KAMP SafeBox – Antragsformular

KV-SafeNet-Access für Krankenhäuser und med. Einrichtungen

gemäß Richtlinie KV-SafeNet (Netzkopplung) in der Version 1.0 vom 31.10.2011,
basierend auf der KV-SafeNet Rahmenrichtlinie 3.2 vom 31.07.2015,
mit KAMP-Zertifikatsgültigkeit bis zum 28.02.2019

Internet-Status

Ist ein Internet-Anschluss zur Nutzung der KAMP SafeBox-Lösung vorhanden?

☐ Ja ☐ Ein Zugang wird durch KAMP geschaltet und gesondert beauftragt

Fernwartungsoption

Wenn Sie keine Fernwartung wünschen, können im Supportfall gesonderte Kosten entstehen.

☐ Ja, gewünscht ☐ Nein, eine Fernwartung durch KAMP ist nicht gewünscht

Antragsteller (Betreiber der anzuschließenden Netzinfrastruktur)

Name der med. Einrichtung

Straße/Hausnummer

PLZ/Ort

Vorwahl/Telefonnummer

Vorwahl/Faxnummer

E-Mail-Adresse

Zuständige KV

SEPA-Lastschriftmandat

KAMP Netzwerkdienste GmbH, Vestische Straße 89–91, 46117 Oberhausen, Gläubiger-Identifikationsnummer DE10ZZZ00000166435, Mandatsreferenz wird bei Rechnungsstellung mitgeteilt.

Ich/Wir ermächtige(n) den Zahlungsempfänger, Zahlungen von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise(n) ich/wir mein/unser Kreditinstitut an, die vom Zahlungsempfänger auf mein/unser Konto gezogenen Lastschriften einzulösen. Hinweis: Ich kann/Wir können innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem/unserem Kreditinstitut vereinbarten Bedingungen. Vor dem ersten Einzug einer SEPA-Basislastschrift wird der Zahlungsempfänger mich/uns über den Einzug in dieser Verfahrensart unterrichten.

Kontoinhaber:

BIC:

IBAN: D E

Ort, Datum, Unterschrift des Kontoinhabers:

Mit der KAMP SafeBox wird die Anbindung an das KV-SafeNet durch einen vorhandenen Internet-Anschluss ermöglicht. Nur durch den Vertrag zwischen Anbieter und Antragsteller entsteht kein Anspruch gegenüber der KV/KBV auf Zulassung zum Sicheren Netz der KVen. Der Vertrag erlangt nur dann Gültigkeit, wenn die zuständige KV diesem ausdrücklich zugestimmt hat. Die Grundlage dieses Vertrages ist die Richtlinie KV-SafeNet (Netzkopplung) in der Version 1.0 vom 31.10.2011, im Folgenden „Richtlinie KV-SafeNet" genannt. Der Antragsteller ist für die Bereitstellung des Internetanschlusses selbst verantwortlich. Eventuelle zusätzliche Kosten, die durch die Bereitstellung eines Internetanschlusses entstehen, werden nicht durch KAMP getragen. Der Antragsteller erhält im Rahmen des Projektes KV-SafeNet einen Zugriff auf das Backbone der Kassenärztlichen Vereinigungen.

[ ] **Der „Antrag auf Zulassung von Teilnehmern zum Sicheren Netz der KVen – Teil 1" und „Antrag auf Zulassung von Teilnehmern zum Sicheren Netz der KVen – Teil 2", das Dokument „KAMP SafeBox – Technisches Beiblatt – Teil 1", „KAMP SafeBox – Technisches Beiblatt – Teil 2", der „Antrag zum Einrichten von Mehrwertdiensten auf der KAMP SafeBox", die „Vertrags- und Leistungsbedingungen für KAMP SafeBox", das KBV-Dokument „Sicheres Netz der KVen – Merkblatt Sicherheitsanforderungen KV-SafeNet-Arbeitsplätze" (Version 1.1) sowie die „Allgemeinen Geschäftsbedingungen der KAMP Netzwerkdienste GmbH" sind Bestandteil dieses Vertrages. Ich habe die Dokumente erhalten und akzeptiere sie.**

[ ] **Ich bestätige, dass alle angeschlossenen Teilnehmer das „Merkblatt – Pflichten des Betreibers der anzuschließenden Netzinfrastruktur und der darin befindlichen Teilnehmer" zur Kenntnis genommen haben bzw. spätestens dann zur Kenntnis nehmen werden, sobald Ihre Anbindung an die Netzinfrastruktur erfolgt ist.**

Ort, Datum, Unterschrift Antragsteller

Ort, Datum, Unterschrift KAMP Netzwerkdienste GmbH

Hiermit bestätigt die KV, dass der Antragsteller zur Teilnahme am KV-SafeNet berechtigt ist.

Ort, Datum, Stempel KV, Unterschrift

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Antrag auf Zulassung von Teilnehmern zum Sicheren Netz der KVen – Teil 1

Name der medizinischen Einrichtung

Straße/Hausnummer

PLZ/Ort

Art der Datenübermittlung für die Teilnehmerzulassung

KAMP bietet die Möglichkeit, die Benennung der berechtigten Teilnehmer im „Antrag auf Zulassung von Teilnehmern zum Sicheren Netz der KVen - Teil 2“ digital zu übermitteln. Dieses PDF-Antragsdokument ist ausfüllbar und ist an „teilnehmerzulassung@kamp.de“ zu übersenden.

Hinweis: Bei Nutzung der digitalen Übermittlungsvariante ist der Antragsteller verpflichtet, Teil 1 des Antrages auf Zulassung von Teilnehmern zum KV-SafeNet unterschrieben per Fax oder Brief miteinzureichen!

[ ] Die Benennung der berechtigten Teilnehmer erfolgt digital.

[ ] Die Benennung der berechtigten Teilnehmer erfolgt per Post oder Fax über nachfolgende Liste.

Ausschließlich für die im Antrag auf Zulassung von Teilnehmern zum KV-SafeNet Teil 2 genannten Teilnehmer wird ein zweckgebundener Zugang zum Sicheren Netz der KVen beantragt. Berechtigte Teilnehmer sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und -psychotherapeuten sowie ggf. Teilnehmer, die Dienste der KVen nutzen möchten. Teilnehmer können nur natürliche Personen sein, Gruppenberechtigungen sind nicht zulässig.

KAMP gewährt ausschließlich den nachfolgend benannten berechtigten Teilnehmern einen Zugang zum Sicheren Netz der KVen. Der Antragsteller ist verpflichtet, Änderungen der benannten Teilnehmer, z. B. wegen Kündigung des Arbeitsverhältnisses eines Teilnehmers, unverzüglich KAMP mitzuteilen.

Jeder berechtigte Teilnehmer erhält für seinen abgesicherten Zugang zum Sicheren Netz der KVen eine von KAMP eingerichtete persönliche Teilnehmerkennung. Diese Teilnehmerkennung darf nicht an andere Teilnehmer weitergegeben oder anderweitig missbraucht werden. Jeder Teilnehmer darf für den Zugang zum Sicheren Netz der KVen ausschließlich seine persönliche Kennung benutzen. Die Teilnehmerkennung wird per Einschreiben zugestellt. Aus diesem Grund müssen die benannten Teilnehmer über die oben genannte Anschrift der medizinischen Einrichtung per Post erreichbar sein. Die benannten Teilnehmer haben den Empfang des Schreibens eigenhändig zu quittieren. Die Teilnehmerkennungen werden ausschließlich durch KAMP eingerichtet, geändert, deaktiviert oder gelöscht.

Die KVen und die KBV haben die Pflicht, den Teilnehmerkreis zu kontrollieren und zu bestimmen. Die KVen und die KBV können innerhalb der Frist von drei Arbeitstagen ein Vetorecht für einzelne Teilnehmer ausüben. Nach Ablauf der Frist richtet KAMP die Teilnehmerberechtigungen auf der KAMP SafeBox ein. Weiterhin behalten sich die KVen und die KBV das Recht vor, Einsicht in die auf der KAMP SafeBox eingerichteten Teilnehmer zu bekommen und ggf. auch zu einem späteren Zeitpunkt einzelne Teilnehmer z. B. im Falle eines Missbrauchs zu sperren oder abzulehnen.

Der Antragsteller haftet für die Richtigkeit der Angaben.

Ort, Datum

Unterschrift Antragsteller

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Antrag auf Zulassung von Teilnehmern zum Sicheren Netz der KVen – Teil 2

Sollte der Platz in der Tabelle für die Anzahl der anzumeldenden Teilnehmer nicht ausreichen, kann dieses Blatt als Vorlage dupliziert werden.

Name der medizinischen Einrichtung

Straße/Hausnummer

PLZ/Ort

Ansprechpartner für nachfolgende Teilnehmerkennungen (Name/E-Mail)

Zuständige KV der nachfolgend benannten Teilnehmer

Benennung berechtigter Teilnehmer

Teilnehmer (Vorname/Nachname)	LANR	BSNR	zu nutzende Anwendungen

Der Antragsteller haftet für die Richtigkeit der Angaben.

Ort, Datum

Unterschrift Antragsteller

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

KAMP SafeBox – Technisches Beiblatt – Teil 1

Angaben zu Konfiguration, Ansprechpartner und Versand der KAMP SafeBox

Technischer Ansprechpartner

Name/Vorname

Vorwahl/Telefonnummer

Telefonnummer für Notfälle

Vorwahl/Faxnummer

E-Mail

Erreichbar von bis

Versandadresse für die KAMP SafeBox

Firma

Name/Vorname

Straße/Hausnummer

PLZ/Ort

IP-Informationen für die KAMP SafeBox

Bitte nennen Sie uns die gewünschte IP-Adresse der KAMP SafeBox in Ihrem internen KV-SafeNet-Netzwerk.

