Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Leitfaden Zertifizierung KV-SafeNet-Provider

[KBV_SNK_LFEX_Zert_KV-SafeNet]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.8
Datum:	31.01.2016
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.8	31.01.2016	KBV	Detaillierung und Schärfung der Vorgaben zur Dokumentation technischer Sicherheitsaspekte	Anpassung des Leitfadens an die Vorgaben der Richtlinie KV-SafeNet V3.2	Kap. 3.9 – 3.14
1.7	30.01.2013	KBV	3.3 Punkte zur Vertragslaufzeit, Zertifikatsgültigkeit an Richtlinie angepasst 3.8 Erläuterung zu (4) 3.11 Erweiterung und Verbesserung	Korrektur genauere Beschreibung der Anforderungen	13 17 19/20
1.6	31.10.2011	KBV	Anpassung an die Richtlinie KV-SafeNet 3.1 Vereinheitlichung der Begriffe und des Dokumentenlayouts	Einarbeitung von Maßnahmen zur kontinuierlichen Verbesserung des Datenschutzes	Alle
1.5 1.4	10.08.2010 02.06.2010	KBV	Prüfkosten	Anpassung nach Aufwandsanalyse	8
1.3	08.02.2010	KBV	Deckblatt und Verzeichnisse Generelle Überarbeitung	Corporate Identity Einarbeitung von Kommentaren	Alle
1.2	11.06.2009	KBV	2.2 Abbildung angepasst 3.1.1 Ergänzende Erklärung 3.1.2 Konformitätserklärung über die Einhaltung des Datenschutzes 3.1.3 Musterteilnehmervertrag unterteilt in KV-SafeNet und Mehrwertdienste 3.1.14 Erklärung über die Einbeziehung von Erfüllungsgehilfen 3.1.15 Sicherheitsbelehrung für den Teilnehmer 3.1.8 Supportkonzept 3.3 praktische Prüfung 4.1 Literaturverzeichnis	Aufnahme von Beschreibung Anpassung Anforderung Anpassung Anforderung redaktionelle Anpassung Aufnahme Rechtsvorschriften Datenschutz	11 12 12 15 17 26
1.1	06.03.2009	KBV	2.1.4 Kosten für Beratungsgespräch 2.2.2 Rezertifizierung 3 Erforderliche Unterlagen	Anpassung Rahmenrichtlinie	9 11
1.0			Erstellung des Dokuments		

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 Präambel

1.1 Das sichere Netz der KVen

Die Kassenärztliche Bundesvereinigung und die Kassenärztlichen Vereinigungen haben eine Online-Infrastruktur aufgebaut, die den hohen Anforderungen an Datenschutz und Datensicherheit Rechnung trägt und die u.a. für die Übermittlung von Patienten- und Honorardaten geeignet ist – das sichere Netz der KVen.

Informationssicherheit im sicheren Netz der KVen ist eines der wichtigsten Ziele aller Beteiligten. Von besonderer Bedeutung ist dabei der Schutz der Sozialdaten und weiterer personenbezogener Daten. Für diese und andere Informationen und Werte werden im Rahmen des Sicherheitsmanagements Schutzziele definiert. Im Mittelpunkt dabei stehen die Sicherung der Vertraulichkeit, die Gewährleistung der Integrität und die Aufrechterhaltung der Verfügbarkeit. Zur Einhaltung dieser Ziele trifft die KBV regulatorische Maßgaben in Form von Richtliniendokumenten und Zertifizierungen. Die Umsetzung obliegt allen Beteiligten.

Die Rechenzentren der Kassenärztlichen Vereinigungen (KVen) und der Kassenärztlichen Bundesvereinigung (KBV) sind hierzu über den KV-Backbone, einem logisch vom Internet getrennten Netzwerk, miteinander verbunden. Die KBV ist der Betreiber des KV-Backbones.

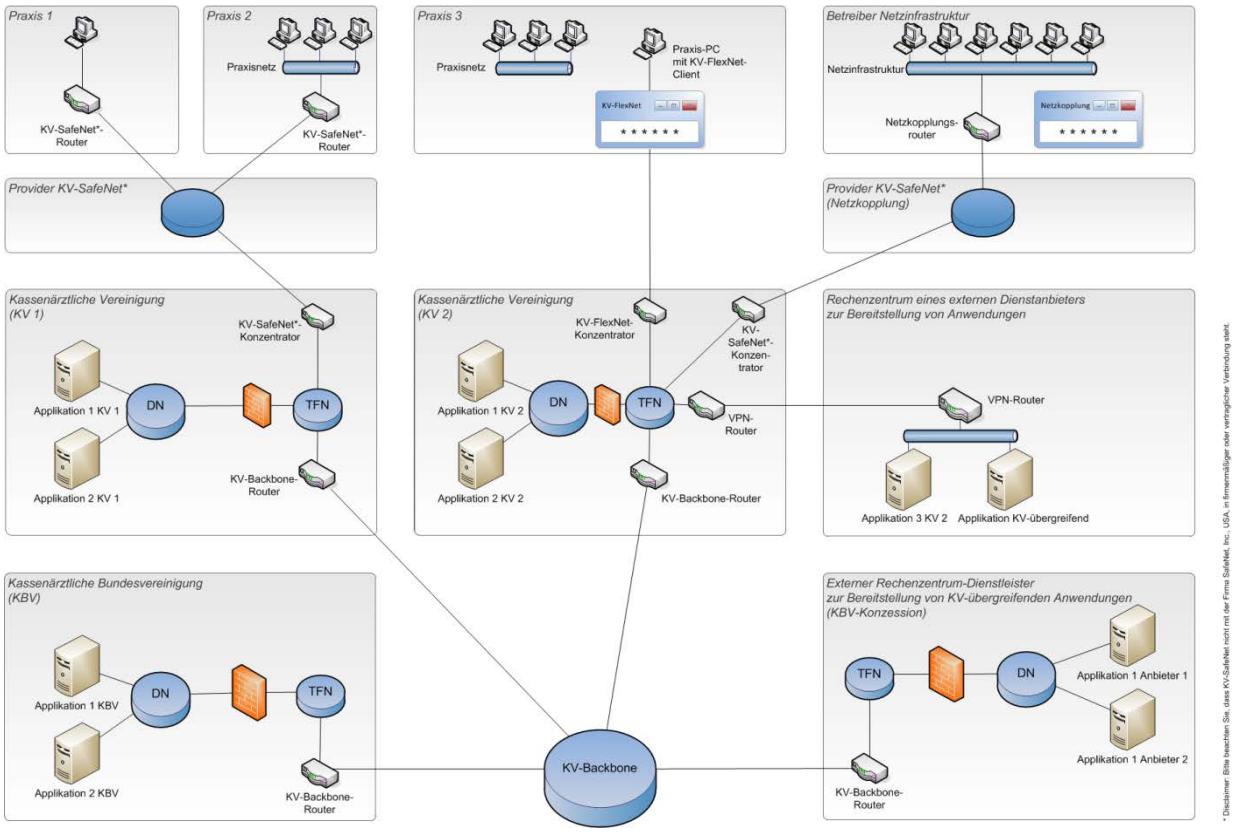

Abbildung 1: Beispielhafte Netztopologie

Teilnehmer am sicheren Netz der KVen sind die Mitglieder der Kassenärztlichen Vereinigungen, also Vertragsärzte und –psychotherapeuten oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des sicheren Netzes der KVen. Ihnen werden sichere Zugangswege zu den Diensten und Anwendungen bereitgestellt. Die Anbindung der Teilnehmer an das sichere Netz der KVen erfolgt mittels einer VPN-Verbindung. Es gibt hierbei zwei Mög-

lichkeiten der sicheren Anbindung, einerseits über das KV-SafeNet*, einem Hardware-VPN und andererseits über das KV-FlexNet[1] einem Software-VPN. Die Bereitstellung eines Zugangs über die Variante KV-FlexNet liegt in der Hoheit der jeweiligen KV. Beide Zugangsvarianten ermöglichen eine sichere Anbindung an das sichere Netz der KVen.

