
E-Mail: cecklebe@kvmv.de

KV Sachsen-Anhalt
Herr Stefan Troschke, Tel. 0391 627-7000
E-Mail: volker.grasshoff@kvsa.de

KV Hamburg
Herr Hans-Heinrich Faby, Tel: 040 2280-2368
E-Mail: hans-heinrich.faby@kvhh.de

KV Niedersachsen
Herr Maik Jahnke, Tel: 0511 380-3388
E-Mail: maik.jahnke@kvn.de

KV Bremen
Herr G. Antpöhler, Tel.: 0421 3404-120
E-Mail: g.antpoehler@kvhb.de

KV Schleswig-Holstein
Herr Udo Karlins, Tel. 04551 883-432
E-Mail: udo.karlins@kvsh.de

KV Rheinland-Pfalz
Herr Franz Masfelder, Tel. 0261 39002-260
E-Mail: franz.masfelder@kv-rlp.de

KV Saarland
Herr Patrick Schumacher, Tel. 0681 998-370
E-Mail: p.schumacher@kvsaarland.de

KV Brandenburg
Herr Kai-Uwe Krüger, Tel. 0331 2309-337
E-Mail: kai-uwe.krueger@kvbb.de

KV Berlin
Herr Andreas Mahling, Tel 030 31003-293
E-Mail: andreas.mahling@kvberlin.de

B Einheitliche Meldestruktur der Statistiken

Gemäß der Richtlinie KV-SafeNet sind die KV-SafeNet-Zugangsprovider zu einem monatlichen Bericht der Teilnehmer-Statistik verpflichtet.

Eine Standardisierung des Statistikformats soll sowohl auf Seiten der Provider als auch auf Seiten der KBV/KVen die Arbeitsabläufe vereinfachen.

Die monatliche Meldedatei ist eine CSV-Datei im ASCII-Format mit definiertem Inhalt (→ Datensatzbeschreibung) und einem der jeweiligen Provider-KV-Beziehung entsprechenden Dateinamen (→ Dateinamenskonvention).

B.1 Dateinamenskonvention

<Dateiname> ::= 'monatsstatistik' . 'p' <ProviderID> . 'kv' <KVID> . <Jahr> . <Monat> . 'csv'

Dateiname der monatlichen Statistikmeldung.

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste KV-SafeNet-Provider
(vgl. http://www.kbv.de/media/sp/KBV_ITA_SIEX_Verzeichnis_KV_SafeNet.pdf).

<KVID> ::= 01 | 02 | 03 | ... | 99

KV-Nummer der KV[13], die den Teilnehmer anerkannt hat.

<Jahr> ::= 2000...2099

Jahr der Statistikmeldung

<Monat> ::= 01 | 02 | 03 | ... | 10 | 11 | 12

Monat der Statistikmeldung

Beispiel:
monatsstatistik.p001.kv02.2011.07.csv → PROVIDER ABC an KV XYZ für Juli 2011

[13] http://applications.kbv.de/keytabs/ita/schluesseltabellen.asp?page=S_KBV_KV_V1.06.htm

B.2 Datensatzbeschreibung Teilnehmerstatistik für KV

<Meldungen> ::= <Meldung> { 'CRLF' <Meldung> }

Datei mit einer Liste von Einträgen

<Meldung> ::= <ProviderID> ; <KVID> ; <BSNr> ; <LANr> ; <IP-Adresse> ;
<Beginn> ; [<Ende>]; <AnzahlTeilnehmer> ; <Internet>

Auflistung der Meldungsparameter je Provider-Arzt-Vertrag

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste[14] KV-SafeNet-Provider.

<KVID> ::= 01 | 02 | 03 | ... | 99

KV-Nummer der KV[15], die den Teilnehmer anerkannt hat.

<BSNr> ::= 010000000...999999999

Neunstellige Betriebsstättennummer der Praxis / Einrichtung

<LANr> ::= 010000000...999999999

Neunstellige „Lebenslange Arztnummer" des Vertragspartners

<IP-Adresse> ::= 188.144.0.1 – 188.145.255.254

IP-Adresse des Teilnehmers im SNK. Wenn diese dynamisch vergeben wird, ist die Angabe eines IP-Bereichs möglich.

<Beginn> ::= (1...31) . (1...12) . (2000...2099)

Datum des Vertragsbeginns (TT.MM.JJJJ)

<Ende> ::= (1...31) . (1...12) . (2000...2099)

Datum der Vertragskündigung (TT.MM.JJJJ)

<AnzahlTeilnehmer> ::= <numerischerWert>

Numerischer Wert: Anzahl der Teilnehmer, die über einen KV-SafeNet-Anschluss an das sichere Netz der KVen angeschlossen sind.

<Internet> ::= 'j' | 'n'

Ist bei dem SafeNet-Vertrag der Mehrwertdienst „Internet" freigeschaltet? j=Ja, n=Nein

[14] http://www.kbv.de/media/sp/KBV_ITA_SIEX_Verzeichnis_KV_SafeNet.pdf
[15] http://applications.kbv.de/keytabs/ita/schluesseltabellen.asp?page=S_KBV_KV_V1.06.htm

Beispielinhalt: monatsstatistik.p001.kv02.2011.07.csv (Provider an KVHH für Juli ´11)
18;2.3;02;021234564;111222333;188.144.179.132;24.02.2009;;1;j
18;2.3;02;024445555;081547110;188.144.179.144;04.12.2007;31.03.2009;2;n

B.3 Datensatzbeschreibung KV-SafeNet-Statistik für KBV

<Meldungen> ::= <Meldung> { 'CRLF' <Meldung> }

Datei mit einer Liste von Einträgen

<Meldung> ::= <ProviderID> ; <TypRouter>; <AnzahlRouter>; <AnzahlTeilnehmer>

Auflistung der Meldungsparameter je Provider-Arzt-Vertrag

<ProviderID> ::= 001 | 002 | 003 ... | 999

Eindeutige ID des KV-SafeNet-Providers; entspricht den letzten drei Stellen der Prüfnummer gemäß Zulassungsliste[16] KV-SafeNet-Provider.

<TypRouter> ::= <text>

Freitext für die Bezeichnung des KV-SafeNet-Routers

<AnzahlRouter> ::= <numerischerWert>

Numerischer Wert: Anzahl der KV-SafeNet-Router je Routertyp

<AnzahlTeilnehmer> ::= <numerischerWert>

Numerischer Wert: Anzahl der Teilnehmer, die über einen KV-SafeNet-Anschluss an das sichere Netz der KVen angeschlossen sind.

[16] http://www.kbv.de/media/sp/KBV_ITA_SIEX_Verzeichnis_KV_SafeNet.pdf