KBV

KASSENÄRZTLICHE
BUNDESVEREINIGUNG

RICHTLINIE KV-SAFENET (NETZKOPPLUNG)

[KBV_SNK_RLEX_NETZKOPPLUNG]

KASSENÄRZTLICHE BUNDESVEREINIGUNG

DEZERNAT DIGITALISIERUNG UND IT

15. MAI 2020

VERSION: 1.1

INHALT

DOKUMENTENHISTORIE UND KENNZEICHNUNG

KENNZEICHNUNG: **ÖFFENTLICH**

STATUS: **IN KRAFT**

GÜLTIG AB: **12. JUNI 2020**

Version	Datum	Autor	Änderung	Begründung	Seite
1.1	15.05.2020	KBV	Aktualisierung der Richtlinie	Anwendung neues Corporate Design der KBV, Entfernung der monatlichen Berichtspflicht, Entfernung Anhänge sowie Notwendigkeit der Vertragsprüfung, Anpassungen aufgrund TI-Verfügbarkeit sowie BSI-Vorgaben, Entfernung von Vorgaben, die bereits durch die Richtlinie KV-SafeNet geregelt sind	Alle

1 PRÄAMBEL

1.1 DAS SICHERE NETZ DER KVEN

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

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

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

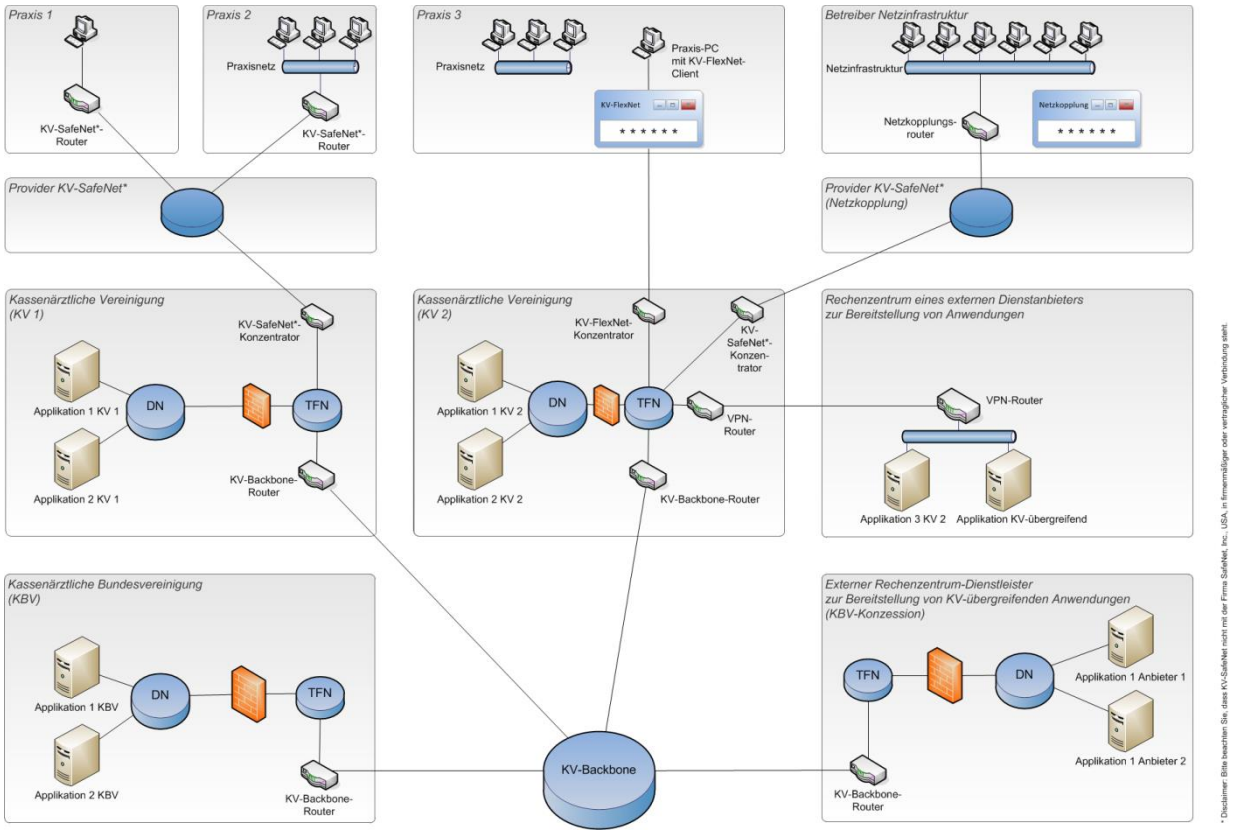

Abbildung 1: Beispielhafte Netztopologie

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

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

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

Im SNK werden den Teilnehmern von den KVen und der KBV, Dienste und Anwendungen zur Verfügung gestellt, die mit dem Begriff Applikationen (oder auch KV-Apps) zusammengefasst werden.

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

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

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

Die Richtlinie KV-SafeNet (Netzkopplung) beschreibt die Bedingungen für den gesicherten Anschluss von Teilnehmern aus bereits in sich abgesicherten gesundheitsmedizinischen Netzinfrastrukturen an das SNK.

Hierzu werden eine gesicherte Verbindung zwischen den Teilnehmern der anzubindenden Netzinfrastruktur, dem Provider sowie der KV und zudem die Bedingungen für die Zertifizierung eines Providers beschrieben. Die gesicherte Verbindung basiert auf der sicheren Hardware-VPN-Lösung KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] und erweitert diese um einen Authentisierungsdienst sowie um die hierfür notwendigen regulatorischen Maßnahmen. Diese Richtlinie bildet die Grundlage für die Zertifizierung von Providern.