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

Im sicheren Netz der KVen werden den Teilnehmern von den KVen und der KBV Dienste und Anwendungen zur Verfügung gestellt, die mit dem Begriff Applikationen (oder auch KV-Apps) zusammengefasst werden. Es besteht auch für KV-fremde Dienstanbieter die Möglichkeit, Dienste anzubieten, Voraussetzung hierfür ist eine Zertifizierung der betreffenden Applikation durch die KBV.

Der Anschluss mittels KV-SafeNet erfolgt durch einen von der KBV zertifizierten Provider. Dieser stellt einem Teilnehmer alle technischen Voraussetzungen zur Anbindung an das sichere Netz der KVen mittels einer Hardware-VPN-Lösung zur Verfügung und garantiert für die Sicherheit dieser Verbindung. Der Provider stellt dem Teilnehmer hierzu einen KV-SafeNet-Router zur Verfügung.

Beim Anschluss eines Teilnehmers über KV-FlexNet stellt die jeweilige KV des Teilnehmers eine von der KBV zugelassene Software-VPN-Lösung zur Verfügung und garantiert für die Sicherheit der Verbindung.

1.2 Ziel des Dokuments

Der Leitfaden beschreibt den prozessualen Ablauf einer Zertifizierung zum KV-SafeNet-Provider. Hierfür werden die normativen Vorgaben der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] erläutert und spezifiziert. In Kapitel 2 werden die allgemeinen Regelungen zur Zertifizierung aufgeführt und in Kapitel 3 die entsprechenden Unterlagen und deren Inhalte, die ein Unternehmen bzw. Provider einreichen muss, der an einem KV-SafeNet-Zertifizierungsverfahren teilnimmt.

Dem KV-SafeNet-Provider obliegen jedoch darüber hinausgehende Pflichten für den Zeitraum der KV-SafeNet-Zertifikatsgültigkeit, welche die Richtlinie [KBV_SNK_RLEX_KV-SafeNet] vorgibt.

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an Unternehmen, die sich als KV-SafeNet-Provider zertifizieren bzw. rezertifizieren möchten.

* Disclaimer: Bitte beachten Sie, dass KV-SafeNet nicht mit der Firma SafeNet, Inc., USA, in firmenmäßiger oder vertraglicher Verbindung steht.
[1] In der jeweiligen KV kann diese Lösung auch einen anderen Namen haben.

2 Regelungen zur Zertifizierung

2.1 Reihenfolge

Alle eingehenden Anträge auf Zertifizierung zum KV-SafeNet-Provider werden nach der Reihenfolge des Eingangs bearbeitet. Ein Anspruch auf Bevorzugung des Antrages besteht nicht.

2.2 Fristen

Die (Re-)Zertifizierung muss grundsätzlich innerhalb des Zeitraumes von sechs Monaten erfolgreich abgeschlossen sein. Bei Überschreitung des Zeitraumes wird die Zertifizierung abgebrochen.

Innerhalb des (Re-)Zertifizierungsprozesses hat der Antragsteller maximal vier Wochen nach Benachrichtigung durch das Referat Sicheres Netz der KVen/Prüfstelle Zeit, fehlende bzw. nachzubessernde Unterlagen einzureichen. Fristverlängerungen werden in Einzelfällen gewährt. Werden die erforderlichen Unterlagen nicht eingereicht, so wird das Zertifizierungsverfahren abgebrochen.

Der Abbruch des Zertifizierungsverfahrens durch eigenes Verschulden entbindet den Antragsteller nicht von der Pflicht, die Zertifizierungspauschale zu bezahlen. Dem Antragsteller steht frei, nach Abbruch des Zertifizierungsverfahrens, eine erneute Beantragung zur Zertifizierung durchzuführen.

Der Prüfvorgang im Zertifizierungsverfahren beginnt, sobald alle geforderten Unterlagen vollständig eingereicht wurden.

2.3 Das Referat Sicheres Netz der KVen/Prüfstelle

Das Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-SafeNet] ist der offizielle Antrag auf Zertifizierung bzw. Rezertifizierung zum KV-SafeNet-Provider. Diese ist – ebenso wie die Datenschutzerklärung – ausgefüllt und unterschrieben per Fax oder auf dem Postweg über folgende Adresse einzureichen:

Kassenärztliche Bundesvereinigung K.d.ö.R.
Referat Sicheres Netz der KVen/Prüfstelle
Herbert-Lewin-Platz 2
10623 Berlin

Alle weiteren Unterlagen bzgl. der Zertifizierung zum KV-SafeNet-Provider – ausgenommen das Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-SafeNet] und die Datenschutzerklärung – können per E-Mail an das Referat Sicheres Netz der KVen/Prüfstelle der KBV (pruefstelle@kbv.de) gesandt werden.

Betreffzeile: „Antrag auf Zertifizierung zum KV-SafeNet-Provider“.

Das Referat Sicheres Netz der KVen/Prüfstelle der KBV versendet ein Protokoll, welches den Verlauf der Prüfung wiedergibt, sobald diese als Teil oder im Ganzen abgeschlossen ist.

2.4 Kosten der Zertifizierung (Pauschale)

Art der Prüfung	Kosten in €
Erstzertifizierung	**2.249,00**
Rezertifizierung	**1.560,00**
Neue Zugangsvariante	**845,00**
Zertifizierung eines neuen Zugangsgeräts	**338,00**
Beratungsgespräch[2]	**338,00**
Verwaltungskosten	
Die Verwaltungskostenpauschale bezieht sich auf die Ausstellung von Konformitätsbescheinigungen und das Umschreiben von Prüfergebnissen (z.B. bei Wechsel der Produktverantwortlichkeit).	**120,00**

Anmerkungen

1. Die genannten Zertifizierungspauschalen verstehen sich immer zuzüglich der Verwaltungskostenpauschale pro Prüfung.
2. In Ausnahmefällen kann die Prüfung auch an einem vom Produktverantwortlichen bezeichneten Ort stattfinden. In diesem Fall trägt der Produktverantwortliche die Reisekosten der KBV-Mitarbeiter. Die Reisekosten werden dem Produktverantwortlichen pauschal berechnet. Die Höhe des Pauschalbetrages richtet sich nach Art und Höhe der Reisekosten und der Verpflegungspauschale für Dienstreisen.
3. Die KBV behält sich vor, einen Zusatzaufwand im Rahmen von Prüfungen gesondert zu berechnen. Ist bspw. über das normale Maß hinaus Aufwand seitens des Referates Sicheres Netz der KVen/Prüfstelle angefallen, so kann dem Antragsteller ein weiterer Kostenbescheid über den in der Tabelle der Zertifizierungspauschalen genannten Betrag gestellt werden. Über die Berechnung der Kosten entscheidet das Referat Sicheres Netz der KVen/Prüfstelle im Einzelfall.
4. Das KBV-Zertifizierungsverfahren gilt als erfolgreich abgeschlossen, wenn die Prüfung bestanden wurde. Nach Beendigung des Prüfverfahrens erhalten Sie für das Begleichen der Prüfkosten einen Kostenbescheid.
5. Bei der Umschreibung von Prüfergebnissen aufgrund von Änderungen bzgl. der Firma und/oder der Rechtsform, dem Wechsel der Verantwortlichkeit sowie Produktnamensänderungen ist erneut eine Verwaltungskostenpauschale zu entrichten. Diese Änderungen müssen in schriftlicher Form eingehen (formloses Anschreiben). Dabei ist seitens des Antragstellers eine neu ausgefüllte und unterschriebene Ergänzende Erklärung beizufügen.
6. Bei Änderungen der Adresse des Verantwortlichen genügt ein formloses Schreiben mit Originalunterschrift an das Referat Sicheres Netz der KVen/Prüfstelle.
7. Änderungen bezüglich der Ansprechpartner für Teilnehmer oder die KBV können formlos via E-Mail angezeigt werden.

