Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Leitfaden Zertifizierung KV-Apps

[KBV_SNK_LFEX_Zert_KV-Apps]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	26.08.2016
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	26.08.2016	KBV	Finale Qualitätssicherung		
0.99	04.08.2016	KBV	Fachliche Finalisierung des Leitfadens		
0.91	25.07.2016	KBV	Überarbeitung		
0.9	18.07.2016	KBV	Einarbeitung von Kommentaren	Kommentierung im Referat SNK	
0.5	13.06.2016	KBV	Erweiterung		
0.2	06.06.2016	KBV	Überarbeitung		
0.1	29.05.2016	KBV	Initiale Erstellung		

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 (SNK).

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

Die Rechenzentren der 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.

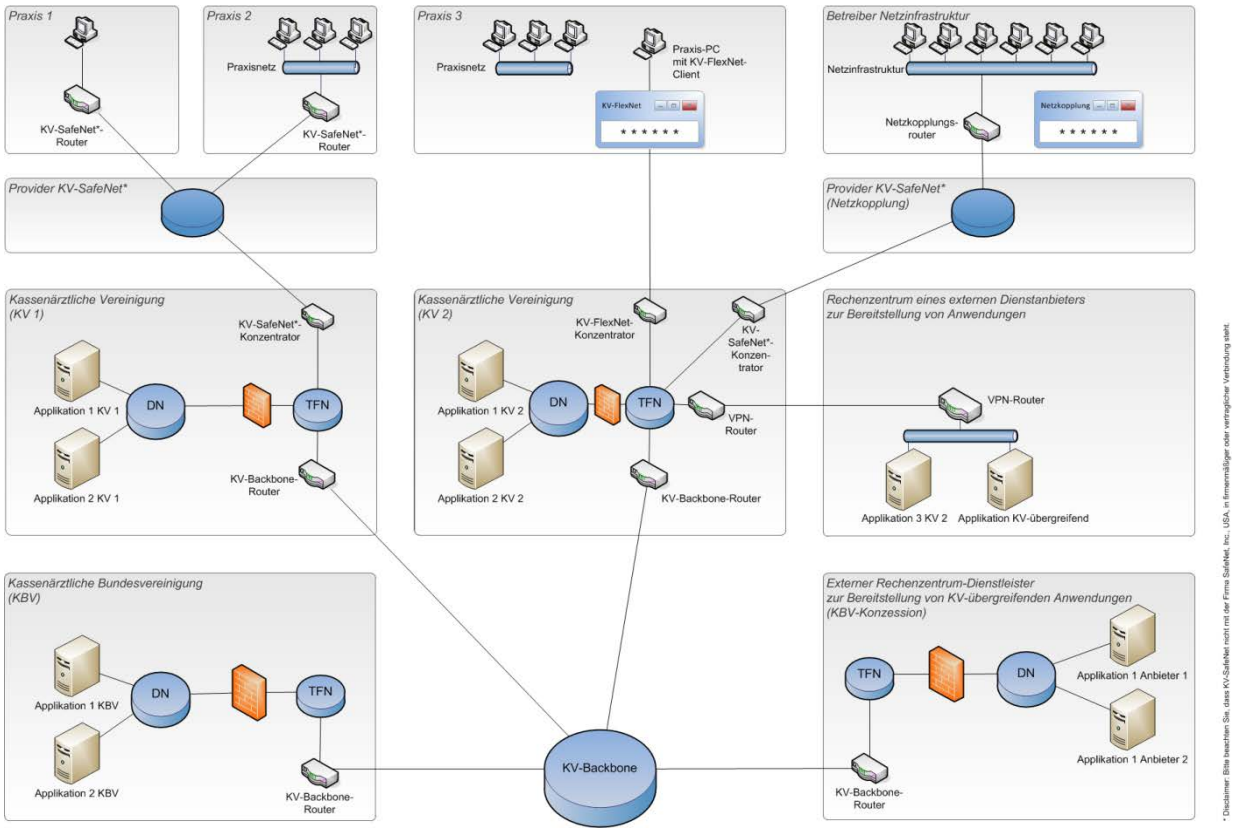

Abbildung 1: Beispielhafte Netztopologie

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 SNK. 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 Möglichkeiten 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 SNK.

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 SNK werden den Teilnehmern von den KVen und der KBV Dienste und Anwendungen zur Verfügung gestellt, die mit dem Begriff Applikationen (oder auch KV-Apps) zusammengefasst werden. 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 SNK mittels einer Hardware-VPN-Lösung zur Verfügung und garantiert für die Sicherheit dieser Verbindung. Der Provider stellt dem Teilnehmer hierzu einen KV-SafeNet-Router zur Verfügung.