1.3 KLASSIFIZIERUNG UND ADRESSATEN DES DOKUMENTS

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich an alle am SNK beteiligten Akteure, insbesondere an bereits zertifizierte KV-SafeNet-Provider, die sich zusätzlich für die Durchführung von Netzkopplungen zertifizieren lassen 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 GÜLTIGKEIT, ANWENDUNGSBEREICH UND ABGRENZUNG

Die Richtlinie KV-SafeNet (Netzkopplung) ist gültig für den Anschluss von Teilnehmern aus anderen, bereits in sich abgesicherten Netzinfrastrukturen des gesundheitsmedizinischen Betriebes der Bundesrepublik Deutschland, z. B. für den Anschluss verschiedener Teilnetze und einzelner oder mehrerer Standorte einer Organisation an das SNK.

Diese Fassung der Richtlinie KV-SafeNet (Netzkopplung) ist ausschließlich gültig und zwingend anzuwenden für den Anschluss von berechtigten Teilnehmern aus Krankenhäusern und Krankenhaus- bzw. Klinikketten an das SNK.

Diese Richtlinie ist nicht gültig und nicht anzuwenden für den Anschluss von Teilnehmern aus dem Internet oder aus Netzwerken außerhalb des gesundheitsmedizinischen Betriebes an das SNK.

Mit Inkrafttreten dieses Dokumentes ist ein Anschluss großer Netzinfrastrukturen ausschließlich nach den Maßgaben dieser Richtlinie zulässig.

3 ANWENDUNG DER RICHTLINIE KV-SAFENET

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

4 GRUNDLEGENDES VORGEHEN UND VERANTWORTLICHKEITEN

In diesem Kapitel wird das grundlegende Vorgehen bei der Durchführung der Netzkopplung umrissen, welches im Anschluss detailliert wird.

Unter Netzkopplung wird der Anschluss von Teilnehmern aus bereits in sich abgesicherten, größeren gesundheitsmedizinischen Netzinfrastrukturen an das SNK verstanden. Ein durch die KBV zertifizierter Provider stellt dem Betreiber der angeschlossenen Netzinfrastruktur alle technischen Voraussetzungen zur Anbindung an das SNK bereit. Die Anbindung erfolgt mittels einer auf der Anbindungsvariante KV-SafeNet basierenden Hardware-VPN-Lösung. Der Provider stellt dem Betreiber der anzuschließenden Netzinfrastruktur hierzu einen Netzkopplungsrouter zur Verfügung. Jeder Teilnehmer muss sich vor dem Zugang zum SNK mit einer persönlichen Kennung am Netzkopplungsrouter authentisieren.