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

2.5 Vorbehalt

Das Referat Sicheres Netz der KVen/Prüfstelle behält sich vor, technische Lösungen des Antragstellers vorführen oder das vorgelegte Konzept persönlich erläutern zu lassen.

2.6 Erstzertifizierung

Der Antragsteller reicht den Antrag in Form des Formulars Ergänzende Erklärung [KBV_SNK_FOEX_KV-SafeNet] mit den in Kapitel 3 näher erläuterten Unterlagen ein (siehe auch). Alle erforderlichen Anforderungsdokumente können von der Webseite http://www.kv-safenet.de heruntergeladen werden.

Nach Eingang aller Unterlagen wird das Referat Sicheres Netz der KVen/Prüfstelle die Unterlagen auf Konformität zur aktuell gültigen Richtlinie [KBV_SNK_RLEX_KV-SafeNet] prüfen.

Genügt das vorgelegte Konzept nicht den Anforderungen der aktuell gültigen Richtlinie [KBV_SNK_RLEX_KV-SafeNet], wird dem Antragsteller ein Brief mit allen zu korrigierenden Fehlern zugestellt. Nach Beseitigung dieser Fehler kann der Antragsteller sein Konzept erneut dem Referat SNK bzw. dem Referat Sicheres Netz der KVen/Prüfstelle vorlegen. Dabei sind die Fristen gemäß Abschnitt 2.2 zu beachten.

Entsprechen die Unterlagen den Anforderungen der Richtlinie, so hat der Antragsteller für jede Hardwarekomponente, welche als KV-SafeNet-Router eingesetzt werden soll, ein Testgerät einzureichen.

Nach erfolgreicher Zertifizierung und der Installation mindestens eines VPN-Konzentrators in einer KV 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. Die für den Verbleib in der KBV bestimmten Geräte sind für die Einwahl ins sichere Netz der KVen zu konfigurieren. Mit diesen Geräten muss jeder Zeit eine Verbindung ins sichere Netz der KVen möglich sein (KBV-Testzugang). Die entsprechenden Einstellungen werden dem Antragsteller mitgeteilt.

2.7 Rezertifizierung

Mindestens vier Monate vor Ablauf des derzeit gültigen Zertifikats müssen alle Dokumente und Geräte durch das Referat Sicheres Netz der KVen/Prüfstelle erfolgreich rezertifiziert sein, sofern die KV-SafeNet-Zertifizierung weiterhin bestehen soll. Der Provider muss hier, wie bei einer Erstzertifizierung, alle Unterlagen gemäß den Anforderungen der aktuell gültigen Richtlinie [KBV_SNK_RLEX_KV-SafeNet] vorlegen (siehe auch Abbildung 2: Vereinfachter Ablauf des Zertifizierungsverfahrens). Der Prozess der Rezertifizierung kann erheblich verkürzt werden, sofern die Änderungen gegenüber dem alten Konzept klar gekennzeichnet sind. Entsprechen die Unterlagen den Anforderungen der aktuellen Richtlinie [KBV_SNK_RLEX_KV-SafeNet], so hat der Antragsteller für jede Hardwarekomponente, welche als KV-SafeNet-Router eingesetzt werden soll, ein Testgerät einzureichen. Der eingereichte KV-SafeNet-Router ist für die Einwahl ins sichere Netz der KVen zu konfigurieren.

Möchte der Provider sein Zertifikat an eine neue gültige Version der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] anpassen, so hat er die Prüfung neuer Zugangsvarianten als auch aller bis dahin zertifizierten Zugangsvarianten zu beantragen.

Sollten die Unterlagen auch mit Nachbesserungen nicht zu einer KV-SafeNet-Konformität führen, so bleibt das ursprüngliche Zertifikat lediglich bis zum Ablauf der Zertifikatsgültigkeit gültig.

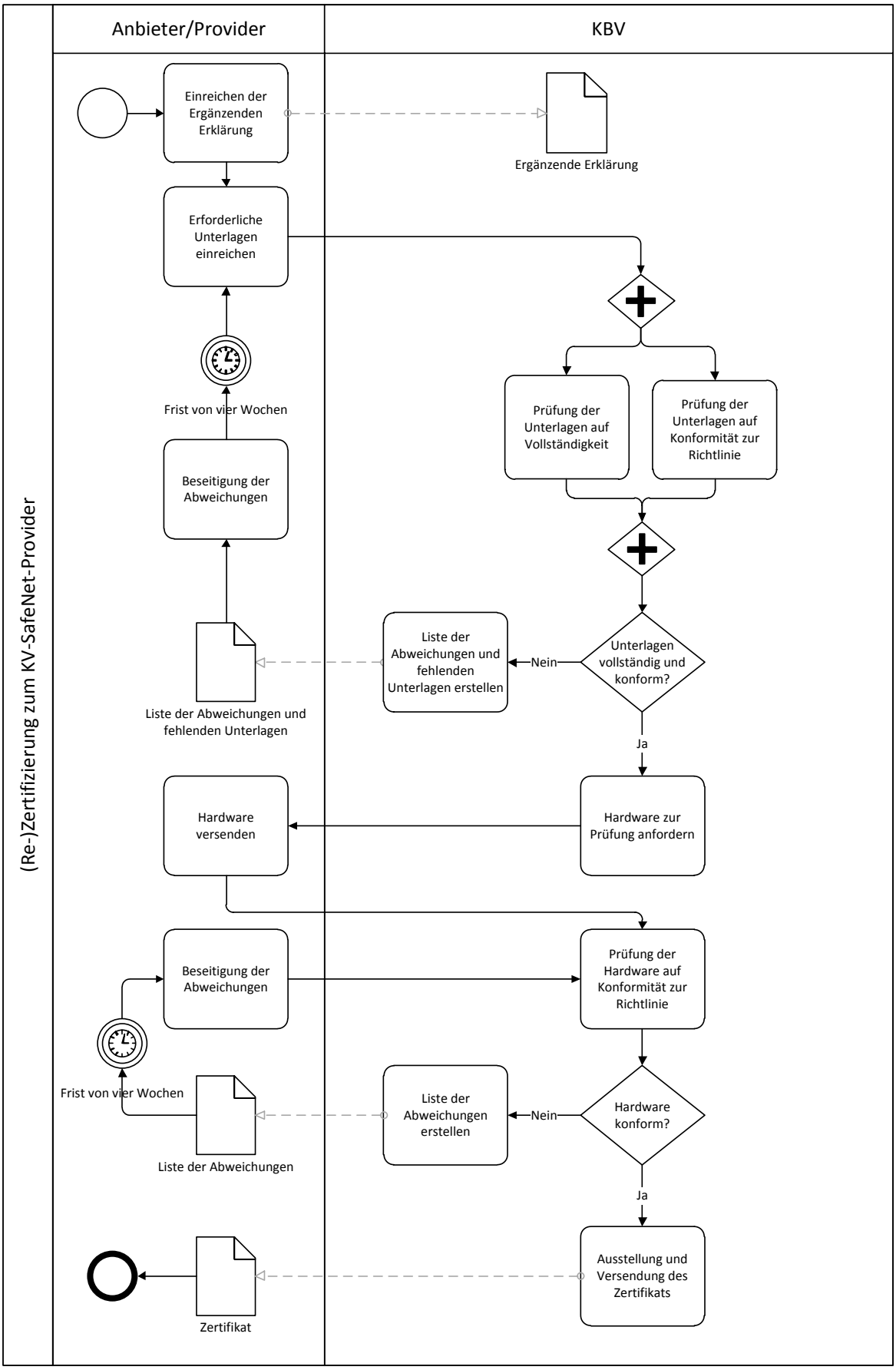

Abbildung 2: Vereinfachter Ablauf des Zertifizierungsverfahrens

3 Einzureichende Unterlagen

Organisatorische Unterlagen

- Konformitätserklärung über Einhaltung des Datenschutzes, siehe Abs. 3.2
- Musterteilnehmervertrag, siehe Abs. 3.3
- Mustervertrag bei Einbeziehung von Erfüllungsgehilfen, siehe Abs. 3.4
- Angebot des Anbieters, siehe Abs. 3.6
- Dokumente zur Informationssicherheit, siehe Abs. 3.7
- Diagramme der Betriebsprozesse, siehe Abs. 3.8
- Supportkonzepte, siehe Abs. 3.9
- Optionale Angaben, siehe Abs. 3.10