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

Unabhängig von der Anbindungsart und der Authentisierung auf Netzwerkebene ist eine weiterführende Authentisierung auf Anwendungsebene durch den Arzt erforderlich. Aus Sicht des Arztes muss eine solche Authentisierung möglichst einfach sein: Egal wo er sich im SNK bei KV-seitigen Anwendungen anmeldet, tut er dies immer mit demselben Benutzernamen und Passwort.

1.2 Ziel des Dokuments

Der Leitfaden beschreibt den prozessualen Ablauf einer Zertifizierung von Applikationen im SNK. Hierfür werden die normativen Vorgaben der Richtlinie [KBV_SNK_RLEX_KV-Apps] 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. Anbieter einreichen muss, der an einem KV-Apps-Zertifizierungsverfahren teilnimmt.

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

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an Unternehmen und Organisationen, die einen Dienst im SNK betreiben 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-Apps-Anbieter 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 vier 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-Apps] ist der offizielle Antrag auf Zertifizierung bzw. Rezertifizierung zum KV-Apps-Anbieter. 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-Apps-Anbieter – ausgenommen das Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-Apps] und die Datenschutzerklärung – können per E-Mail an das Referat SNK/Prüfstelle der KBV (pruefstelle@kbv.de) gesandt werden.

Betreffzeile: „Antrag auf Zertifizierung zum KV-Apps-Anbieter“.

Das Referat SNK/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 €
Zertifizierung	**1.040,00**
Begehung des Rechenzentrums	**624,00**
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 SNK/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 SNK/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 SNK/Prüfstelle.
7. Änderungen bezüglich der Ansprechpartner für Teilnehmer oder die KBV können formlos via E-Mail angezeigt werden.

2.5 Vorbehalt

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

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

2.6 Erstzertifizierung

Der Antragsteller reicht den Antrag in Form des Formulars Ergänzende Erklärung [KBV_SNK_FOEX_KV-Apps] mit den in Kapitel 3 näher erläuterten Unterlagen ein (siehe auch Abs. 2.3). Alle erforderlichen Anforderungsdokumente können von dem Referat SNK/Prüfstelle (siehe Abs. 2.3) angefordert werden.

Nach Eingang aller Unterlagen wird das Referat SNK/Prüfstelle die Unterlagen auf Konformität zur aktuell gültigen Richtlinie [KBV_SNK_RLEX_KV-Apps] prüfen.

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

2.7 Rezertifizierung

Mindestens vier Monate vor Ablauf des derzeit gültigen Zertifikats müssen alle Dokumente und die Applikation durch das Referat SNK/Prüfstelle erfolgreich rezertifiziert sein, sofern die KV-Apps-Zertifizierung weiterhin bestehen soll. Der Anbieter muss hier, wie bei einer Erstzertifizierung, alle Unterlagen gemäß den Anforderungen der aktuell gültigen Richtlinie [KBV_SNK_RLEX_KV-Apps] 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 und die Unterlagen den Anforderungen der aktuellen Richtlinie [KBV_SNK_RLEX_KV-Apps] entsprechen.

Möchte der Anbieter sein Zertifikat an eine neue gültige Version der Richtlinie [KBV_SNK_RLEX_KV-Apps] anpassen, so hat er die Prüfung der Applikation erneut zu beantragen.