IP-Adresse

Netzmaske

IP-Informationen zum bestehenden Internetzugang

Wenn ein Internet-Zugang eines Fremdproviders genutzt werden soll, nennen Sie uns bitte nachfolgend die IP-Informationen Ihres Internet-Routers. Die IP des Internet-Routers muss sich in einem anderen Netzbereich als die KAMP SafeBox befinden. Beispiel: Netzbereich des Internet-Routers = 192.168.**0**.xxx, Netzbereich der KAMP SafeBox = 192.168.**1**.xxx

IP-Adresse Ihres Internet/DSL-Routers

Netzmaske

Freie IP-Adresse in Ihrem Netzwerk für die KAMP SafeBox

Externe (statische) IP-Adresse der KAMP SafeBox, wenn NAT zum Einsatz kommt

Ort, Datum

Unterschrift Antragsteller

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen **Kontakt** Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

KAMP SafeBox – Technisches Beiblatt – Teil 2

nur auszufüllen beim Betrieb von Terminalservern oder Clients hinter NAT-IPs

Bei Einsatz von Terminalservern oder Clients hinter NAT-IPs gilt Folgendes:

Da die Freischaltung der Dienste auf IP-Basis stattfindet (Freischaltung für authentisierte Quell-IPs) gibt es keine Möglichkeit zur Unterscheidung von Anwendern/Benutzern mit identischer IP-Adresse. Wenn eine Verbindung freigeschaltet wurde, kann diese von jedem weiteren Anwender/Benutzer ohne weitere Authentisierung genutzt werden. Daher ist der Betreiber verpflichtet, jedem KV-SafeNet Netzkopplungsteilnehmer unterschiedliche Quell-IPs zur eindeutigen Unterscheidung je Anwender/Benutzer zuzuordnen.

Wir nehmen die beschriebene, technische Spezifikation zur Kenntnis und verpflichten uns jedem KV-SafeNet Netzkopplungsteilnehmer unterschiedliche Quell-IPs zur eindeutigen Unterscheidung je Anwender/Benutzer zuzuweisen.

Ort, Datum

Unterschrift Antragsteller

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Antrag zum Einrichten von Mehrwertdiensten auf der KAMP SafeBox

Angaben zu den beantragten Mehrwertdiensten

Zieladresse Mehrwertdienst Einzeladresse/Adressbereich	Art des Dienstes	Name, Adresse

Daten Antragsteller

Stempel der med. Einrichtung

Ansprechpartner

Telefon Ansprechpartner

E-Mail

Die beantragten Mehrwertdienste werden gemäß der aktuell gültigen Richtlinie KV-SafeNet eingerichtet.

Das KBV-Dokument „Sicheres Netz der KVen - Merkblatt Sicherheitsanforderungen KV-SafeNet-Arbeitsplätze“ (Version 1.1, vom 31.01.2011) habe ich erhalten und akzeptiere es.

Ort, Datum

Unterschrift Antragsteller

Hiermit bestätigt die KV, dass dem Antragsteller die Einrichtung o.g. Mehrwertdienste auf dem KV-SafeNet-Router gestattet ist.

Ort, Datum, Unterschrift, Stempel KV

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Vertrags- und Leistungsbedingungen

für KAMP SafeBox der KAMP Netzwerkdienste GmbH, Vestische Straße 89–91, 46117 Oberhausen, im folgenden „KAMP“ genannt.

Der Antragsteller ist der Betreiber der anzuschließenden Netzinfrastruktur. Die kassenärztliche Bundesvereinigung wird im Nachfolgenden mit KBV abgekürzt, die Kassenärztliche Vereinigung mit KV.

1. Allgemeines

Der Anschluss von Teilnehmern der gesundheitsmedizinischen Netzinfrastruktur des Antragstellers an die Dienste der KVen erfolgt über einen KV-SafeNet-Zugang, der um einen Authentisierungsdienst erweitert wird (Netzkopplung).

Der Anschluss mittels KV-SafeNet erfolgt durch einen von der KBV zertifizierten Provider (KAMP). Dieser stellt dem Antragsteller alle technischen Voraussetzungen zur Anbindung an das Sichere Netz der KVen (KV-SafeNet) mittels einer Hardware-VPN-Lösung zur Verfügung und garantiert für die Sicherheit dieser Verbindung. KAMP stellt dem Antragsteller hierzu einen KV-SafeNet-Router zur Verfügung, die KAMP SafeBox. Voraussetzung für die Nutzung der KAMP SafeBox ist ein aktiver, uneingeschränkt nutzbarer Internetanschluss (i.d.R. intern übergeben durch eine Ethernet-Schnittstelle am Internet-Router). Wenn zwischen mehreren KV-SafeNet-Netzkopplungszugängen eine Verbindung geschaltet werden soll – wie z. B. im digitalen Mammographie-Screening – kann die KAMP SafeBox nur dann gewählt werden, wenn der genutzte Internetanschluss von KAMP bereitgestellt wird.

2. Leistungsmerkmale

Durch die KAMP SafeBox wird eine dedizierte Verbindung vom Netz des Antragstellers in den Backbone der KV hergestellt. KAMP routet die IP-Adressräume, die dem Antragsteller zugewiesen wurden.

Im Leistungsumfang der KAMP SafeBox ist Folgendes enthalten:

- Zugangsmöglichkeit zum KV-SafeNet über eine vorhandene Internetanbindung des Antragstellers
- Datentransfer innerhalb des KV-SafeNet-VPN
- Router/VPN-Gateway (KAMP SafeBox) als Leihstellung inklusive Hardwaretausch im Falle eines Defektes
- Authentifizierungsdienst zur Identifikation der zugelassenen Teilnehmer

KAMP sichert dem Antragsteller die Erreichbarkeit des Sicheren Netzes der KVen mindestens für den Zeitraum der Vertragslaufzeit zu.

3. Bereitstellung des Dienstes

KAMP stellt den Netzkopplungszugang nach Freigabe durch die zuständige Landes-KV zur Verfügung. In der Regel steht dem Antragsteller der Netzkopplungszugang innerhalb von 15 Arbeitstagen zur Verfügung. Die betriebsbereite Bereitstellung des Dienstes erfolgt durch die Zusendung der KV-SafeBox durch KAMP an den Antragsteller.

4. Authentisierung der Teilnehmer

Jeder berechtigte Teilnehmer erhält für seinen abgesicherten Zugang zum Sicheren Netz der KVen eine persönliche Teilnehmerkennung. Diese Teilnehmerkennungen dürfen nicht an andere Teilnehmer weitergegeben oder anderweitig missbraucht werden. Die Teilnehmerkennungen werden ausschließlich von KAMP eingerichtet und gepflegt, der Antragsteller hat keinen Zugriff auf die Teilnehmerkennungen.

Nur Teilnehmer, die von der KV bestätigt wurden, erhalten Zugang zum Sicheren Netz der KVen. Die KVen und die KBV behalten sich das Recht vor, auch zu einem späteren Zeitpunkt einzelne Teilnehmer im Falle eines Missbrauchs zu sperren.

Teilnehmerzugriffe auf das Sichere Netz der KVen werden von KAMP im rechtmäßigen Rahmen protokolliert. Änderungen der gesetzlichen Vorgaben zur Protokollierung werden von KAMP unverzüglich umgesetzt.

KAMP sperrt Teilnehmerkennungen nach fünfmaliger Fehleingabe des Teilnehmerpassworts. KAMP entsperrt Teilnehmerkennungen durch Vergabe eines neuen Teilnehmerpassworts. Der Prozess zur Übermittlung eines neuen Passworts erfolgt äquivalent zum initialen Prozess einer Teilnehmerkennung.

5. Vertragslaufzeit/Kündigung

Die Mindestvertragslaufzeit beträgt ab Datum der Bereitstellung der KV-SafeNet-Dienstleistung 36 Monate. Der Vertrag verlängert sich anschließend automatisch um jeweils weitere 12 Monate. KAMP ist vor einer Vertragsverlängerung mit dem Antragsteller dazu verpflichtet, bei der jeweils zuständigen KV die Rechtmäßigkeit der Zulassung des Antragstellers zum Sicheren Netz der KVen bestätigen zu lassen. Eine Kündigung ist schriftlich auszustellen und muss 3 Monate vor Ablauf des Vertrags bei KAMP eingegangen sein.

Dem Antragsteller steht ein ordentliches Kündigungsrecht zu. 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 ist der bestehende KV-SafeNet-Vertrag mit einer Frist von 6 Monaten kündbar.

Dem Antragsteller steht ein außerordentliches Kündigungsrecht aus wichtigem Grund zu, beispielsweise bei nicht erfolgter Aufklärung durch KAMP hinsichtlich der technischen Voraussetzungen, welche notwendig für den Netzkopplungsanschluss sind.

KAMP hat die Pflicht und die entsprechende KV das Recht, den Antragsteller 4 Monate vor Ende der Gültigkeit des Zertifikats entsprechend zu informieren, falls sich KAMP nicht rezertifizieren lassen hat. KAMP räumt dem Antragsteller hierbei ein außerordentliches Kündigungsrecht ein.

KAMP stellt bei Beendigung des Vertragsverhältnisses sicher, dass mit dem Tag des Vertragsendes kein Zugriff von Teilnehmern aus der angeschlossenen Netzinfrastruktur des Antragstellers zum Sicheren Netz der KVen mehr möglich ist.

Nach Beendigung des Vertragsverhältnisses muss die überlassene Hardware (KAMP SafeBox) innerhalb von 4 Wochen vollständig bei KAMP eingegangen sein. Die Kosten für die Rücksendung übernimmt der Antragsteller.

6. Rezertifizierung

Falls eine Rezertifizierung nicht angestrebt wird, muss KAMP mindestens 6 Monate vor Ablauf der Zertifikatsgültigkeit eine Information an den Antragsteller versenden. Bei einem Verstoß gegen diese Regelung übernimmt KAMP eventuelle Wechselkosten des Antragstellers zu einem anderen KV-SafeNet-Anbieter. Der Vertrag zwischen KAMP und dem Antragsteller erlischt bei Auflösung der KAMP-KV-SafeNet-Zertifizierung durch die KBV.