Technische Unterlagen

- Beschreibung der Anbindungsvarianten, siehe Abs. 3.11
- Dokumentation des VPN-Konzentrators, siehe Abs. 3.12
- Dokumentation des KV-SafeNet-Routers, siehe Abs. 3.13
- Format der kryptographischen Angaben, siehe Abs. 3.14

3.1 Ergänzende Erklärung

Anforderung

Einreichung des vollständig ausgefüllten Formulars Ergänzenden Erklärung [KBV_SNK_FOEX_ KV-SafeNet]

Erläuterung

Das Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-SafeNet] ist der offizielle Antrag auf Zertifizierung bzw. Rezertifizierung zum KV-SafeNet-Provider. Diese ist ausgefüllt und unterschrieben per Post oder Fax an das Referat Sicheres Netz der KVen/Prüfstelle zu senden (siehe 2.3).

Mit dem Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-SafeNet] stimmt der Antragsteller zu, dass er die aktuell gültige Richtlinie [KBV_SNK_RLEX_KV-SafeNet] und die darin referenzierten Dokumente ohne Einschränkungen anerkennt, sowie jegliche Änderungen, die KV-SafeNet-relevant sind, an das Referat Sicheres Netz der KVen/Prüfstelle zu melden. Dies betrifft insbesondere Änderungen an der vom Provider auf Seiten des Teilnehmers verwendeten KV-SafeNet-Hardware (KV-SafeNet-Router).

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in Abschnitt 2.1.1 (Zertifizierung)

3.2 Konformitätserklärung über Einhaltung des Datenschutzes

Anforderung

Einreichung der Konformitätserklärung über Einhaltung des Datenschutzes

Erläuterung

Der Antragsteller hat in einem unterschriebenen, formlosen Schreiben (welches per Post oder Fax einzureichen ist (siehe 2.3)) dem Referat Sicheres Netz der KVen/Prüfstelle mitzuteilen, dass alle an der KV-SafeNet-Lösung beteiligten Mitarbeiter des Antragstellers sowohl nach Datengeheimnis § 5 Bundesdatenschutzgesetz (BDSG) als auch nach Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz (TKG) verpflichtet wurden (siehe auch Abschnitt 3.7).

Als Grundlage für die Unterweisung der Mitarbeiter in die Einhaltung des Datenschutzes kann das auf der Webseite der KBV hinterlegte Dokument „Einschlägige Rechtsvorschriften zum Datenschutz“[3] benutzt werden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in Kapitel 2 (Regelungen)

3.3 Musterteilnehmervertrag

Anforderung

Einreichung des Musterteilnehmervertrages, der folgenden Mindestanforderungen berücksichtigt:

(1) Nur durch den Vertrag zwischen Anbieter und Teilnehmer entsteht dem Teilnehmer kein Anspruch gegenüber den KVen oder der KBV auf Zulassung zum sicheren Netz der KVen.

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

(3) Der Teilnehmer muss darauf hingewiesen werden, dass der Anbieter vor einer Vertragsverlängerung bei der jeweils zuständigen KV die Rechtmäßigkeit der Zulassung des Teilnehmers zum sicheren Netz der KVen bestätigen lassen muss.

(4) Der Anbieter muss im Rahmen des Vertrages den Teilnehmer über die Laufzeit seines Zertifikates als KV-SafeNet-Provider informieren.

(5) Dem Teilnehmer steht ein ordentliches Kündigungsrecht zu. Als ordentlicher Kündigungsgrund gilt u. a. 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.

(6) Dem Teilnehmer steht ein außerordentliches Kündigungsrecht aus wichtigem Grund zu, beispielsweise bei nicht erfolgter Aufklärung hinsichtlich der technischen Voraussetzungen, welche notwendig für den KV-SafeNet-Anschluss sind.

(7) Dem Teilnehmer muss vier Monate vor Ablauf der Zertifikatsgültigkeit des Anbieters ein außerordentliches Kündigungsrecht entsprechend 2.5.6 der Richtlinie

[3] Siehe: http://www.kbv.de/html/5536.php

[KBV_SNK_RLEX_KV-SafeNet] zum Ende der Zertifikatsgültigkeit eingeräumt werden. 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, falls sich der Anbieter nicht entsprechend 2.1.7 der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] rezertifizieren lassen hat.

(8) Falls eine Rezertifizierung nicht angestrebt wird, so muss der Anbieter mindestens sechs Monate vor Ablauf der Zertifikatsgültigkeit eine Information an die Teilnehmer versenden. Bei einem Verstoß gegen diese Regelung übernimmt der Anbieter die Wechselkosten der Teilnehmer.

(9) Der Anbieter sichert dem Teilnehmer die Erreichbarkeit des sicheren Netzes der KVen mindestens für den Zeitraum der Vertragslaufzeit zu.

(10) Der Vertrag muss eine für den Teilnehmer verständliche Übersicht der Kosten enthalten. Dazu gehört die Angabe aller Voraussetzungen und zusätzlich anfallender Kosten.

(11) Der Anbieter stellt dem Teilnehmer die Kontaktdaten für den Teilnehmersupport zur Verfügung, inklusive Servicezeiten und -kosten für Serviceanfragen des Teilnehmers.

(12) Der Vertrag muss Regelungen über Zugriffe auf den KV-SafeNet-Router für Fälle von Störungen, Wartungen und Updates etc. enthalten, inkl. Angabe eines Ansprechpartners oder einer Supporthotline. Diese Regelungen müssen gewährleisten, dass

a. der Teilnehmer die aktive Möglichkeit hat, den Wartungszugang zu steuern, indem er zum Einen grundsätzlich der Fernwartung zustimmen und zum Anderen den Zeitpunkt eines jeweiligen Wartungszugriffs bestimmen und autorisieren kann,

b. der Teilnehmer über Zeitpunkt und Inhalt aller durchgeführten Wartungs- und Administrationsaktivitäten auf Verlangen schriftlich zu informieren ist,

c. der Teilnehmer darüber informiert wird, dass der Provider alle Wartungsaktivitäten umfassend protokolliert und die Protokolle dem Teilnehmer auf Anforderung zur Einsicht überlassen werden sowie dass auf Wunsch des Teilnehmers auch von ihm beauftragte Personen berechtigt sind, diese Protokolle zu prüfen.

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

(14) Der Teilnehmer muss darauf hingewiesen werden, dass die Weitergabe des KV-SafeNet-Routers an Dritte verboten ist.

(15) 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.

(16) Es muss eine Regelung enthalten sein über die Rückgabe des KV-SafeNet-Routers bei Vertragsende bzw. die vollständige Zurücksetzung des Gerätes, wenn dieses Eigentum des Teilnehmers ist. Ein aktives Einbinden des Kunden ist nicht gestattet.

(17) Der Teilnehmer erhält ein Kontrollrecht über die fortlaufende Einhaltung der Richtlinie [KBV_SNK_RLEX_KV-SafeNet], welches die KBV für ihn ausüben kann.

(18) Der Teilnehmer ist im Vertrag darauf hinzuweisen, dass der KV/KBV das Recht eingeräumt wird, den KV-SafeNet-Anschluss des Teilnehmers im Falle eines Missbrauches zu sperren.