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

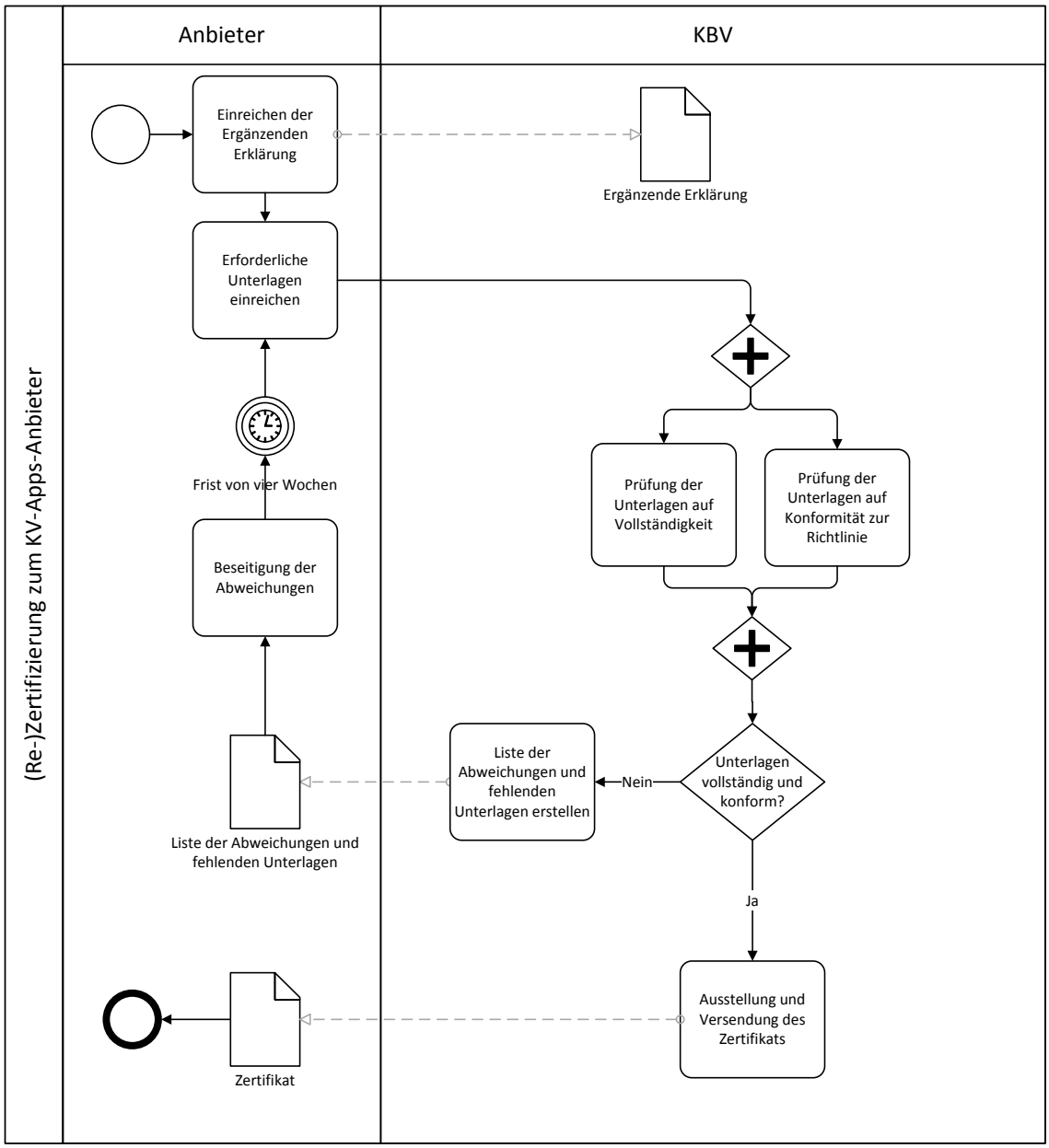

Abbildung 2: Vereinfachter Ablauf des Zertifizierungsverfahrens

3 Einzureichende Unterlagen

In diesem Dokument wird die sicherheitstechnische Zertifizierung einer Anwendung für den Betrieb im SNK erläutert. Hierfür werden zu den konkreten Anforderungen aus der Richtlinie [KBV_SNK_RLEX_KV-Apps] für die Umsetzung erklärt und (wenn möglich) Best-Practice-Ansätze vorgestellt.

Alle Angaben in diesem Dokument dienen lediglich zur Unterstützung einer Zertifizierung. Alle von der KBV als Hilfestellung bereitgestellten Dokumente garantieren nicht den erfolgreichen Abschluss eines Zertifizierungsverfahrens und erheben keinen Anspruch auf Vollständigkeit.

3.1 Ergänzende Erklärung

Anforderung

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

Erläuterung

Das Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-Apps] ist der offizielle Antrag auf Zertifizierung bzw. Rezertifizierung zum KV-Apps-Anbieter. Diese ist ausgefüllt und unterschrieben per Post oder Fax an das Referat SNK/Prüfstelle zu übermitteln.

Mit dem Formular Ergänzende Erklärung [KBV_SNK_FOEX_KV-Apps] stimmt der Antragsteller zu, dass er die aktuell gültige Richtlinie [KBV_SNK_RLEX_KV-Apps] und die darin referenzierten Dokumente ohne Einschränkungen anerkennt, sowie jegliche Änderungen, die für den Betrieb einer KV-App relevant sind, an das Referat SNK/Prüfstelle zu melden.