7. Verfügbarkeit

KAMP garantiert eine Verfügbarkeit des KV-SafeNet-Dienstes von 99,95%. „Verfügbarkeit” bezieht sich auf die Verfügbarkeit des KAMP KV-SafeNet-Dienstes, der im Rahmen des geschlossenen Vertrages, Bestandteil dieses Dokumentes ist. Die Verfügbarkeit bezieht sich insbesondere nicht auf die Verfügbarkeit der technologischen Infrastrukturen des Antragstellers (beispielsweise Netzwerkkomponenten, Internetanbindung o.Ä.) oder auf die Verfügbarkeit der technologischen Infrastrukturen und Dienste der KVen.

Die Verfügbarkeit wird wie folgt berechnet:

$$\text{Verfügbarkeit in \%} = 100 - \frac{\text{Ausfallzeit in Kalendertagen x 100}}{\text{Messperiode}}$$

Die Messperiode für die angegebene Verfügbarkeit beträgt jeweils ein rechnerisches Kalenderjahr von 365 Tagen.

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Die Ausfallzeit wird über das KAMP-Fehlermanagementsystem gemessen. Die Ausfallzeit beginnt, wenn der Antragsteller einen Fehler meldet oder das KAMP-Fehlermanagement einen Ausfall automatisch erkannt hat, der den KV-SafeNet-Dienst beeinträchtigt und ein Trouble-Ticket im Fehlermanagementsystem von KAMP geöffnet wird. Sie endet, wenn KAMP den Fehler behoben hat. KAMP wird den Antragsteller darüber informieren, wenn der Fehler behoben wurde. Ausfallzeiten aufgrund geplanter Wartungen werden nicht in die Berechnung der Verfügbarkeit aufgenommen.

8. Entstörzeiten

KAMP beginnt mit der Entstörung an ihren technischen Einrichtungen, im Rahmen der technischen Möglichkeiten, unverzüglich nach eigener Kenntnis oder nach ordnungsgemäßer Meldung seitens des Antragstellers. Resultiert eine Störung aus einem Problem der Internetanbindung und die Verbindung wird nicht durch KAMP gestellt, liegt die Problembeseitigung nicht im Verantwortungsbereich von KAMP und tangiert nicht die Entstörzeit. KAMP beseitigt Störungen im eigenen Backbone sowie Störungen des KV-SafeNet-Zugangs innerhalb von 12 Stunden.

9. Wartungsfenster

Zur Erhaltung und zur Ergänzung der KAMP-Netzinfrastruktur müssen regelmäßig Wartungsarbeiten durchgeführt werden. Hierzu steht ein tägliches Wartungsfenster zwischen 03:00 Uhr und 06:00 Uhr zur Verfügung.

KAMP informiert den Antragsteller über geplante Wartungsarbeiten mit einem Vorlauf von mindestens 72 Stunden. Der Antragsteller hat die Möglichkeit, dem geplanten Zeitfenster für die Wartung innerhalb von 48 Stunden aus wichtigen Gründen zu widersprechen. Erfolgt kein Widerspruch, gilt dies als Zustimmung. Das Widerspruchsrecht des Antragstellers gilt nicht im Not- oder Havariefall des KAMP-Dienstes, der eine umgehende Handlung durch KAMP zur Wiederherstellung der Effizienz bedarf. Der Antragsteller ist verpflichtet, die Teilnehmer der angeschlossenen Netzinfrastruktur im Falle einer Wartungsaktivität zu informieren. KAMP protokolliert alle Wartungsaktivitäten umfassend und überlässt die Protokolle dem Antragsteller auf Anforderung zur Einsicht. Auf Wunsch des Antragstellers sind auch von ihm beauftragte Personen berechtigt diese Protokolle zu prüfen.

10. Support-Service

Für Supportanfragen, die die Dienste und Netzinfrastrukturen der KV betreffen, ist die KV zu kontaktieren. Bei technischen Supportanfragen zur KAMP Dienstleistung kann sich der Antragsteller direkt mit KAMP über Telefon, Fax und Internetkontaktformular in Verbindung setzen. Der Antragsteller ist verpflichtet, zur Legitimation bei der Kontaktaufnahme seine Kundennummer oder Support-ID zu nennen.

Unter der Telefonnummer 0208.89402-61 ist der direkte Kontakt zu einem Ansprechpartner des KAMP-Supportteams während der Geschäftszeiten Mo. bis Fr. von 8:00 Uhr bis 18:00 Uhr möglich. Die Reaktionszeit bei Anfragen beträgt an Werktagen 2 Stunden und an Wochenenden/Feiertagen nächster Werktag/8:00 Uhr plus 2 Stunden. Von KAMP werden hierfür keine eigenen Servicegebühren erhoben. Der 24 h Online-Support kann jederzeit über das Kontaktformular auf der KAMP-Website https://www.kamp.de erfolgen.

Die Hardware, die der Antragsteller von KAMP für den Dienst KV-SafeNet zur Verfügung gestellt bekommt, ist für die Fernwartung vorkonfiguriert. Im Falle einer Internetverbindung, die nicht durch KAMP gestellt wird, muss die KAMP SafeBox über eine öffentliche IP-Adresse der Internetverbindung des Antragstellers für KAMP erreichbar sein. Dieser Remotezugriff für Wartungsarbeiten oder Störungsbeseitigungen kann auf ausdrücklichen und schriftlichen Wunsch des Antragstellers deaktiviert werden. Eine Störanalyse und oder Störbeseitigung wird in einem solchen Fall zeit- und kostenintensiver. Technischer Support vor Ort verursacht ebenfalls zusätzliche Kosten, die unter Punkt 11 „Nutzungsentgelte und Servicekosten“ einzusehen sind. Sollte ein Austausch der KAMP SafeBox notwendig werden, trägt KAMP die Kosten für das Ersatzgerät und den Versand.

11. Bestimmungen laut Richtlinie KV-SafeNet

Voraussetzung für die Nutzung von KV-SafeNet ist ein vorhandener Teilnehmer-PC mit geeigneter Software. Bei technischen Problemen, die durch KAMP verursacht wurden, verpflichtet sich KAMP gegenüber dem Antragsteller diese innerhalb der Wiederherstellungszeit zu beheben. Die Wiederherstellungszeit beträgt von Montag bis Freitag eine Zeitspanne von 24 Stunden ab Eingang der Störungsmeldung, an Wochenenden und Feiertagen nächster Arbeitstag 8:00 Uhr plus 24 Stunden. Mit Überschreiten der Wiederherstellungszeit verpflichtet sich KAMP zur Zahlung einer Vertragsstrafe von 100,00 Euro je weiteren angefangenen Kalendertag. Die Summe der Vertragsstrafen ist auf 1.000,00 Euro pro Jahr begrenzt. Diese Vertragsstrafe befreit KAMP nicht von Regressansprüchen seitens des Antragstellers für Schäden, die diesem durch einen Verstoß von KAMP gegen die Richtlinie KV-SafeNet entstanden sind.

Es ist dem Antragsteller untersagt, den KV-Backbone zur internen Vernetzung mit weiteren Netzinfrastrukturen anderer Organisationen zu nutzen.

Die Vertragspartner räumen der KV/KBV das Recht ein, bei Missbrauch der Anbindung des Antragstellers oder bei Missbrauch dieser Anbindung durch einzelne Teilnehmer die Anbindung des Netzes oder einzelner Teilnehmer jederzeit zu unterbrechen bzw. durch KAMP unterbrechen zu lassen, um Schaden an Daten, Anwendungen oder angeschlossenen Systemen zu vermeiden.

Der Antragsteller der anzuschließenden Netzinfrastruktur und KAMP liefern im Falle eines Missbrauchs auf Anforderung die entsprechenden Verbindungs- und Protokolldaten an die KV/KBV.

Die KBV/KV übernimmt keinerlei Haftung für die Verfügbarkeit und Sicherheit des Zugangsnetzes von KAMP. Die KBV/KV übernimmt keinerlei Haftung für die Verfügbarkeit und Sicherheit der Netzinfrastruktur des Antragstellers.

Der Antragsteller besitzt ein Kontrollrecht hinsichtlich der fortlaufenden Einhaltung der Richtlinie KV-SafeNet, welches die KBV für ihn ausüben kann.

12. Nutzungsentgelte und Servicekosten

Die vom Antragsteller zu zahlende Vergütung setzt sich aus Einmalzahlungen und monatlichen Entgelten zusammen. Alle Preise sind Entgelte in Euro inklusiv gesetzlicher Mehrwertsteuer. Diese gliedern sich wie folgt:

- einmalige Setup-Pauschale pro KAMP SafeBox: 177,31 Euro
- einmalige Setup-Pauschale für Teilnehmerzugangsdaten (Teilnehmerkennung und Passwort) pro Teilnehmer: 29,75 Euro
- monatliches Entgelt pro KAMP SafeBox: 41,65 Euro
- monatliches Entgelt pro Teilnehmerkennung: 4,76 Euro

Die monatlichen Entgelte sind im Voraus fällig.

Folgende Servicekosten können ggf. entstehen:

- Die Setup-Pauschale für zusätzliche Teilnehmerzugangsdaten, nach erstmaliger Teilnehmer-Initialeinrichtung, beträgt pro Teilnehmer 62,48 Euro.
- Die erneute Zusendung von Teilnehmerzugangsdaten bei postalischen Rückläufern beträgt pro Teilnehmer 29,75 Euro.
- Die Pauschale im Falle einer Neuzusendung eines Teilnehmerpasswortes beträgt 62,48 Euro.
- Remote-Support: Technischer Support für Fernwartung wird mit 41,65 Euro je angefangene 15 Minuten berechnet.
- Vor-Ort-Tages-Service-Pauschale: Wenn kein Fernwartungszugriff per Remotezugang seitens des Antragstellers gewünscht und ein Vor-Ort-Tages-Service beantragt ist, wird dieser mit pauschal 1130,50 Euro berechnet.

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Merkblatt

Pflichten des Betreibers der anzuschließenden Netzinfrastruktur und der darin befindlichen Teilnehmer

Der Antragsteller benennt die Teilnehmer, die mit den KV-Diensten kommunizieren sollen. KAMP ermöglicht den Teilnehmern den Zugang zum Sicheren Netz der KVen. Die KVen und KBV haben das Recht zur Kontrolle der Teilnehmer und können diese auch nachträglich – zum Beispiel im Falle eines Missbrauchs – ablehnen.