(19) Der Anbieter muss den Teilnehmer darauf hinweisen, dass die KBV/KV keinerlei Haftung sowohl bzgl. der Verfügbarkeit und der IT-Sicherheit des Zugangsnetzes des Anbieters, als auch bzgl. der Sicherheit des Teilnehmernetzes übernimmt.

Zusätzliche Anforderungen bei der Umsetzung von Mehrwertdiensten

(20) Die Nutzung von Mehrwertdiensten ist als frei wählbare Option im Vertrag aufzuführen.

(21) Der Teilnehmer beantragt das Angebot von Mehrwertdiensten, separat zum KV-SafeNet-Zugang über ein gesondertes Netz des Anbieters, mit seiner Unterschrift.

(22) Falls neben den Sicherheitsmaßnahmen für den KV-SafeNet-Zugang gemäß Abschnitt 3.5 weitere hinzukommen, so ist dem Teilnehmer eine Sicherheitsbelehrung für den Mehrwertdienst mitzuliefern.

Zusätzliche Angaben bei der Einbeziehung von Erfüllungsgehilfen

(23) Der Anbieter muss dem Teilnehmer benennen, welche Erfüllungsgehilfen er für welchen Aufgabenbereich zur Erfüllung des Vertrages einsetzt.

Erläuterung

Der Teilnehmervertrag unterteilt sich generell in den Teil, der den Zugang zum sicheren Netz der KVen regelt und in den Teil, der sich mit den vom Antragsteller angebotenen Mehrwertdiensten befasst. Sollten seitens des Anbieters keine Mehrwertdienste angeboten werden, entfällt der zweite Teil.

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

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in Abschnitt 2.5 (Anforderungen an den Teilnehmervertrag)

3.4 Mustervertrag bei Einbeziehung von Erfüllungsgehilfen

Anforderung

Einreichung des Mustervertrages mit etwaigen Erfüllungsgehilfen, der folgende Mindestangaben beinhaltet:

(1) Eine Verpflichtung des Erfüllungsgehilfen zur Einhaltung der Richtlinie [KBV_SNK_RLEX_KV-SafeNet].

(2) Eine Klarstellung, dass sich der Anbieter eines Erfüllungsgehilfen bedient und für Verschulden des Erfüllungsgehilfen und seiner Hilfspersonen nach § 278 BGB einsteht.

(3) Umfang und Art der Tätigkeiten aller Erfüllungsgehilfen müssen angegeben werden.

(4) Der Erfüllungsgehilfe hat dem Anbieter alle Personen zu nennen, die im Rahmen dieses Vertrages eine Aufgabe erfüllen.

(5) Die Bereitstellung von geheimen, datenschutzrechtlichen Informationen hat auf sicherem Wege zu erfolgen.

(6) Der Erfüllungsgehilfe und seine Hilfspersonen verpflichten sich zur Einhaltung der Geheimhaltungs- und Datenschutzpflichten gemäß Abschnitt 0.

(7) Der Anbieter hat ein Weisungsrecht gegenüber Erfüllungsgehilfen und seinen für den Anbieter eingesetzten Hilfspersonen.

(8) Der Erfüllungsgehilfe und seine Hilfspersonen treten nach außen sichtbar als Erfüllungsgehilfe des Anbieters auf.

Erläuterung

Der Anbieter hat dem Referat Sicheres Netz der KVen/Prüfstelle mitzuteilen, wenn er im Rahmen der Bereitstellung des KV-SafeNet-Zugangs Erfüllungsgehilfen einsetzt.

Sollte es Anpassungen seitens des Anbieters an den Vertrag mit den Erfüllungsgehilfen geben, so hat der Anbieter vor Einsetzen des neuen Vertrages diesen dem Referat Sicheres Netz der KVen/Prüfstelle vorzulegen.

Sollte der Antragsteller keine Erfüllungsgehilfen einsetzen, so ist dies explizit zu erwähnen.

Hinweis: Vertriebspartner dürfen im Gegensatz zu Erfüllungsgehilfen nicht als KV-SafeNet-Provider auftreten.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in Abschnitt 2.6.11 (Sicherheit der Zugangsdaten)

3.5 Sicherheitsbelehrung für den Teilnehmer

Anforderung

Sicherheitsbelehrung für den Teilnehmer bei Nutzung von Mehrwertdiensten

Erläuterung

Dem Anbieter ist es freigestellt das Angebot zur Nutzung des sicheren Netzes der KVen mit sogenannten Mehrwertdiensten (z.B. parallele Nutzung des Internets) zu erweitern.

Für den Fall, dass der Teilnehmer Mehrwertdienste nutzen möchte, hat der Antragsteller dem Teilnehmer eine Sicherheitsbelehrung über die Nutzung des sicheren Netzes der KVen vorzulegen.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.5 (Anforderungen an den Teilnehmervertrag) und 2.6.16 (Besondere Sicherheitsmaßnahmen bei Nutzung von Mehrwertdiensten)

3.6 Angebot des Anbieters

Anforderung

Einreichung einer Übersicht mit den für den Teilnehmer relevanten Kosten

Erläuterung

Das Angebot bzw. die Kostenübersicht, welche der Antragsteller gemäß der Ergänzenden Erklärung an das Referat Sicheres Netz der KVen/Prüfstelle zu senden hat, muss nach Art des Zugangs, Einmalkosten und laufenden Kosten aufgeschlüsselt werden (siehe auch Abschnitt 3.3).

Es müssen alle anfallenden Kosten nachvollziehbar aufgelistet werden. Sollte es neben den Kosten für das KV-SafeNet-Angebot weitere Kosten geben, so ist dies gesondert kenntlich zu machen.

3.7 Dokumente zur Informationssicherheit

Anforderung

Einreichung dokumentierter interner Regelungen zum Informationssicherheitsmanagement

Erläuterung

Zu folgenden Themen, die das Informationssicherheitsmanagement beim Anbieter beschreiben, müssen interne Regelungen in dokumentierter Form zur Prüfung eingereicht werden:

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

Weitere Informationen zu den Anforderungen an ein Informationssicherheitsmanagement sind dem Leitfaden Überprüfung Provider [KBV_SNK_LFEX_Überprüfung_Provider] sowie der Richtlinie Informationssicherheit [KBV_SNK_RLEX_Informationssicherheit] zu entnehmen.

Falls der Anbieter im Rahmen einer Zertifizierung nach ISO 27001 (oder vergleichbar) oben genannte Nachweise bereits erbracht hat, so kann das entsprechende Zertifikat eingereicht werden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in Kapitel 2 (Regelungen)

3.8 Diagramme der Betriebsprozesse

Anforderung

Beschreibung der folgenden Betriebsprozesse (1) Einrichtung eines neuen Zugangs, vom Auftrag des Teilnehmers bis zur Freischaltung (2) Temporäre Sperrung eines Zugangs (inkl. Gründe der Sperrung) (3) Erneute Freischaltung eines Zugangs (4) Endgültige Sperrung bei Kündigung (5) Monitoring (Überwachen) des laufenden Netzbetriebes (6) Erkennen, Abwehr und Meldung von Angriffen mit der Angabe der dafür verwendeten

Tools (Firewall, Intrusion Detection System, Monitoring Systeme etc.)

(7) Übermittlung des techn. Berichtswesens inkl. Ausfälle an die KBV

(8) Übermittlung der Vertrags- und Teilnahmestatistiken an die KVen

(9) Übermittlung der kumulierten Teilnehmerstatistiken an die KBV

Erläuterung

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

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

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

Ausgewählte Anforderungen an die Dokumentation werden im Folgenden genauer beschrieben.