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 dem Referat SNK/Prüfstelle mitzuteilen, dass alle an der KV-Apps-Lösung beteiligten Mitarbeiter des Antragstellers nach Datengeheimnis § 5 Bundesdatenschutzgesetz (BDSG) verpflichtet wurden.

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.

3.3 Dokumente zur Informationssicherheit

Anforderung

Einreichung dokumentierter interner Regelungen zum Informationssicherheitsmanagement

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

Erläuterung

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

(1) Sicherheitsleitlinie und Organisation der Sicherheit
(2) Datenschutz, Vertraulichkeit und Zugangskontrolle
(3) Personalsicherheit
(4) Gebäude- und Arbeitsplatzsicherheit
(5) Management der Betriebs- und Kommunikationsprozesse
(6) Beschaffung, Entwicklung und Wartung
(7) Business Continuity Management (BCM)
(8) Management von Informationssicherheitsereignissen (Incident Management)
(9) Compliance

Weitere Informationen zu den Anforderungen an ein Informationssicherheitsmanagement sind der DIN-Norm ISO 27001 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-Apps] im Abschnitt 8.1

3.4 Diagramme der Betriebsprozesse

Anforderung

Beschreibung der folgenden Betriebsprozesse

(1) Prozess zur Provisionierung von Nutzern
(2) Prozess zur Rückabwicklung von Nutzern
(3) Übermittlung des techn. Berichtswesens inkl. Ausfälle an die KBV

Erläuterung

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.

zu (1) Provisionierung bezeichnet einen Prozess, der einen Anwender eines IT-Systems mit den grundsätzlichen Voraussetzungen für seine Tätigkeit ausstattet.

Ein Beispiel hierfür ist die Erstellung eines Benutzerkontos. Über das Benutzerkonto kann gesteuert werden, was ein Nutzer für Funktionen in einem IT-System nutzen kann.

zu (2): Rückabwicklung bezeichnet einen Prozess zur Beendigung der Nutzung einer Ap-

plikation durch Nutzer, die die Applikation nicht mehr nutzen möchten oder nicht mehr nutzen dürfen.

Ein Beispiel hierfür ist die endgültige Sperrung eines Benutzerkontos.

Richtlinienverweis

►Richtlinie [KBV_SNK_RLEX_KV-Apps] im Abschnitt 8.3

3.5 Supportkonzepte

Der Applikationsanbieter ist verantwortlich für die Bereitstellung des Supports für die Applikation.
Der Support umfasst sowohl die Behandlung von inhaltlichen Anfragen zur Applikation, als auch zur Meldung von technischen Störungen.
Der Applikationsanbieter stellt den Anwendern hierzu die Kontaktdaten (Ansprechpartner, Telefonnummer, Zeiten der Erreichbarkeit) zur Verfügung.

Für die Organisation und Leitung des Supports kann das Kapitel „Geeignetes Konzept für Personaleinsatz und -qualifizierung“ aus dem BSI Grundschutzkatalog (M 3.51) verwendet werden. Hier werden weiterführende Regelungen und Anforderungen an das Wartungs- und Administrationspersonal gestellt (M 3.11).

3.6 Berechtigungs- und Rollenkonzept

Dokumentation mit folgenden Mindestangaben:

(1) Angabe der existierenden Nutzerrollen inkl. der zugehörigen Berechtigungen

(2) Angaben zur Verwaltung der Zugangsdaten der Nutzer

Erläuterung

zu (1) Festlegung von Inhalt und Umfang einer Nutzerrolle mittels mehrerer Kriterien innerhalb eines Rollenmodells. Die zugehörigen Berechtigungen legen für die konkrete Nutzerrolle fest, in welchem Umfang eine Rolle eine Aktivität ausführen darf.

zu (2) Detailangaben zum Umgang mit den Nutzerdaten, wie werden bspw. die Passwörter abgelegt (Klartext/gehasht).

3.7 Datenhaltung und Datensicherung

Dokumentation mit folgenden Mindestangaben:

(1) Es ist sicherzustellen, dass die Daten der Applikationen in regelmäßigen Abständen gesichert werden und jederzeit vollständig wiederhergestellt werden können.

zu (1) Bei der Umsetzung können die Empfehlungen des BSI-Grundschutzkataloge des Bausteins B 1.4 „Datensicherungskonzept“ eine unterstützende Rolle spielen, insbesondere die Maßnahmen

- Entwicklung eines Datensicherungskonzeptes
- Festlegung der Verfahrensweise für die Datensicherung
- Dokumentation der Datensicherung
- Geeignete Aufbewahrung der Backup-Datenträger
- Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- Regelmäßige Datensicherung

sind zu beachten.