Nur erfolgreich authentisierte Teilnehmer erhalten Zugang zum Sicheren Netz der KVen. Jeder berechtigte Teilnehmer erhält eine persönliche Kennung, die nicht an eine andere Person weitergegeben werden darf.

Der Antragsteller ist insbesondere in den Bereichen PC-Sicherheit, Netzinfrastruktur und organisatorische Maßnahmen zu folgenden Regelungen verpflichtet:

PC-Sicherheit

Die PC-Arbeitsplätze, von denen aus die Teilnehmer Zugang zum Sicheren Netz der KVen erhalten können, sind folgendermaßen durch den Antragsteller der anzubindenden Netzinfrastruktur bereitzustellen bzw. zu konfigurieren:

- Der PC-Arbeitsplatz soll dem aktuellen Stand der Technik entsprechen und insbesondere aktuelle Versionen von Betriebssystemen, Anti-viren-Software, Anti-Malware und Firewall enthalten und entsprechend sicher konfiguriert sein.
- Die Arbeit an dem PC-Arbeitsplatz erfordert eine Anmeldung des Teilnehmers am PC, der Zugriff von unbefugten Personen auf den PC-Arbeitsplatz ist durch ein Benutzer- und Rollenkonzept zu verhindern.
- Grundsätzliche Administrationsrichtlinien insbesondere im Bereich der Benutzerberechtigungen für die PC-Arbeitsplätze sind einzuhalten, entsprechend der BSI Maßnahme M 2.382 (Aufteilung der Administrationstätigkeiten).
- Bei Inaktivität wird eine automatische Sperre des PC-Arbeitsplatzes mit anschließend erforderlicher Anmeldung zum Aufheben der Sperre vorgenommen.
- Der PC-Arbeitsplatz darf keine direkte Verbindung mit dem Internet haben. Eine Verbindung des PC-Arbeitsplatzes mit dem Internet über die Netzinfrastruktur des Antragstellers ist erlaubt.
- Benutzerrechte während des Parallelbetriebs müssen auf die nötigsten Dienste und Berechtigungen reduziert werden. Der Betrieb mit Administratorenrechten ist nur bei administrativen Tätigkeiten zulässig.
- Bei der Einstellung der browserinternen Sicherheitsstufen ist die höchstmögliche Sicherheit zu wählen. Es dürfen nur die aktiven Inhalte (Web-Scripting, PlugIns) zugelassen werden, die für den Betrieb zwingend notwendig sind. Die Einschränkung des Zugriffs auf die absolut notwendigen Seiten bietet einen hohen Schutz und kann organisatorisch oder technisch umgesetzt werden.
- Generell ist jeder an einem Netzwerk angeschlossene Computer mittels einer Desktop-Firewall vor unerlaubten Zugriffen zu schützen. Die Firewall-Regeln sind so restriktiv zu konfigurieren, dass nur die für den Betrieb zwingend notwendigen Verbindungen möglich sind.
- Die Firewall im KV-SafeNet-Router ersetzt nicht die lokalen Desktop-Firewalls.
- Die Räumlichkeiten des PC-Arbeitsplatzes müssen so gestaltet sein, dass unbefugte Personen keinen Zugriff auf den Arbeitsplatz erlangen können.

Netzinfrastruktur

Für den Datenschutz und die Datensicherheit in der angeschlossenen Netzinfrastruktur ist der Antragsteller der angeschlossenen Netzinfrastruktur voll verantwortlich.

In der angeschlossenen Netzinfrastruktur empfiehlt es sich, folgende Maßnahmen umzusetzen:

- 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
- Benutzung aller vorhandenen und rechtmäßigen Protokollmechanismen

Der Antragsteller hat technisch und organisatorisch sicherzustellen, dass ausschließlich Personen aus der Organisation bzw. Institution des Antragstellers Zugang zur KAMP SafeBox erlangen können. Zu diesem Zweck ist die KAMP SafeBox gegen unbefugten Zugang zu sichern, z.B. durch Aufbewahrung in einem sicheren Serverraum des Antragstellers.

Der Antragsteller ist verpflichtet,

- die KAMP SafeBox nur durch KAMP administrieren und betreiben zu lassen
- die KAMP SafeBox nicht an Dritte weiterzugeben
- Eingriffe in den Netzbetrieb von KAMP zu unterlassen
- bei einer Störungsanalyse und Störungsbeseitigung aktiv mitzuwirken
- Personen außerhalb der Organisation z. B. aus anderen angeschlossenen Netzinfrastrukturen den Zugang zur KAMP SafeBox zu verwehren. Das erfolgt mittels einer Zugriffssteuerungsliste (ACL Access Control List) auf der KAMP SafeBox. Der Antragsteller benennt KAMP hierfür die erlaubten Netzwerke bzw. Netzbereiche. Die Regeln richtet KAMP entsprechend in der SafeBox ein.

Organisatorische Maßnahmen

Der Antragsteller muss die Teilnehmer über folgende Pflichten informieren:

- Die Regelungen der BSI Maßnahme M 2.373 (Der aufgeräumte Arbeitsplatz) sind einzuhalten.
- Bei Verlassen des PC-Arbeitsplatzes muss sich der Teilnehmer abmelden.
- Der Teilnehmer darf die ihm zugewiesene persönliche Kennung keinesfalls an andere Personen weitergeben.
- Der Teilnehmer darf ausschließlich seine eigene persönliche Kennung für den Zugang zum Sicheren Netz der KVen benutzen.

Bei Verstößen oder Missbrauch der Betreiberpflichten haftet der Antragsteller.

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

Kassenärztliche Bundesvereinigung

Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Merkblatt Sicherheitsanforderungen KV-SafeNet-Arbeitsplätze

[KBV_SNK_MBEX_Sicherheit_Arbeitsplätze]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

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

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.1	31.10.2011	KBV	Dokumentenlenkung, und redaktionelle Anpassungen		
1.0	06.03.2009	KBV	Initiales Dokument		

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.

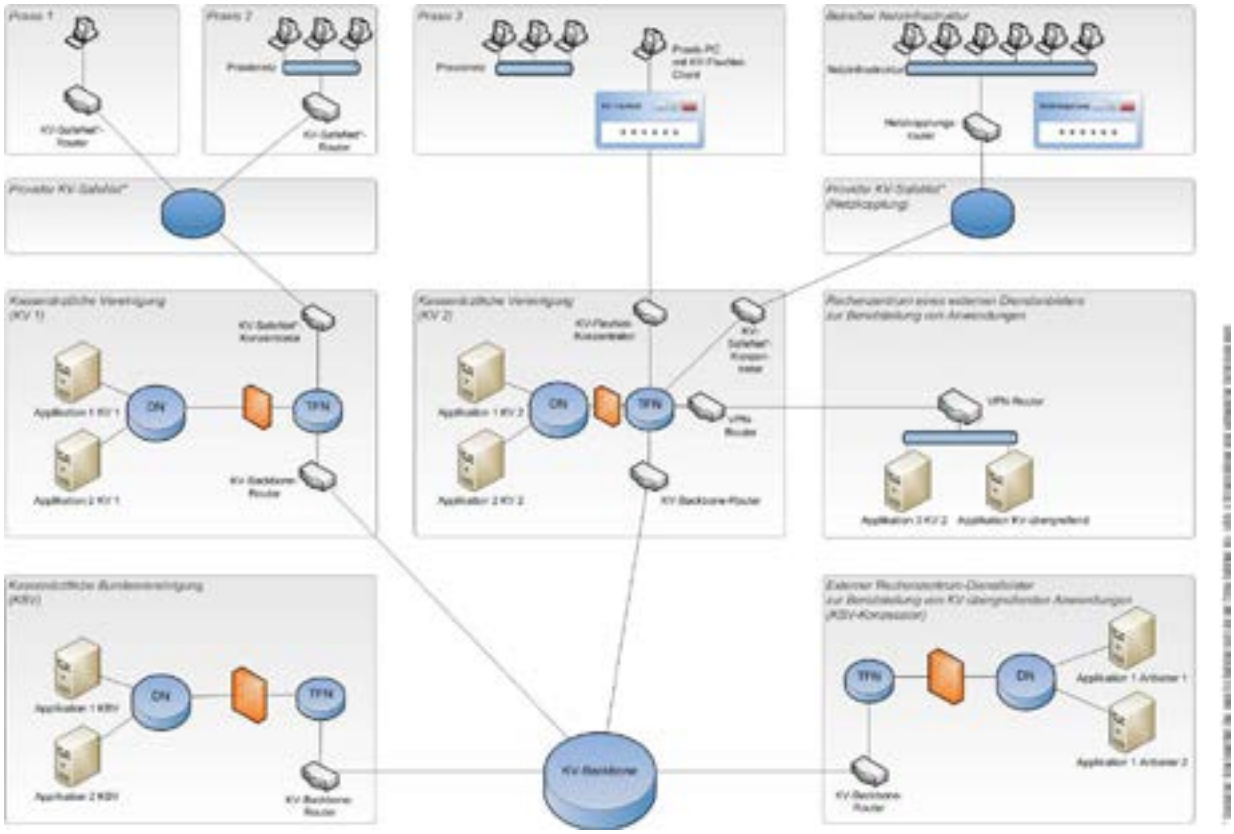

Abbildung 1: Beispielhafte Netztopologie

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

Durch Nutzung von Onlinediensten außerhalb des KV-SafeNet-Angebots, wie z.B. das Internet, werden die PC-Arbeitsplätze im internen Praxisnetz einer nicht zu unterschätzenden Gefahr durch Angriffe ausgesetzt. Diese Gefahr muss durch konsequenten und verantwortungsvollen Einsatz organisatorischer und technischer Sicherungsmaßnahmen minimiert werden.

Die vorhandenen Patientendaten haben einen besonderen Schutzbedarf, wie er auch durch die allgemein bekannte ärztliche Schweigepflicht ausgedrückt wird. Die eingesetzten Sicherungsmechanismen sind an den besonderen Schutzbedarf anzupassen.