(1) – (6) Integration des Prozesses Statistiklieferung (techn. Berichtswesens inkl. Ausfälle und der Teilnahmestatistiken) in den jeweiligen Diagrammen.

zu (4): Bei der endgültigen Sperrung des Zugangs ist das Löschen der Konfiguration des KV-SafeNet-Routers (Werkszustand wiederherstellen) zwingend erforderlich und muss durch den Anbieter erfolgen. Ein aktives Einbinden des Kunden ist nicht gestattet.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.4 (Berichtswesen), 2.6.13 (Überwachungsmaßnahmen - Anbieter), 2.6.14 (Betriebszeit und Verfügbarkeit) und 2.6.15 (Wartungsarbeiten)

3.9 Supportkonzepte

3.9.1 Supportkonzept für den KV-SafeNet-Router

Anforderung

Einreichung eines Supportkonzeptes für den KV-SafeNet-Router, welches die folgenden Mindestangaben enthält:

(1) Zugriff auf den KV-SafeNet-Router
   a. Remote (Fernwartung), in Verbindung mit (2)
   b. Vor Ort, in Verbindung mit (3)

(2) Beschreibung und Absicherung des Wartungszugangs, siehe Abschnitt 3.14

(3) Prozess der Störungsbehebung beim Teilnehmer

(4) Beschreibung des Anwendersupports mit
   a. Kontaktdaten
   b. Zeiten der Erreichbarkeit
   c. Organisatorischem Aufbau des Service

(5) Protokollierung der Wartungsaktivitäten

(6) Angaben zu den verwendeten Passwörtern

(7) Verwaltung der Passwörter auf den Geräten

Erläuterung

Das Supportkonzept muss den Wartungsablauf des KV-SafeNet-Routers und die Betreuung der Teilnehmer beschreiben. Ausgewählte Anforderungen an das Supportkonzept werden im Folgenden genauer beschrieben.

zu (1): Die Wartung des KV-SafeNet-Routers muss unter Wahrung der vertraglichen Rechte und Pflichten gem. Abschnitt 3.3 (Musterteilnehmervertrag) erfolgen.

zu (1a): Die Fernwartung kann nur durchgeführt werden, sofern dies vom Teilnehmer gewünscht und zum Zeitpunkt des Zugriffs autorisiert wurde. Zudem muss der Antragsteller sicherzustellen, dass eine Gefährdung des KV-SafeNet-Routers, des Teilnehmernetzwerkes und somit des sicheren Netzes der KVen durch einen Fernzugriff jederzeit ausgeschlossen ist (siehe auch Abschnitt 3.3 ((12)/(12)a/(12)b/(12)c)). Der Einsatz von Third-Party-Software sowie die Vermittlung der Fernwartung über Fremdserver sind nicht erlaubt.

zu (3): Der Prozess der Störungsbehebung muss eine Unterscheidung verschiedener eintretender Szenarien nachvollziehbar darstellen.

zu (4c): Beschreibung des organisatorischen Aufbaus des Supports, sowie die Detaillierungen der jeweiligen Support-Level (1st-Level, 2nd-Level und 3rd-Level).

zu (5) Protokollierung mit Angabe der folgenden Informationen: Datum, Beginn, Ende, Dauer sowie Inhalt der durchgeführten Maßnahmen.

zu (6): Verwendete Passworte müssen den Regelungen zum Passwortgebrauch des BSI folgen (siehe M 2.11 Regelung des Passwortgebrauchs) [4].

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.6.1 (KV-SafeNet-Router) und 2.6.15 (Wartungsarbeiten)

3.9.2 Supportkonzept des VPN-Konzentrators

Anforderung

Einreichung eines Supportkonzeptes des VPN-Konzentrators, welches die folgende Mindestangaben enthält:

(1) Beschreibung des Supportprozesses im Falle

   a. einer Wartung

   b. einer Störung

   c. eines Updates

(2) Beschreibung des Wartungszugangs, insbesondere

   a. auf welchem Weg der Zugang erfolgt,

   b. wie die Sicherheit des Wartungszugangs gewährleistet wird, siehe Abschnitt

[4] Siehe: http://www.bsi.bund.de

3.14 und

c. wie die Unsichtbarkeit aus dem Internet realisiert wird.

(3) Angabe der Reaktionszeiten

(4) Angabe der Wiederherstellungszeiten

(5) Angaben zu den verwendeten Passwörtern

(6) Verwaltung der Passwörter auf den Geräten

Erläuterungen

Das Supportkonzept muss den Wartungsablauf des VPN-Konzentrators beschreiben. Ausgewählte Anforderungen an das Supportkonzept werden im Folgenden genauer beschrieben.

zu (5): Verwendete Passworte müssen den Regelungen zum Passwortgebrauch des BSI folgen (siehe M 2.11 Regelung des Passwortgebrauchs) [5].

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.6.2 (VPN-Konzentratoren) und 2.6.15 (Wartungsarbeiten)

3.10 Optionale Angaben

Anforderung

Einreichung weiterer Zertifikate

Erläuterung

Liegen für die Managementprozesse oder für die eingesetzten Komponenten bzw. Lösungen und Konzepte bereits Zertifikate (z.B. BSI, Common Criteria, ISO) vor, so können diese im Rahmen der KV-SafeNet-Zertifizierung vorgelegt werden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in Kapitel 2 (Regelungen)

3.11 Beschreibung der Anbindungsvarianten

Anforderung

Dokumentation der angebotenen Anbindungsvarianten, die folgende Mindestanforderungen erfüllt:

(1) Grafische Darstellung der Anbindungsvarianten inkl. Abgrenzung der Verantwortlichkeitsbereiche

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

a. aus dem oder den lokalen Netzen des Anbieters auf Komponenten des siche-

[5] Siehe: http://www.bsi.bund.de

ren Netzes der KVen

b. auf das Teilnehmernetzwerk aus dem sicheren Netz der KVen heraus

c. auf die Konfigurationsschnittstelle des KV-SafeNet-Routers

(3) Erläuterung zur Sicherstellung der Unsichtbarkeit der Teilnehmercomputer

(4) Erläuterung der Maßnahmen zur Gewährleistung der Sicherheit bei Nutzung von Mehrwertdiensten

(5) Nennung des zum Einsatz kommenden VPN-Protokolls

(6) Nennung der Konfiguration des VPN-Tunnels

(7) Nennung der Konfiguration der Protokoll-Suite IPsec

(8) Beschreibung der verwendeten Kryptographie Verfahren

(9) Bestätigung, dass der „Nutzdatentunnel“ nicht unterbrochen wird, sondern eine Site-to-Site-Sicherheit des VPN-Tunnels zwischen KV-SafeNet-Router (beim Teilnehmer) und dem VPN-Konzentrator (in der jeweiligen KV) gegeben ist.

Erläuterung

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

zu (1): Die angeforderte grafische Darstellung der Anbindungsvarianten muss in Form eines detaillierten Netzplans bzw. eines technischen Schaubildes (inkl. Angabe der konkreten IP-Adressen des jeweiligen Interfaces) eingereicht werden.

zu (4) Bspw. darf der Datenverkehr, welcher im Rahmen des Mehrwertdienstes „Internetnutzung“ auftritt, nicht in den Nutzdatentunnel geleitet werden. Dies muss entsprechend dargelegt werden.

(5) – (8) Die Vorgaben zum Format der kryptographischen Angaben entnehmen Sie Abschnitt 3.14.

zu (6) Die Angaben zur Konfiguration des VPN-Tunnels umfassen **u.a.**:

- Verpflichtender Einsatz von Zertifikaten
- Adressierung der im VPN übertragenen IP-Pakete (Siehe Konzept IP-Adressvergabe [KBV_SNK_KNEX_IP-Adressvergabe])
- Keine Einschränkung der **im VPN** offenen Ports und übertragenen Protokolle

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.3 (Schutz der Anbindung) und 2.6 (Technische Anforderungen)

3.12 Dokumentation des VPN-Konzentrators

Anforderung

Dokumentation jedes VPN-Konzentrators mit folgenden Mindestangaben:

(1) (Geplante) Standorte der VPN-Konzentratoren

(2) Technische Unterlagen oder Produktbeschreibungen zum Nachweis der Unterstützung des Routingprotokolls BGP-4

(3) Vollständige Liste der verwendeten Dienste/Ports

(4) Erläuterung zu Sicherungsmaßnahmen des VPN-Konzentrators

(5) Textuelle Beschreibung der Gerätekonfiguration

(6) Verwendete Routingtabelle(n)

(7) Aufzählung und Beschreibung der verwendeten Management-Tools

(8) Nachweis bzw. Zusicherung der Verfügbarkeitsgewährleistung von 99,5% p.a.