3.8 Dokumentation der Betriebsbasis

Anforderung

Dokumentation mit folgenden Mindestangaben:

(1) Angaben zur Betriebsumgebung der Applikation (Rechenzentrum)

(2) Technische Unterlagen oder Produktbeschreibungen (Produktblätter) der Betriebsbasis

(3) Vollständige Liste der verwendeten Dienste / Ports

(4) Erläuterung und Darstellung der eingesetzten Schutzmaßnahmen vor unbefugten Zugriffen (Applikation, Managementschnittstellen) - Erläuterungen zum Zugang und zur Absicherung der Managementschnittstelle

(5) Aufzählung und Beschreibung der verwendeten Management-Tools bzw. –Protokolle (SSH, etc.)

(6) Grafische Darstellung der Betriebsumgebung inkl. Firewalls, eingesetzter Server, Managementnetz inkl. Anbindungsweg (Netzplan), IP-Adressen

(7) Details zur Absicherung der „2-Bein-Strategie“

Erläuterung

Es müssen Unterlagen und Informationen bzgl. der Betriebsbasis eingereicht werden. Dies umfasst alles, was für den Betrieb der Applikation in Bezug auf eingesetzte Hard- und Software zum Einsatz kommt.

zu (2) Server, Firewalls, eingesetzte(s) Betriebssystem(e) und Härtung, eventuell zum Einsatz kommende 3rd-Party-Software

Firewall (bei „2-Bein-Strategie“, Angabe der FW-Policies, welche die Anforderungen aus (7) umsetzen)

zu (4): Die Erläuterung der Sicherungsmaßnahmen der Betriebsbasis umfasst das Deaktivieren nicht benötigter Dienste - insbesondere Dienste, wie telnet oder ftp - bzw. die Deaktivierung ungenutzter Ports. Absicherung von Managementschnittstellen bspw. durch Konfiguration von Zugriffssteuerungslisten (Access Control Lists) (siehe BSI-Maßnahmen M4.201 und M4.202).

Die Erläuterung zum Zugang und zur Absicherung der Managementschnittstellen soll folgende Mindestangaben umfassen:

a. Konfiguration des VPN-Tunnels (SSL/TLS oder IPsec), sofern verwendet

b. Aufzählung der verwendeten Verschlüsselungsverfahren insbesondere un-

ter Angabe der verwendeten Algorithmen zum Schlüsselaustausch und der Schlüssellängen der verwendeten symmetrischen Verfahren

zu (5): Die Aufzählung der verwendeten Management-Tools umfasst auch die Erwähnung der ggf. eingesetzten Fault- und Anti-Fraud-System-Tools.

zu (7): Grundsätzlich muss sichergestellt werden und vom Applikationsanbieter zugesichert werden, dass unter keinen Umständen

- ein unbefugter Zugriff auf die Applikation oder die Betriebsumgebung der Applikation aus einem anderen Netz erfolgen kann,
- ein über die Nutzung der Applikation hinausgehender Zugriff auf das SNK aus einem anderen Netz erfolgen kann und
- ein Teilnehmer über die Applikation oder die Betriebsumgebung der Applikation aus dem SNK in andere Netze gelangen kann bzw. Dienste, welche in anderen Netzen betrieben werden, nutzen kann.

Applikationen und Betriebsumgebungen, die ausschließlich für Teilnehmer im SNK bereitgestellt werden, dürfen keine direkte oder indirekte Verbindung zu anderen Netzen, z.B. dem Internet, haben.

Applikationen, die gleichzeitig sowohl Nutzern aus dem SNK als auch aus anderen Netzen bereitgestellt werden sollen, müssen eine strikte Trennung der beteiligten Netze nachweisen, um die weiter oben definierten Anforderungen dieses Kapitels umsetzen zu können.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-Apps] im Abschnitt 7

3.9 Format der kryptographischen Angaben

Anforderung

Dokumentation der Angaben zu eingesetzten Kryptographie Mechanismen, sofern diese verwendet werden[4]:

(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 o. ä. 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:

[4] In Anlehnung an die Techn. Richtlinien des BSI (TR-02102 – Kryptographische Verfahren: Empfehlungen und Schlüssellängen)

- 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)[5] entnommen werden.

Richtlinienverweis

► Richtlinie [KBV_SNK_RLEX_KV-Apps] im Abschnitt 7

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

4 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.
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 bereitge-stellte 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.

5 Referenzierte Dokumente

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

Referenz	Dokument
[KBV_SNK_RLEX_KV-Apps]	Richtlinie KV-Apps