Der Arzt trägt die Verantwortung für Sicherheit seiner Praxis-IT und für den Schutz der Patientendaten. Ziel dieses Dokumentes ist es in diesem Zusammenhang, Empfehlungen und Vorgaben für die sichere Nutzung des Internets als Mehrwertdienst der KV-SafeNet-Anbindung im Praxisumfeld zu geben.

1.3 Klassifizierung und Adressaten des Dokuments

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

* 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

Im Allgemeinen ist ausdrücklich auf die Bekanntmachung im Deutschen Ärzteblatt (DÄB), Jg. 105, Heft 19 vom 9. Mai 2008 zum Thema „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“[2] hinzuweisen.

2.1 Sicherheitsmaßnahmen

Die Hinweise in diesem Abschnitt zeigen Maßnahmen, die ein Administrator zum Schutz von PCs vor unerlaubten Zugriff durchführen kann.

2.1.1 Beschränkung der Arbeit mit Administratorrechten

Benutzerrechte während des Parallelbetriebs müssen auf die nötigsten Dienste und Berechtigungen reduziert werden. Der Betrieb mit Administratorenrechten ist nur bei administrativen Tätigkeiten (siehe 2.1.2 Softwareaktualisierung) zulässig.

2.1.2 Softwareaktualisierung

Durch zeitnahe Installation von empfohlenen Programm-Updates, wodurch bekannt gewordene Sicherheitslücken der beteiligten Softwarekomponenten[3] geschlossen werden, ist dessen größtmöglicher Sicherheitszustand zu gewährleisten.

2.1.3 Einstellung von Webbrowsern

Bei der Einstellung der browserinternen Sicherheitsstufen ist die höchstmögliche Sicherheit zu wählen. Es dürfen nur die aktiven Inhalte (Web-Scripting, PlugIns) zugelassen werden, die für den Betrieb zwingend notwendig sind. Die Einschränkung des Zugriffs auf die absolut notwendigen Seiten bietet einen hohen Schutz und kann organisatorisch oder technisch umgesetzt werden.

2.2 Sicherheitssoftware

In diesem Abschnitt werden Softwarekomponenten beschrieben, wodurch PCs eines Netzwerkes vor unerlaubten Zugriffen und Angriffen geschützt werden können.

2.2.1 Einsatz von lokalen Firewalls

Generell ist jeder an einem Netzwerk angeschlossener Computer mittels einer Desktop-Firewall vor unerlaubten Zugriffen zu schützen. Die Firewall-Regeln sind so restriktiv zu konfigurieren, dass nur die für den Betrieb zwingend notwendigen Verbindungen möglich sind.

Die Firewall im KV-SafeNet-Router ersetzt nicht die lokalen Desktop-Firewalls.

[2] Dieser Beitrag ist auch im Internet unter der Adresse http://www.bundesaerztekammer.de/page.asp?his=0.7.47.6188 verfügbar.
[3] Hierzu zählen grundlegende Programme wie Betriebssystem, Internetbrowser und Client-Programme (z.B. E-Mail-Client) sowie die zur Systemsicherung eingesetzten Programme wie Firewall, Malware-Schutzprogramm usw.

2.2.2 Einsatz von Malware[4]-Schutzprogrammen

Der Einsatz von aktuellen und anerkannten Malware-Schutzprogrammen ist für alle Rechner im Praxisnetz anzuwenden.

2.2.3 Content-Security für Web-Scriptings[5]

Als konsequente Erweiterung des Schutzes vor Malware-Programmen ist auch die sichere Abwehr vor bösartigem Inhalt auf Internetseiten zu gewährleisten. Hier ist der Gefahrenquelle des Web-Scriptings durch geeignete Verfahren entgegen zu wirken.

2.3 Netzwerk

Dieser Abschnitt enthält Sicherheitsmaßnahmen für das PC-Netzwerk in der Praxis.

2.3.1 Zugriffe über einen dedizierten Internet-Rechner

Um das Gefährdungspotential so niedrig wie möglich zu halten, dürfen Rechner mit Patientendaten generell nur dann mit dem Haus Netz verbunden sein, wenn dieses zwingend nötig ist (Minimierungsprinzip).

Die Verwendung eines dedizierten Internet-Rechners für die Nutzung der Mehrwertdienste reduziert die Systemverletzlichkeit des Hausnetzes und der angeschlossenen Arbeitsplätze erheblich. Soweit der produktive Betrieb der Praxissoftware keinen direkten Internetzugang benötigt, ist der Einsatz eines gesonderten Internet-Rechners unbedingt angeraten.

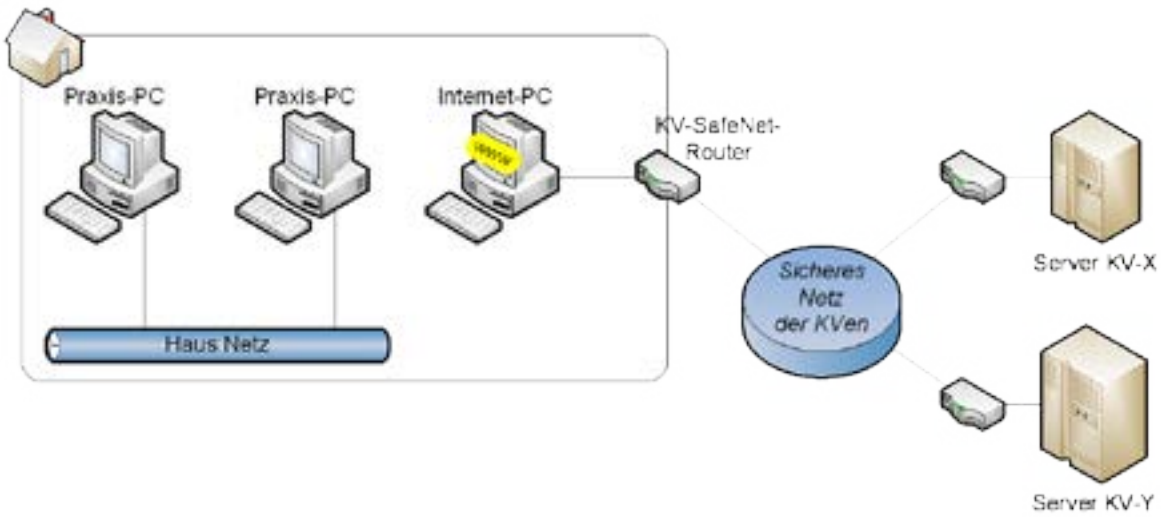

Abbildung 2: Einsatz eines gesonderten Internet-PCs

2.3.2 Zugriffe über eigenen Proxy

Wenn die Verwendung eines gesonderten Internet-Rechners nicht möglich ist, empfiehlt sich der Einsatz eines Proxys für den Datenaustausch mit dem Internet. Ein Proxy arbeitet als Vermittler, der Anfragen auf dem Haus Netz entgegennimmt, um diese dann stellvertretend ans Internet weiterzuleiten und die Rückmeldungen wieder auf dem Hausnetz zurückzugeben.

[4] **Maleware** ist der Oberbegriff für schädliche und unerwünschte Computerprogramme, welche die Funktion und Sicherheit des Rechnersystems negativ beeinflussen. Hierzu zählen Computerviren, Trojaner, Würmer, Spyware, Scareware, usw.
[5] Mit **Web-Scripting** wird die Programmiertechnik dynamischer Web-Seiten mit JavaScript, Dynamic HTML, ColdFusion, Flash usw. bezeichnet.

Somit wird die Bedrohung vermindert, dass die PCs des Praxisnetzes angegriffen werden können.

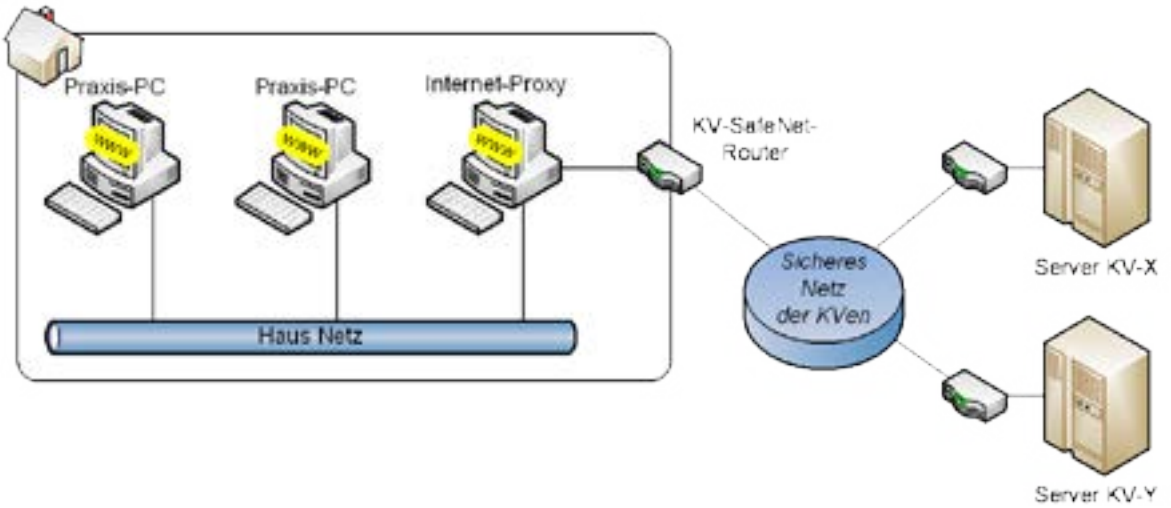

Abbildung 3: Einsatz eines Internet-Proxy

2.3.3 Keine Nebenzugänge zum Internet

Außer dem KV-SafeNet-Zugang dürfen keine weiteren Verbindungen zum Internet bestehen, da sonst die Sicherheit des gesamten Praxis-EDV-Systems nicht mehr gewährleistet ist. Besonders von Rechnern mit Funknetzanschlüssen (sog. Wireless LAN oder WLAN) geht hier eine besondere Gefahr aus. Blockieren Sie sämtliche Funknetzverbindungen mit Gegenstellen außerhalb des PC-Netzes Ihrer Praxis.