(9) Erläuterungen zum Zugang und zur Absicherung der Management-Schnittstelle

(10) Benennung der Personen, die Zugriff auf die Konfigurationsdateien und Schlüssel haben

Erläuterung

Es müssen Unterlagen und Informationen bzgl. des VPN-Konzentrators eingereicht werden. Ausgewählte Anforderungen an die Dokumentation werden im Folgenden genauer beschrieben.

zu (4): Die Erläuterung der Sicherungsmaßnahmen des VPN-Konzentrators umfasst das Deaktivieren nicht benötigter Dienste - insbesondere Dienste, wie telnet oder ftp - bzw. die Stilllegung ungenutzter Ports des Konzentrators bzw. die Konfiguration von Zugriffssteuerungslisten (Access Control Lists) (siehe BSI-Maßnahmen M4.201 und M4.202)[6].

zu (5): Die textuelle Beschreibung der Gerätekonfiguration (bspw. durch zusätzliche Konfigurationsdatei) soll mindestens Angaben zu folgenden Eigenschaften/Parametern enthalten:

a. Externes/internes Interface
b. VPN
c. Firewall
d. weitere sicherheitsrelevante Parameter

zu (7): Die Aufzählung der verwendeten Management-Tools umfasst auch die Erwähnung der ggf. eingesetzten Fault- und Anti-Fraud-System-Tools.

zu (8): Zusätzlich zum Nachweis der Verfügbarkeitsgewährleistung kann optional ein Redundanzkonzept eingereicht werden.

zu (9): Die Erläuterung zum Zugang und zur Absicherung der Management-Schnittstellen soll folgende Mindestangaben umfassen:

a. Konfiguration des VPN-Tunnels (SSL/TLS oder IPSEC), siehe Abschnitt 3.14
b. Aufzählung der verwendeten Verschlüsselungsverfahren insbesondere un-

[6] Siehe: http://www.bsi.bund.de

ter Angabe der verwendeten Algorithmen zum Schlüsselaustausch und der Schlüssellängen der verwendeten symmetrischen Verfahren entsprechend der Vorgaben aus Abschnitt 3.14.

c. Die Passwörter auf den Geräten sind in gehashter Form zu speichern. Die Hashverfahren müssen den aktuellen Empfehlungen des BSI[7] entsprechen.

d. Die Zugangsdaten müssen beim Anbieter verschlüsselt abgespeichert werden und dürfen nicht im Klartext vorliegen.

zu (10) Es müssen sämtliche Personen angegeben werden, die Zugriff auf die Konfigurationsdateien und Schlüssel haben. Diese Angabe kann im Rahmen des Supportkonzeptes für den KV-SafeNet-Router (siehe Abschnitt 3.9.1) bzw. das Servicekonzept des VPN-Konzentrators (siehe Abschnitt 3.9.2) erfolgen.

Falls diese Angaben bereits vollständig und korrekt auf der eingereichten Datenschutzerklärung abgegeben wurden, so müssen die Daten nicht erneut eingereicht werden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.2.1 (Anzahl Einwahlknoten), 2.3 (Schutz der Anbindung) und 2.6 (Technische Anforderungen)

3.13 Dokumentation des KV-SafeNet-Routers

Anforderung

Dokumentation jedes Gerätes, das als KV-SafeNet-Router eingesetzt wird, mit folgenden Mindestangaben:

(1) Technische Unterlagen oder Produktbeschreibungen

(2) Erläuterung der realisierten Sicherungsmaßnahmen

(3) Vollständige Liste der verwendeten Dienste/Ports

(4) Erläuterung zu Schutzmaßnahmen der Konfigurationsschnittstelle vor unbefugtem Zugriff

(5) Beschreibung der Gerätekonfiguration

(6) Verwendete Routingtabelle(n)

(7) Beschreibung der verwendeten Verschlüsselungsverfahren, siehe Abschnitt 3.14

(8) Vorgehen bei notwendigen Firmware-Updates

Optionale Angaben (sofern zutreffend bzw. vorhanden)

(9) Benutzerhandbuch/Installationshandbuch für den Teilnehmer

(10) Beschreibung der individuellen Anpassung - sofern ein OTS (of the shelf) Produkt verwendet und für den Einsatz als KV-SafeNet-Router modifiziert wurde

(11) Beschreibung der zusätzlich auf dem KV-SafeNet-Router installierten bzw. installierbaren Funktionalitäten

(12) Benennung der Personen, die Zugriff auf die Konfigurationsdateien und Schlüssel haben

[7] Siehe: http://www.bsi.bund.de

Erläuterung

Es muss für jeden KV-SafeNet-Router eine Dokumentation eingereicht werden. Ausgewählte Anforderungen an die einzureichenden Unterlagen werden im Folgenden genauer beschrieben.

zu (1): Die technischen Unterlagen können bspw. in Form von Datenblättern oder Produktbeschreibungen (Handbücher) des KV-SafeNet-Routers eingereicht werden.

zu (2): Die Erläuterung zu den Sicherungsmaßnahmen des KV-SafeNet-Routers umfasst bspw. das Deaktivieren nicht benötigter Dienste und Funktionalitäten (dies betrifft insbesondere Dienste, wie telnet oder ftp) bzw. die Stilllegung ungenutzter Ports des Routers bzw. die Konfiguration von Zugriffssteuerungslisten (Access Control Lists) (siehe BSI-Maßnahmen M4.201 und M4.202)[8].

zu (3) Intern dürfen maximal die Ports 22, 443 und 53 verwendet werden.

zu (4) Die Erläuterung zum Zugang und zur Absicherung der Konfigurationsschnittstelle vor unbefugten Zugriff soll folgende Mindestangaben umfassen:

a. Die Passwörter auf den Geräten sind in gehashter Form zu speichern. Die Hashverfahren müssen den aktuellen Empfehlungen des BSI[9] entsprechen.

b. Die Zugangsdaten müssen beim Anbieter verschlüsselt abgespeichert werden und dürfen nicht im Klartext vorliegen.

zu (5) Die Beschreibung der Gerätekonfiguration (bspw. durch zusätzliche Konfigurationsdatei) soll mindestens Angaben zu folgenden Eigenschaften/Parametern enthalten:

a. Externes/internes Interface

b. VPN

c. Firewall und konfigurierte Firewall-Regeln

d. weitere sicherheitsrelevante Parameter

zu (11) Der Anbieter darf zusätzlich zur Anbindung an das sichere Netz der KVen weitere Funktionalitäten auf dem KV-SafeNet-Router installieren bzw. bereits installierte Funktionalitäten freischalten und konfigurieren, wenn diese den VPN Zugang zum sicheren Netz der KVen nutzen, um durch die KBV zertifizierte oder registrierte Applikationen im sicheren Netz der KVen ansprechen zu können.

Der Anbieter hat sicherzustellen, dass die Funktionalität und Sicherheit der KV-SafeNet-Anbindung an das sichere Netz der KVen unter allen Umständen gewährleistet ist.

Zu (12) Es müssen sämtliche Personen angegeben werden, die Zugriff auf die Konfigurationsdateien und Schlüssel haben. Diese Angabe kann im Rahmen des Supportkonzeptes für den KV-SafeNet-Router (siehe Abschnitt 3.9.1) bzw. das Servicekonzept des VPN-Konzentrators (siehe Abschnitt 3.9.2) erfolgen.