Mit dem Begriff Betreiber der angeschlossenen Netzinfrastruktur ist immer die verantwortliche Institution gemeint, unabhängig davon, ob die Institution den Betrieb selbst durchführt oder diesen an andere Unternehmen ausgelagert hat.

Ein für die Netzkopplung zertifizierter Provider richtet auf Antrag eines Betreibers einer anzuschließenden Netzinfrastruktur eine gesicherte Verbindung zum SNK ein, um den Teilnehmern aus der anzuschließenden Netzinfrastruktur Zugang zu den dort bereitgestellten Applikationen zu ermöglichen.

Im Rahmen der Netzkopplung muss die KV, in deren Gebiet der Anschluss erfolgen soll, gegenüber dem Provider die Zulassung des Anschlusses des Betreibers einer Netzinfrastruktur an das SNK bestätigen und spricht damit eine Genehmigung für die Organisationseinheit aus.

Der Betreiber einer anzuschließenden Netzinfrastruktur schließt mit dem Provider einen Vertrag, der den in seinem Netz befindlichen Teilnehmern einen Zugang zum SNK ermöglicht.

Der Netzkopplungsrouter stellt die Funktionalität eines KV-SafeNet-Routers sowie einen Authentisierungsdienst bereit. Zusätzlich zur Routing-Funktionalität ermöglicht der Netzkopplungsrouter damit die eindeutige Identifizierung und personenbezogene Authentisierung der Teilnehmer.

Der Betreiber einer anzuschließenden Netzinfrastruktur benennt dem Provider die Teilnehmer, die Zugang zum SNK erhalten sollen. Der Provider ermöglicht diesen berechtigten Teilnehmern den Zugang zum SNK. Der Provider teilt allen betreffenden KVen mit, welche Teilnehmer aus dem entsprechenden KV-Gebiet eingerichtet werden. Die KBV/KVen haben hierbei ein rückwirkendes Einsichtnahme- und Vetorecht für einzelne Teilnehmer.

Die Teilnehmer müssen sich bei jedem Zugang zum SNK am Netzkopplungsrouter mit einer persönlichen Teilnehmerkennung (z. B. Nutzername und Passwort) authentisieren. Eine eindeutige Identifikation des Teilnehmers durch den Netzkopplungsrouter muss sichergestellt werden.

5 ZERTIFIKAT

Das Zertifikat bescheinigt dem Provider, dass seine Anbindung den Bestimmungen dieser Richtlinie erfüllt.

Die in den folgenden Abschnitten definierten Anforderungen müssen für die Erlangung und die Aufrechterhaltung des Zertifikates zur Durchführung der Netzkopplung erfüllt sein.

Zusätzlich sind folgende Anforderungen aus der gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] zu erfüllen:

- Überprüfung [KBV_SNK_LFEX_Überprüfung_Provider]
- Bereitstellung der Hardware
- Änderung der Zugangskomponenten
- Einzureichende Unterlagen
- Änderungen der Richtlinie
- Rezertifizierung
- Entzug des Zertifikates
- Haftungsausschluss der KVen und der KBV

5.1 VORAUSSETZUNGEN FÜR DIE ZERTIFIZIERUNG

Voraussetzung für die Erlangung des Zertifikates zur Durchführung der Netzkopplung ist ein gültiges Zertifikat des Providers entsprechend der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet].

5.2 ZERTIFIZIERUNG

Mit dem Antrag auf eine Zertifizierung verpflichtet sich der Provider zur Einhaltung der Maßgaben dieser Richtlinie. Die Zertifizierung erfolgt durch die KBV anhand des Leitfadens zur Zertifizierung Netzkopplungsprovider [KBV_SNK_LFEX_Zert_Netzkopplung]. Die Gebühren der Zertifizierung trägt der Provider. Ausschließlich zertifizierte Provider erhalten die Möglichkeit zur Anbindung von Teilnehmern an das SNK und können die Anbindung einer anzuschließenden Netzinfrastruktur realisieren.

Für die Zertifizierung zur Durchführung der Netzkopplung wird die zum Zeitpunkt der Zertifizierung geltende Fassung der Richtlinie KV-SafeNet zugrunde gelegt.

5.3 BEREITSTELLUNG DER HARDWARE

Der Provider stellt der KBV zu Zertifizierungszwecken je einen als Netzkopplungsrouter einzusetzenden Gerätetyp zur Verfügung.