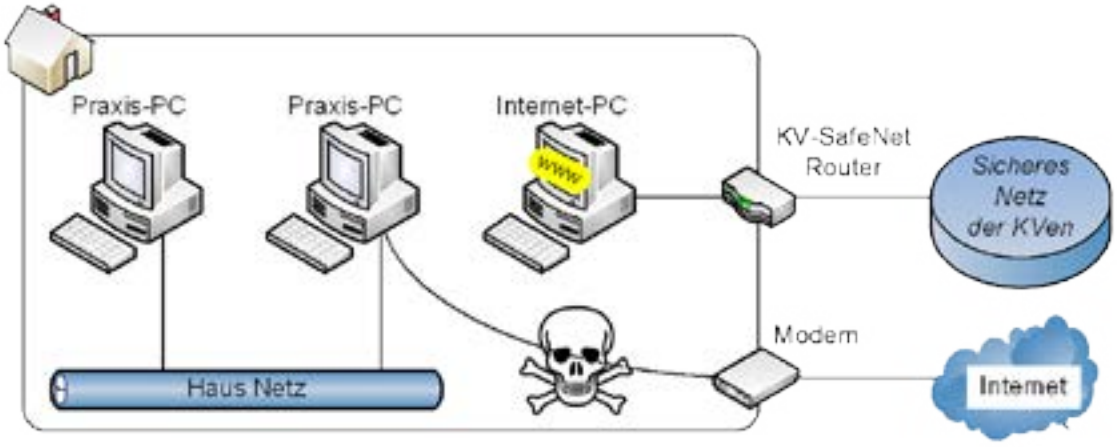

Abbildung 4: Unsichere Nutzung des Internets

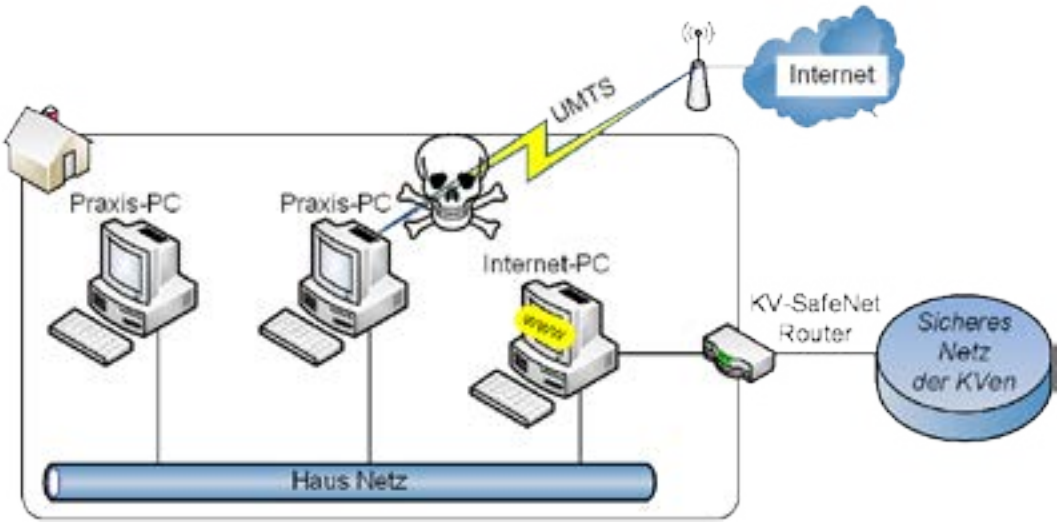

Abbildung 5: Unsichere Verwendung des Internets via UMTS

2.4 Anforderungen an KV-SafeNet-Provider

Die Anbieter (Provider) von KV-SafeNet-Zugängen sind prinzipiell auch in der Lage, Sie als angeschlossenen Teilnehmer beim Schutz vor Angriffen aus dem Internet zu unterstützen. Hier unterscheiden sich jedoch die Leistungen je nach Vertragsart und Geschäftsbeziehung.

2.4.1 Proxy-, Gateway- und Sicherheitssysteme des Providers

Um das Gefährdungspotential bereits im Vorfeld von den angeschlossenen Praxen fernzuhalten, empfehlen wir, die Teilnehmer ausschließlich über ein gesichertes und vom Anbieter administriertes Transfernetzwerk[6] ans Internet anzuschließen.

Der Übergang zwischen Transfernetzwerk und Internet ist durch geeignete Proxy-, Gateway- und Sicherheitssysteme vor Zugriffen aus dem Internet zu schützen. Der Proxy befindet sich in einer sog. Demilitarisierten Zone (DMZ) wodurch ein direkter Durchgriff des Internets auf das Providernetz verhindert wird.

Dieser Service erhöht die Sicherheit des Praxisnetzes vor unerlaubten Zugriffen erheblich, da sich das Sicherheitssystem der Praxis sowie das Sicherheitssystem des Providers ergänzen.

[6] Das **Transfernetzwerk** besteht lediglich aus Teilnehmern des Anbieters und ist über ein Proxy-Gateway mit dem Internet verbunden.

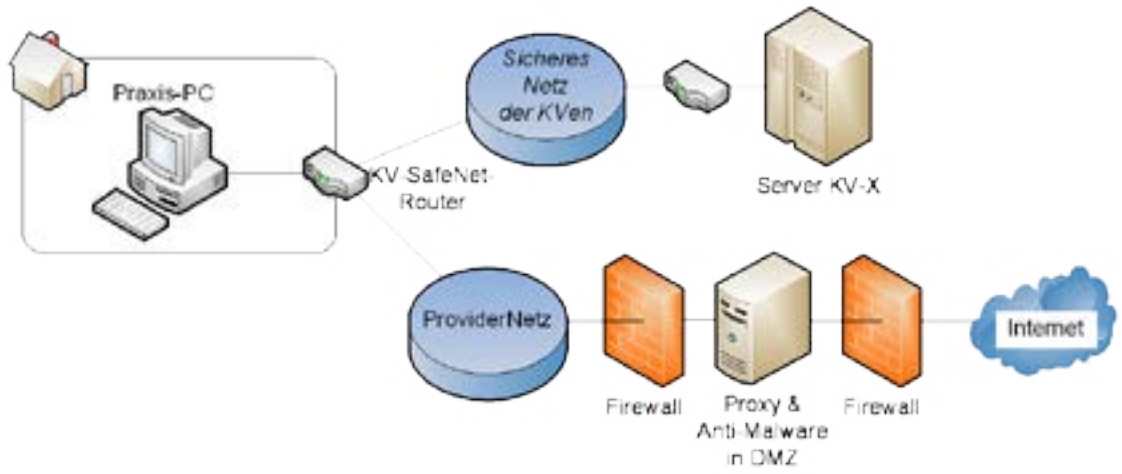

Abbildung 6: Einsatz einer DMZ im Providernetz

2.4.2 Sicherheitsstandards für Provider

Achten Sie darauf, dass Ihr Provider die allgemeinen Hinweise aus dem IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) umsetzt.

Bei fahrlässiger Unterlassung der Sicherheitsmaßnahmen behalten sich die KVen und KBV vor, den Zugang des einzelnen Teilnehmers oder sogar des Anbieters zu sperren.

2.5 Sicherheitsszenarien

Je nach Kommunikationspartner werden unterschiedliche Sicherheitsszenarien definiert.

2.5.1 Szenario 1

Der Datenaustausch erfolgt ausschließlich innerhalb des *Sicheren Netzes der KVen*. In diesem Szenario kann von einem sehr geringen Angriffspotential ausgegangen werden, zumal auch alle Teilnehmer bekannt sind.

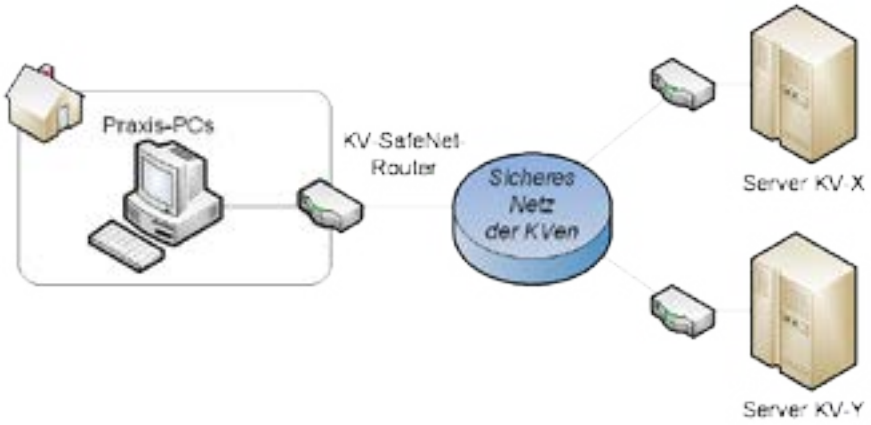

Abbildung 7: Sicherheitsszenario 1

2.5.2 Szenario 2

Der Datenaustausch erfolgt ausschließlich innerhalb des *Sicheren Netzes der KVen*. Hier werden Datendienste benutzt, die nicht durch die KVen kontrolliert werden, wie z.B. ein gemeinsamer Server eines Versorgungszentrums. In diesem Szenario kann von einem mäßigen Angriffspotential ausgegangen werden.