Falls diese Angaben bereits vollständig und korrekt auf der eingereichten Datenschutzerklärung abgegeben wurden, so müssen die Daten nicht erneut eingereicht werden.

Hinweis: Im Anschluss an die erfolgreiche Prüfung der eingereichten Dokumente wird eine hardwareseitige Prüfung des jeweiligen KV-SafeNet-Routers durchgeführt (siehe Kapitel 4).

[8] Siehe: http://www.bsi.bund.de
[9] Siehe: http://www.bsi.bund.de

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.3 (Schutz der Anbindung) und 2.6 (Technische Anforderungen)

3.14 Format der kryptographischen Angaben

Anforderung

Dokumentation der Angaben zu eingesetzten Kryptographie Mechanismen, sofern diese verwendet werden:

(1) Angaben zur Version des Transport Layer Security (TLS) Protokolls

(2) Angabe der im Protokoll TLS verwendeten kryptografischen Algorithmen

(3) Angabe der Konfiguration der Protokoll-Suite IPsec

(4) Angabe zum Einsatz von kryptographischen Algorithmen bei der Verwendung von SSH

(5) Detaillierte Angaben zu eingesetzten digitalen Zertifikaten

Erläuterung

Alle Angaben zu den Sicherheitseinstellungen müssen an den jeweiligen Stellen in der Dokumentation oder z.B. in einem separaten Kapitel beschrieben werden. Wenn diese Beschreibungen in einem separaten Kapitel erfolgen, so muss klar ersichtlich sein, für welches Gerät/Komponente/Software/Zugriff die jeweilige Einstellung gilt. Dabei bietet es sich an ggf. an den entsprechenden Stellen der Dokumentation auf dieses (separate) Kapitel zu verweisen.

zu (2): Dies umfasst die Angabe der verwendeten Algorithmen für die Funktionalitäten:

- TLS Version
- Schlüsselaustausch / -einigung
- Darlegung der Umsetzung von Perfect Forward Secrecy (PFS)
- (Schlüssel-) Authentifizierung
- Verschlüsselung (inkl. Schlüssellänge)
- Hashfunktion

Die Angabe der Kombination der verwendeten Algorithmen hat dabei in der folgenden Form zu erfolgen:

TLS_[Schlüsselaustausch]_[Autentifizierung]_WITH_[Verschlüsselung]_[Modus Verschlüsselung]_[Hashfunktion]

Beispiel: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

zu (3) Die folgenden Detailinformationen sind anzugeben:

- Angaben zum IKE-Protokoll
  - IKE-Version
  - Eingesetzte Verschlüsselungsverfahren (inkl. Schlüssellängen)
  - Integritätsschutzverfahren (z. B. AUTH_HMAC_SHA2_512_256)
  - Darlegung der Umsetzung von Perfect Forward Secrecy (PFS) (Diffie-Hellmann-Gruppe in beiden IKE-Phasen)
  - Verfahren zur gegenseitigen Authentisierung

- Angaben zum ESP-Protokoll
  - Eingesetzte Verschlüsselungsverfahren (inkl. Schlüssellängen)
  - Eingesetzter Integritätsschutz der ESP-Pakete

zu (4) Die folgenden Detailinformationen sind anzugeben:

- SSH-Version
- Schlüsselaustausch/-einigung
- Verschlüsselung (inkl. Schlüssellänge)
- MAC-Sicherung
- Server-Authentisierung
- Client-Authentisierung

zu (5) Die folgenden Detailinformationen sind anzugeben:

- Algorithmus (RSA, inkl. Schlüssellänge)
- Hashfunktion (SHA) → Signaturerstellung
- Gültigkeitsdauer
- Zertifikatstyp mit Version –(bspw. X.509v3)
- Offizielles oder selbst erzeugtes Zertifikat

Hinweis: 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)[10] entnommen werden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] im Abschnitt 2.6

[10] BSI TR-02102 siehe: https://www.bsi.bund.de

4 Praktische Prüfung des KV-SafeNet-Routers

Anforderung

Erfolgreiche Prüfung der verwendeten Hardwarekomponenten

Erläuterung

Entsprechen die Unterlagen den Anforderungen der Richtlinie, so hat der Antragsteller für jede Hardwarekomponente, welche als KV-SafeNet-Router eingesetzt werden soll, ein Testgerät einzureichen.

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

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

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

Das Referat Sicheres Netz der KVen/Prüfstelle behält sich vor, den Anschluss und die Wartung eines KV-SafeNet-Routers praktisch vorführen zu lassen.

Im Anschluss an die erfolgreiche Prüfung verbleibt für die Laufzeit des Zertifikates mindestens ein im Rahmen der Zertifizierung geprüftes Gerät des Anbieters in der KBV. Die Auswahl dieses Gerätes erfolgt durch die KBV.

Der KV-SafeNet-Router ist grundsätzlich in der zum Zeitpunkt der Zertifizierung bzw. Re-Zertifizierung verfügbaren maximalen Konfiguration, d.h. mit allen verfügbaren Diensten und Funktionalitäten, zu prüfen. Im Rahmen der hardwareseitigen Prüfung wird ausschließlich die Anbindung an das sichere Netz der KVen überprüft.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-SafeNet] in den Abschnitten 2.1.3 (Bereitstellung der Hardware) und 2.6.1 (KV-SafeNet-Router)

5 Glossar

Begriff	Erklärung
Anbieternetz	Zum Netz des Anbieters zählen alle notwendigen Dienste und Infrastrukturelemente, die zur Einrichtung, Aufrechterhaltung und Wartung der KV-SafeNet Anbindung zwischen Teilnehmer und KV notwendig sind.
Applikation	Services und Anwendungen im sicheren Netz der KVen
Applikationsanbieter	Anbieter eines Dienstes
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.
Fault-, bzw. Anti-Fraud Systeme	Diese Managementsysteme dienen der Vorbeugung, Entdeckung und adäquaten Reaktion von Computer- bzw. Wirtschaftskriminalität. Dazu gehören u. a. Ausspähen von vertraulichen Informationen, unerlaubtes Modifizieren der Daten oder der Verlust von Daten.
Firewall	Eine Firewall dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall unerlaubte Netzwerkzugriffe zu unterbinden.
Firmware	Firmware bezeichnet Software, die in elektronische Geräte fest eingebettet und somit mit dem Gerät untrennbar verbunden ist. Eine Firmware benötigt u.U. in regelmäßigen Abständen ein Update.
Fremdprovider/VPN-Provider	Ein VPN-Provider stellt im Gegensatz zum ISDN, DSL oder UMTS Provider nicht die technischen Voraussetzungen bzgl. der Übertragungstechnik zur Verfügung, sondern nutzt eine bereits bestehende Internetverbindung.
KV-App	Siehe 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 Verantwortung des KV-Backbone-Betreibers.
Tunnel/VPN-Tunnel	Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt. Daher spricht man bei VPN vom Tunnel.
Zertifizierung	Prozess in dem explizit nachgewiesen wird, wie der Antragsteller die in der Richtlinie geregelten Anforderungen umsetzt. Wird dieses Verfahren erfolgreich abgeschlossen, erhält der Antragsteller eine Konformitätserklärung.
Zugangsnetz	Dazu gehören Netzelemente und Vermittlungsstellen, die Grundlagen der techn. Infrastruktur zwischen Anbieter- und Teilnehmeranschluss schaffen.

6 Referenzierte Dokumente

Alle im Folgenden aufgelisteten Dokumente sind unter http://www.kbv.de/html/5536.php beziehbar.

Referenz	Dokument
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_FOEX_KV-SafeNet]	Formular Ergänzende Erklärung zur Zertifizierung zum KV-SafeNet-Provider
[KBV_SNK_LFEX_Überprüfung_Provider]	Leitfaden Überprüfung Provider