Der Provider ist verpflichtet, die notwendigen Maßnahmen zu ergreifen, um zu Überprüfungszwecken innerhalb von zehn Werktagen jeden zertifizierten und im Einsatz befindlichen Gerätetyp der KBV im vollständig konfigurierten Zustand zur Verfügung zu stellen.

Für die Laufzeit des Zertifikates verbleibt kein Netzkopplungsrouter bei der KBV.

5.4 ZERTIFIKATSLAUFZEIT

Das Zertifikat zur Bereitstellung der Netzkopplung ist an die Laufzeit des zugrundeliegenden KV-SafeNet-Zertifikates gebunden. Es erlischt, wenn das als Voraussetzung dieser Zertifizierung zugrundeliegende KV-SafeNet-Zertifikat erloschen ist.

5.5 ZULASSUNGSFÄHIGE LÖSUNGEN

In Abhängigkeit von den zu nutzenden Anwendungen und von der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur sind verschiedene Lösungskonzepte jeweils separat zulassungsfähig.

Der Provider erhält die Zertifizierung ausschließlich für das eingereichte Konzept und die darin spezifizierte Lösung. Der Provider muss mindestens die in 7.1 „Basisanforderungen“ definierten Regelungen umsetzen und kann ergänzend die in 7.2 „Optionale Anforderungen“ definierten Regelungen umsetzen.

Das Zertifikat berechtigt den Provider zum Anschluss von Betreibern von Netzinfrastrukturen ausschließlich mittels des zugelassenen Konzeptes.

6 ANFORDERUNGEN AN DEN NETZKOPPLUNGSVERTRAG

Die in den folgenden Abschnitten definierten Anforderungen müssen im Netzkopplungsvertrag berücksichtigt sein.

Die Regelungen der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] bezüglich des Teilnehmervertrages beziehen sich auf das zwischen Teilnehmer und Provider geschlossene Vertragsverhältnis. Diese Regelungen sind äquivalent auf den zwischen Betreiber der anzubindenden Netzinfrastruktur und Provider zu schließenden Netzkopplungsvertrag umzusetzen.

Folgende Anforderungen der Richtlinie KV-SafeNet sind umzusetzen.

- Außerordentliche Kündigung,
- Beendigung des Vertragsverhältnisses,
- Transparenz des Angebotes,
- Bereitstellungszeitraum des Zugangs,
- Teilnehmersupport des Anbieters,
- Servicezeiten und
- Vertragsstrafe

sind daher entsprechend im Netzkopplungsvertrag zu berücksichtigen.

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in den folgenden Abschnitten definiert.

6.1 VERTRAGSPARTNER

Vertragspartner des Providers bei der Leistungserbringung ist ausschließlich der Betreiber der anzuschließenden Netzinfrastruktur.

Teilnehmer und Provider gehen kein unmittelbares Vertragsverhältnis ein.

6.2 VERTRAGSVORAUSSETZUNG

Voraussetzung für die Wirksamkeit des Vertrages zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider ist die Zulassung des Betreibers der anzuschließenden Netzinfrastruktur als Organisationseinheit zum SNK durch die jeweils zuständige KV. Die zuständige KV ist die, in deren Gebiet der Anschluss an das SNK erfolgen soll. Im Allgemeinen ist das die KV, in deren Gebiet sich der Netzkopplungsrouter des Betreibers der anzuschließenden Netzinfrastruktur befindet.

Die Zulassung eines Teilnehmers kann auch durch die KBV erfolgen.

Der Provider informiert den Vertragspartner über das Zertifikat und die entsprechende Zertifikatslaufzeit. Der Provider garantiert dem Teilnehmer die Bereitstellung eines Zugangs zum SNK.

6.3 NUTZUNG DES ZUGANGS ZUM SNK

Teilnehmer aus der angeschlossenen Netzinfrastruktur erhalten einen zweckgebundenen Zugang zum SNK und den dort angebotenen Diensten.

Es ist dem Betreiber der angeschlossenen Netzinfrastruktur untersagt, den KV-Backbone zur internen Vernetzung oder zur Vernetzung mit weiteren Netzinfrastrukturen anderer Organisationen zu nutzen.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine diesbezügliche Regelung beinhalten.