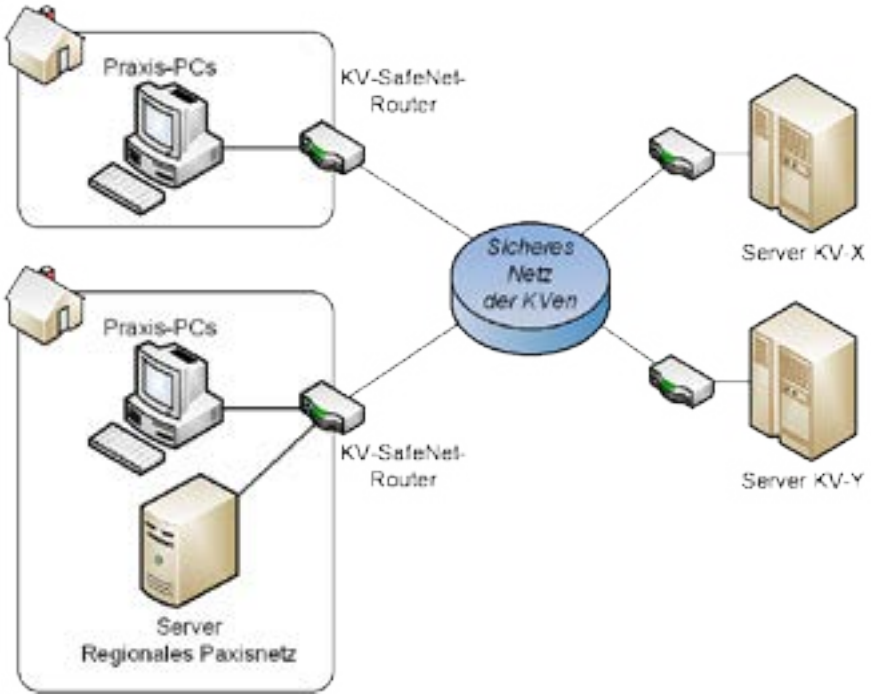

Abbildung 8: Sicherheitsszenario 2

2.5.3 Szenario 3

Der Datenaustausch erfolgt auch außerhalb des *Sicheren Netzes der KVen*. Hier werden auch Datendienste aus dem Internet benutzt, wie z.B. das Internet.

Da auf Seiten des Internets ein sehr großes Angriffspotential liegt, muss in diesem Szenario von einem großen Angriffspotential ausgegangen werden. Die Sicherheitsmaßnahmen des Providers können die Gefahr vor Angriffen aus dem Internet jedoch reduzieren.

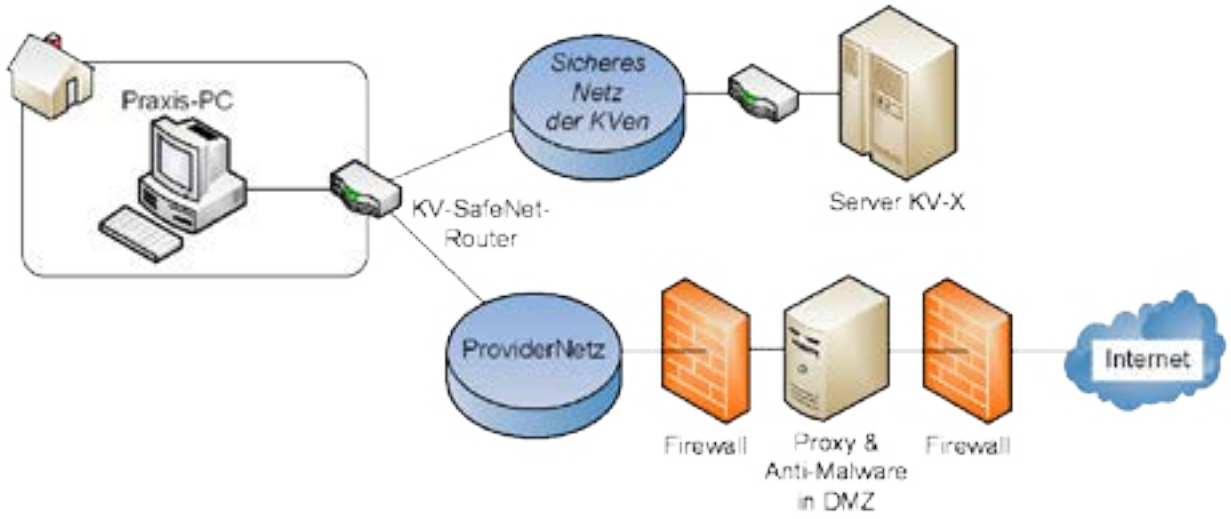

Abbildung 9: Sicherheitsszenario 3

2.5.4 Szenario 4

Der Datenaustausch erfolgt wie in Szenario 3 außerhalb des *Sicheren Netzes der KVen*. Es existiert jedoch kein abgeschirmtes Providernetz, sondern ein direkter Anschluss des KV-SafeNet-Routers an das Internet.

Da auf Seiten des Internets ein sehr großes Angriffspotential liegt, muss in diesem Szenario ebenfalls von einem großen Angriffspotential ausgegangen werden. Sämtliche Sicherheitsmaßnahmen vor unerlaubten Zugriffen auf das Praxisnetz sind auf dem KV-SafeNet-Router zu konfigurieren.

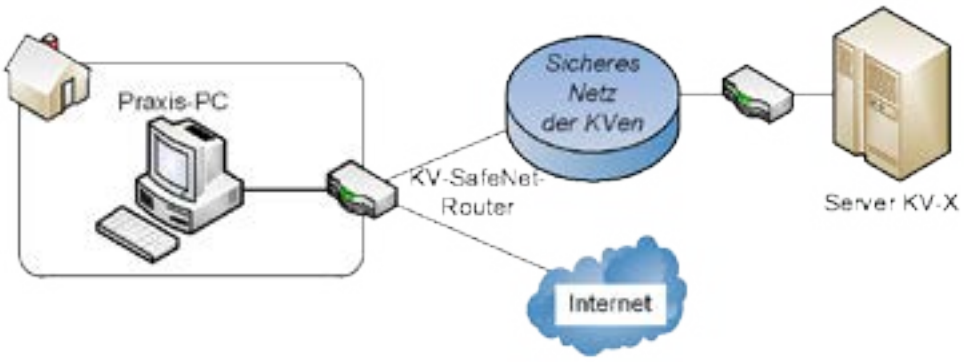

Abbildung 10: Sicherheitsszenario 4

3 Glossar

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

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*.
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.

Allgemeine Geschäftsbedingungen

der KAMP Netzwerkdienste GmbH, Vestische Straße 89-91, 46117 Oberhausen,
im Folgenden „KAMP“ genannt.

§ 1 Geltungsbereich; Definitionen

1.1 Diese Allgemeinen Geschäftsbedingungen (im Folgenden: AGB) gelten für Verträge zwischen KAMP und dem Vertragspartner. Vertragspartner im Sinn dieser AGB sind sowohl Verbraucher als auch Unternehmer. Verbraucher im Sinn dieser AGB ist jede natürliche Person, die ein Rechtsgeschäft mit KAMP zu einem Zweck abschließt, der weder ihrer gewerblichen noch ihrer selbstständigen beruflichen Tätigkeit zugerechnet werden kann. Unternehmer im Sinn dieser AGB ist eine natürliche oder juristische Person oder rechtsfähige Personengesellschaft, die bei Abschluss eines Rechtsgeschäfts mit KAMP in Ausübung ihrer gewerblichen oder selbstständigen beruflichen Tätigkeit handelt.

1.2 Diese AGB gelten ausschließlich. Abweichende, entgegenstehende oder ergänzende AGB werden nicht Vertragsbestandteil. Dem formularmäßigen Hinweis auf Geschäftsbedingungen des Vertragspartners wird widersprochen.

§ 2 Leistungen von KAMP

2.1 Das Leistungsspektrum wird zwischen KAMP und dem Vertragspartner jeweils im Hauptvertrag vereinbart. Die Regelung des Hauptvertrags haben Vorrang vor diesen AGB.

2.2 Soweit nicht ausdrücklich anders vereinbart, darf KAMP die ihr obliegenden Leistungen von ihren Mitarbeitern oder Dritten erbringen lassen.

2.3 Der Vertragspartner wird rechtzeitig alle in seinem Einflussbereich liegenden Voraussetzungen zur Ausführung der Leistung durch KAMP treffen.

§ 3 Vergütung, Zahlung, Aufrechnung und Preise

3.1 Monatliche Entgelte sind monatlich ab Vertragsbeginn im Voraus zu zahlen. Beginnt die Vertragslaufzeit im Laufe eines Kalendermonats oder endet sie im Laufe eines Kalendermonats, ist das Entgelt für jeden Tag der Vertragslaufzeit dergestalt zu berechnen, dass das monatliche Entgelt durch die Anzahl der Tage des betreffenden Kalendermonats geteilt wird.

3.2 Leistungen, für die nur ein einmaliges Entgelt geschuldet ist, sind innerhalb von 14 Kalendertagen nach deren Erbringung zu vergüten.

3.3 Die Zahlung von Rechnungen erfolgt per SEPA-Basis-Lastschriftverfahren. Wenn das Konto die erforderliche Deckung nicht aufweist, besteht seitens des kontoführenden Kreditinstituts keine Verpflichtung zur Einlösung.

3.4 Der Vertragspartner verpflichtet sich, die vereinbarten Preise fristgerecht zu zahlen. Für jede nicht einlösbare bzw. zurückgereichte Lastschrift hat der Vertragspartner KAMP die entstandenen Kosten in dem Umfang zu erstatten, wie er das kostenauslösende Ereignis zu vertreten hat.

3.5 Der Vertragspartner ist zur Aufrechnung nur berechtigt, sofern und soweit seine Gegenansprüche rechtskräftig festgestellt, unbestritten oder von uns anerkannt sind.

§ 4 Eigentumsvorbehalt

4.1 Alle dem Vertragspartner im Rahmen des Vertrags überlassene Hardware (z.B. Router, Modem, Server) bleibt Eigentum von KAMP. Sie sind KAMP innerhalb von 14 Kalendertagen nach Vertragsbeendigung zurück zu geben.

4.2 KAMP ist nicht dazu verpflichtet, dem Vertragspartner Hardware zur Verfügung zu stellen oder zu beschaffen.

§ 5 Haftungsbeschränkung

5.1 KAMP schließt die Haftung für Schäden, die durch einfache Fahrlässigkeit verursacht worden sind, aus, sofern diese nicht aus der Verletzung vertragswesentlicher Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf (im Folgenden: Kardinalpflichten), resultieren und nicht, Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Ansprüche nach dem Produkthaftungsgesetz betroffen sind. Gleiches gilt für Pflichtverletzungen von Erfüllungsgehilfen von KAMP.