6.4 BENENNUNG DER BERECHTIGTEN TEILNEHMER

Der Betreiber der anzuschließenden Netzinfrastruktur benennt dem Provider die berechtigten Teilnehmer seiner Organisationseinheit und haftet für die Richtigkeit der Angaben. Die Benennung erfolgt mit folgenden Pflichtangaben:

- Nutzername
- Nachname und Vorname des Teilnehmers
- Gebiet der KV-Zugehörigkeit des Teilnehmers

Folgende weitere Angaben sollen gemacht werden:

- Lebenslange Arztnummer (LANR) des Teilnehmers
- Betriebsstättennummer (BSNR) des Teilnehmers

Berechtigte Teilnehmer sind die Mitglieder der KVen sowie ggf. Teilnehmer, die Dienste der KVen nutzen möchten.

Teilnehmer können nur natürliche Personen sein, Gruppenberechtigungen sind nicht zulässig.

Der Provider gewährt ausschließlich den benannten berechtigten Teilnehmern Zugang zum SNK, eine explizite Bestätigung einzelner Teilnehmer durch KVen ist nicht notwendig.

Der Betreiber der anzuschließenden Netzinfrastruktur muss Änderungen der benannten Teilnehmer, z. B. wegen Kündigung des Arbeitsverhältnisses eines Teilnehmers, unverzüglich dem Provider mitteilen, der diese Änderungen wiederum unverzüglich umsetzen muss.

6.5 KONTROLLRECHT UND VORBEHALT DER KVEN/KBV BEZÜGLICH DER TEILNEHMER

Die KVen haben die Pflicht, den Teilnehmerkreis zu kontrollieren und zu bestimmen.

Hierzu teilt der Provider allen betreffenden KVen mit, welche Teilnehmer aus dem jeweiligen KV-Gebiet auf dem Netzkopplungsrouter eingerichtet werden. Die KVen können innerhalb der Frist von drei Arbeitstagen ein Vetorecht für einzelne Teilnehmer ausüben. Nach Ablauf der Frist richtet der Provider die Teilnehmerberechtigungen auf dem Netzkopplungsrouter ein.

Weiterhin behalten sich die KVen und die KBV das Recht vor, Einsicht in die auf dem Netzkopplungsrouter eingerichteten Teilnehmer zu bekommen und ggf. auch zu einem späteren Zeitpunkt ein Vetorecht gegenüber einzelnen Teilnehmern auszuüben. Der Provider muss die betroffenen Teilnehmer unverzüglich deaktivieren.

6.6 AUTHENTISIERUNG DER TEILNEHMER FÜR DEN ZUGANG ZUM SNK

Der Zugang eines Teilnehmers zum SNK wird durch eine Authentisierung des Teilnehmers am Netzkopplungsrouter abgesichert. Nur erfolgreich authentisierte Teilnehmer erhalten Zugang zum SNK.

Jeder berechtigte Teilnehmer erhält hierzu eine persönliche Teilnehmerkennung. Diese Teilnehmerkennungen dürfen nicht an andere Teilnehmer weitergegeben oder anderweitig missbraucht werden.

Die Teilnehmerkennungen werden ausschließlich vom Provider eingerichtet und gepflegt, der Betreiber der anzuschließenden Netzinfrastruktur hat keinen Zugriff auf die Teilnehmerkennungen.

6.7 PROTOKOLLIERUNG DER TEILNEHMERZUGRIFFE

Teilnehmerzugriffe auf das SNK sind im rechtmäßigen Rahmen zu protokollieren. Änderungen der gesetzlichen Vorgaben müssen vom Provider unverzüglich umgesetzt werden.

6.8 PFLICHTEN DES BETREIBERS DER ANZUSCHLIEßENDEN NETZINFRASTRUKTUR UND DER DARIN BEFINDLICHEN TEILNEHMER

Aufgrund des erhöhten Sicherheitsbedarfs beim Anschluss von Teilnehmern an das SNK müssen die Betreiber der angeschlossenen Netzinfrastruktur eine dem Stand der Technik entsprechende Umsetzung des Datenschutzes und Datensicherheit gewährleisten. Der Stand der Technik wird durch die aktuellen Maßnahmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) definiert.

Der Betreiber der anzuschließenden Netzinfrastruktur verpflichtet sich gegenüber dem Provider zur Einhaltung der Regelungen dieses Abschnittes.

Der Betreiber der anzuschließenden Netzinfrastruktur muss die Kenntnisnahme der in diesem Abschnitt festgelegten Sicherheitshinweise schriftlich im Vertrag bestätigen. Weiterhin muss er bestätigen, dass die über seine Netzinfrastruktur angeschlossenen Teilnehmer die Sicherheitshinweise zur Kenntnis genommen haben bzw. zur Kenntnis nehmen werden, sobald die Anbindung der Teilnehmer erfolgt.

6.8.1 PC-Arbeitsplätze

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

- Der PC-Arbeitsplatz muss dem aktuellen Stand der Technik entsprechen und insbesondere aktuelle Versionen von Betriebssystemen, Antiviren-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.
- 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 abgesicherte Verbindung des PC-Arbeitsplatzes mit dem Internet über die Netzinfrastruktur des Betreibers ist erlaubt.
- Die Räumlichkeit des PC-Arbeitsplatzes muss so gestaltet sein, dass unbefugte Personen keinen Zugriff auf den Arbeitsplatz erlangen können.

6.9 VORBEHALT DER KV/KBV BEZÜGLICH MISSBRAUCH DER ANBINDUNG

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

6.10 VERFÜGBARKEIT

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss eine Regelung beinhalten, die die Verfügbarkeit der Anbindung der anzuschließenden Netzinfrastruktur an das SNK definiert.

6.11 AUFSTELLUNG UND PHYSIKALISCHE ABSICHERUNG DES NETZKOPPLUNGSROUTERS

Der Netzkopplungsrouter bzw. die einzelnen Komponenten des Netzkopplungsrouters werden vom Provider bereitgestellt.

Die einzelnen Komponenten des Netzkopplungsrouters müssen physikalisch gegen unbefugten Zugang gesichert werden, z. B. durch Aufbewahrung in einem gesicherten Rechenzentrum.

Der Vertrag zwischen dem Betreiber der anzuschließenden Netzinfrastruktur und dem Provider muss diesbezügliche Regelungen beinhalten.

7 TECHNISCHE ANFORDERUNGEN AN DEN PROVIDER

Die in der aktuell gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] definierten Regelungen bezüglich der technischen Anforderungen an den Provider sind entsprechend für die Richtlinie KV-SafeNet (Netzkopplung) gültig:

- Nutzung des KV-Backbones
- Einschränkung der Nutzung
- Deaktivierung ungenutzter Ports
- Routing
- DNS
- Sichtbarkeit
- Sicherheit der Zugangsdaten
- Überwachungsmaßnahmen des Providers
- Betriebszeit und Verfügbarkeit

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in diesem Kapitel definiert.

7.1 BASISANFORDERUNGEN

7.1.1 VPN-Konzentrator

Bereits im Rahmen einer Zertifizierung nach Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] installierte VPN-Konzentratoren dürfen zur Durchführung der Netzkopplung genutzt werden.

7.1.2 Netzkopplungsrouter

Der Netzkopplungsrouter besteht technisch aus der Router-Komponente und einer Authentisierungskomponente.

Der Netzkopplungsrouter wird vom Provider bereitgestellt. Falls sich der Netzkopplungsrouter aus einzelnen Komponenten zusammensetzt, ist der Provider für die Bereitstellung der einzelnen Komponenten verantwortlich.

Die Gesamtkonstruktion des Netzkopplungsrouters soll aus Gründen der Wartbarkeit aus möglichst wenigen physischen Komponenten bestehen.

7.1.2.1 Identifizierbarkeit der Zugriffe

Zugriffe auf das SNK müssen eindeutig identifizierbar sein. Die Identifizierbarkeit muss sowohl auf Ebene des Netzkopplungsrouters als auch auf Ebene der Teilnehmer gewährleistet sein.

Jeder Netzkopplungsrouter muss im SNK durch eine eindeutige, feste IP-Adresse adressierbar und identifizierbar sein.

Die Teilnehmer müssen eindeutig anhand persönlicher Merkmale (z. B. einer Teilnehmerkennung) am Netzkopplungsrouter identifizierbar sein.