5.2 Bei der Verletzung von Kardinalpflichten ist die Haftung in Fällen einfacher Fahrlässigkeit auf die Schäden beschränkt, die in typischer Weise mit dem Vertrag verbunden und vorhersehbar sind.

§ 6 Freistellung

6.1 Der Vertragspartner verpflichtet sich, keine Informationsangebote mit rechts- oder sittenwidrigen Inhalten anzubieten, insbesondere keine Informationen zu übermitteln, die i. S. d. §§ 130, 130a und 131 StGB zum Rassenhass aufstacheln, Gewalt verherrlichen oder verharmlosen, sexuell anstößig sind, i. S. d. § 184 StGB pornographisch sind, den Krieg verherrlichen, geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden oder in ihrem Wohl zu beeinträchtigen und/oder auf Angebote mit solchen Inhalten hinzuweisen.

6.2 Der Vertragspartner verpflichtet sich im Fall eines Verstoßes gegen die zuvor genannten Verpflichtungen KAMP von allen Ansprüchen, die Dritte wegen des Angebots des Vertragspartners gegen KAMP geltend machen, freizustellen sowie KAMP unverzüglich jede Unterstützung zur Verteidigung gegen diesen Anspruch zu gewähren.

6.3 Die Verpflichtung zur Freistellung nach Ziffer 8.2 gilt auch in Bezug auf Ansprüche, die Dritte wegen einer angeblichen Rechtsverletzung durch den Vertragspartner, insbesondere einer Verletzung des Urheber-, Datenschutz-, Wettbewerbsrechts und/oder der Verletzung gewerblicher Schutzrechte, gegen KAMP geltend machen.

§ 7 Kündigung des Vertrages

7.1 Falls keine Vertragslaufzeit vereinbart wurde, kann das Vertragsverhältnis von beiden Vertragsparteien mit einer Frist von zwei Wochen zum Monatsende gekündigt werden. Ist eine Vertragslaufzeit vereinbart, so ist vor Ablauf der Vertragslaufzeit die ordentliche Kündigung ausgeschlossen.

7.2 Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt vorbehalten. Einen wichtigen Grund stellt es insbesondere dar, wenn der Vertragspartner (a) mit zwei aufeinanderfolgenden Zahlungen oder (b) in einem Zeitraum, der sich über mehr als zwei Monate erstreckt, mit der Zahlung in Höhe eines Betrags, der die Summe von zwei monatlichen Zahlungen erreicht oder übersteigt, in Verzug gerät oder (c) das Insolvenzverfahren über das Vermögen einer Partei eröffnet ist oder wenn eine Partei einen Eigenantrag auf Eröffnung des Insolvenzverfahrens gestellt hat.

7.3 Kündigungen haben in Textform zu erfolgen.

7.4 Ist ein Vertrag von KAMP aus wichtigem Grund fristlos gekündigt worden, nachdem der Vertragspartner verpflichtet ist, monatliche Zahlungen zu leisten, ist KAMP berechtigt, pauschalierten Schadensersatz zu verlangen. Die Höhe beträgt 50% der monatlich geschuldeten Vergütung, die bis zum Ende der Vertragslaufzeit zu zahlen gewesen wäre, jedoch nicht mehr als 50% der geschuldeten Vergütung für drei Jahre. Das gilt nicht, wenn der Vertragspartner nachweist, dass kein Schaden entstanden ist oder der tatsächlich entstandene Schaden wesentlich niedriger als die Pauschale ist. Für den Fall, dass KAMP einen höheren Schaden nachweisen kann, so ist dieser höhere Schaden zu ersetzen.

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de

§ 8 Weitere Pflichten und Haftung des Vertragspartnern

Der Vertragspartner ist insbesondere verpflichtet,

8.1 Gefährdungen und Behinderungen anderer Netzteilnehmer, die von seinem System (z.B. durch Viren und Trojaner) ausgehen, unverzüglich zu beseitigen. Für den Fall, dass der Vertragspartner dem nicht nachkommt, ist KAMP aus Sicherheitsgründen berechtigt, die Internetverbindung bis zur Beseitigung der Gefährdung bzw. Behinderung zu deaktivieren.

8.2 sicherzustellen, dass die Ursache des Problems bei einer Störungsmeldung nicht sein eigener Service, seine eigenen Anlagen oder seine Hardwarekomponenten sind. Der Vertragspartner hat nach Abgabe einer Störungsmeldung an KAMP, die durch die Überprüfung der Einrichtungen entstandenen Aufwendungen zu ersetzen, wenn sich nach der Prüfung herausstellt, dass keine Störung der technischen Einrichtungen von KAMP vorlag, es sei denn, der Vertragspartner weist nach, dass die Ursache des Problems der Störungsmeldung auch nicht der eigene Service des Vertragspartners, seine eigenen Anlagen oder seine Hardwarekomponenten sind.

8.3 sicherzustellen, dass KAMP Zugang zu den entsprechenden Räumen des Vertragspartners erhält, um Installations-, Test-, Überwachungs-, Wartungs-, Reparatur und ähnliche Arbeiten vorzunehmen.

8.4 alle bei Verlust oder Beschädigung einer von KAMP ihm überlassenen Hardware (z.B. Router, Modem, Server) verbundenen Kosten zu tragen. Die Kosten für Equipment, welches der Vertragspartner aufgrund seiner Hardware oder Software benötigt, trägt der Vertragspartner.

8.5 Hardware von KAMP nicht zu verändern und/oder zu reparieren. Zudem ist der Vertragspartner nicht berechtigt, Hardware von KAMP zu entfernen oder an einen anderen Platz zu verbringen.

8.6 die elektrische Energie für die Installation, den Betrieb und die Instandhaltung einer von KAMP in den Räumen des Vertragspartners bereitgestellten IP-Anbindung einschließlich aller dort untergebrachten, für den ordnungsgemäßen Betrieb notwendigen Hardwarekomponenten, bereitzustellen und aufrecht zu erhalten. Der Stromanschluss sowie ein – unter Umständen notwendiger – Potenzialausgleich mit zugehöriger Erdung, wird/werden vom Vertragspartner auf dessen Kosten bereitgestellt.

8.7 die Anschalteinrichtung (z.B. DSL-Modem, Router) ständig betriebsbereit zu halten.

8.8 die „Acceptable Use Policy“ in der bei Vertragsschluss geltenden Version zu befolgen.

§ 9 Höhere Gewalt

Weder KAMP noch der Vertragspartner können gegen die jeweils andere Vertragspartei Ansprüche wegen eines von außen kommenden, nicht vorhersehbaren und auch bei Anwendung äußerster Sorgfalt nicht abwendbaren Ereignisses (Höhere Gewalt) geltend machen. Höhere Gewalt liegt insbesondere vor bei Unwetter, Erdbeben, Überschwemmungen, Brand, -nationalen Notständen, Versorgungsengpässen, Unruhen, Kriegen, Streiks, Aussperrungen und Ausfall von Telekommunikationsverbindungen.

§ 10 Sonstige Bedingungen

10.1 Der Vertragspartner kann die Rechte und Pflichten aus diesem Vertrag nur nach vorheriger schriftlicher Zustimmung durch KAMP auf einen Dritten übertragen.

10.2 Die Vorschriften des Produkthaftungsgesetzes bleiben unberührt.

§ 11 Änderung des Vertrags

11.1 KAMP ist berechtigt, diese Allgemeinen Geschäftsbedingungen mit einer Frist von 8 Wochen im Voraus zu ändern. Die jeweilige Änderung wird KAMP den Vertragspartner in Textform oder schriftlich bekannt geben. Gleichzeitig wird der Vertragspartner ausdrücklich darauf hingewiesen, dass die jeweilige Änderung Gegenstand des zwischen den Vertragsparteien bestehenden Vertrages wird, wenn der Vertragspartner dieser Änderung nicht innerhalb einer Frist von 8 Wochen ab Bekanntgabe der Änderung in Textform oder schriftlich widerspricht. Widerspricht der Kunde, hat jede Partei das Recht, den Vertrag mit der für eine ordentliche Kündigung geltenden Frist zu kündigen.

11.2 KAMP ist berechtigt, die Vertrags- und Leistungsbedingungen mit einer Frist von 8 Wochen im Voraus zu ändern, wenn die Änderung durch gesetzliche Änderungen und/oder Änderungen der Rechtsprechung und/oder Vorgaben der zuständigen Aufsichtsbehörde bedingt ist. Die jeweilige Änderung wird KAMP den Vertragspartner in Textform oder schriftlich bekannt geben. Gleichzeitig wird der Vertragspartner ausdrücklich darauf hingewiesen, dass die jeweilige Änderung Gegenstand des zwischen den Vertragsparteien bestehenden Vertrages wird, wenn der Vertragspartner dieser Änderung nicht innerhalb einer Frist von 8 Wochen ab Bekanntgabe der Änderung in Textform oder schriftlich widerspricht. Widerspricht der Kunde, hat jede Partei das Recht, den Vertrag mit der für eine ordentliche Kündigung geltenden Frist zu kündigen.

11.3 Die vorstehenden Regelungen dieses § 11 finden keine Anwendung auf einmalige Austauschverhältnisse (bspw. Kauf eines Produkts), sondern nur auf Dauerschuldverhältnisse.

§ 12 Schlussbestimmungen

12.1 Dieser Vertrag unterliegt deutschem Recht.

12.2 Soweit der Vertragspartner Kaufmann, juristische Person öffentlichen Rechts oder öffentliches Sondervermögen ist, ist Oberhausen Gerichtsstand. KAMP ist aber auch berechtigt, den Vertragspartner an seinem Wohn- oder Geschäftssitz zu verklagen.

KAMP Netzwerkdienste GmbH
Vestische Straße 89–91 | 46117 Oberhausen Kontakt Fon: +49 (0) 208.89 402-0 | Fax: +49 (0) 208.89 402-40 | Internet: www.kamp.de | E-Mail: info@kamp.de