Das Konzept zur Umsetzung der Anforderung obliegt dem Provider und ist im Rahmen der Zertifizierung vorzulegen.

7.1.2.2 Adressierung des Netzkopplungsrouters

Abweichend von den Regelungen der zum Zeitpunkt der Zertifizierung gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] wird jedem Netzkopplungsrouter eine feste IP-Adresse zugeordnet, die dynamische Adressvergabe ist für Netzkopplungsrouter nicht zulässig.

7.1.2.3 Authentisierung der Teilnehmer

Jeder Zugang eines Teilnehmers zum SNK wird durch eine Authentisierung des Teilnehmers am Netzkopplungsrouter abgesichert. Der Provider stellt die notwendigen Komponenten eines Authentisierungs- und Verzeichnisdienstes bereit, der ausschließlich vom Provider betrieben wird. Nur erfolgreich authentisierte Teilnehmer erhalten Zugang zum SNK. Die Authentisierung ist ausschließlich für den Teilnehmer gültig.

Jeder berechtigte Teilnehmer erhält hierfür eine persönliche Teilnehmerkennung. Teilnehmerkennungen dürfen nicht an andere Teilnehmer weitergegeben oder anderweitig missbraucht werden. Gruppenaccounts sind nicht zulässig.

Für jede Teilnehmerkennung müssen zusätzlich zum Berechtigungsnachweis die im Abschnitt 6.4 „Benennung der berechtigten Teilnehmer“ genannten Attribute im Netzkopplungsrouter eingerichtet werden.

Die Authentisierung eines Teilnehmers muss vor der Übertragung von Nutzdaten erfolgen. Erst nach erfolgreicher Authentisierung eines Teilnehmers erfolgt die Übertragung von Nutzdaten in das SNK. Die Authentisierung ist für die Dauer der Verbindung gültig, eine nochmalige Authentisierung ist nicht notwendig.

Nach einer Inaktivität von zwei Stunden muss die Verbindung automatisch vom Netzkopplungsrouter beendet werden.

Eine mehrfache gleichzeitige Anmeldung derselben Benutzerkennung muss durch geeignete Maßnahmen verhindert werden, ein Teilnehmer kann nur eine aktive Verbindung haben.

Die Teilnehmerkennungen werden ausschließlich durch den Provider eingerichtet, geändert, deaktiviert oder gelöscht.

Der Berechtigungsnachweis (z. B. das Passwort) wird ausschließlich durch den Provider erstmalig erzeugt und kann nur durch den Provider oder durch den jeweiligen Teilnehmer (z. B. bei Änderung des eigenen Passwortes) geändert werden. Die erstmalige Übermittlung des Berechtigungsnachweises an den Teilnehmer muss auf vertraulichem Weg, z. B. verschlüsselte E-Mail, postalisch per Brief oder persönlich (d. h. nicht telefonisch) erfolgen.

Im Falle der Verwendung von Passwörtern ist nach der ersten Anmeldung am Netzkopplungsrouter eine Änderung des Passwortes durch den Teilnehmer zwingend notwendig.

Der Betreiber der anzuschließenden Netzinfrastruktur hat keinen administrativen Zugang zum Authentisierungs- und Verzeichnisdienst.

Es muss eine anerkannte und sichere Authentisierungs-Lösung eingebunden werden. Diese muss dem Stand der Technik entsprechen und soll den vom BSI herausgegebenen Maßnahmen (geeignete Auswahl von Authentifikationsmechanismen) entsprechen. Zugelassene Authentisierungsmechanismen sind Passwörter, Zugangskarten und biometrische Techniken. Eine ergänzende Zwei-Faktor-Authentisierung ist möglich.

Bei einem erfolglosen Authentisierungsversuch darf dem Teilnehmer kein Hinweis darauf gegeben werden, ob die Kennung des Teilnehmers überhaupt im System vorhanden ist. Dem Teilnehmer muss eine Meldung wie z. B. „Name und/oder Passwort fehlerhaft“ angezeigt werden.

Nach einer vorgegebenen Anzahl erfolgloser Authentisierungsversuche muss die betroffene Benutzerkennung gesperrt werden oder es muss jeder weitere Authentisierungsversuch zeitlich zunehmend verzögert werden.

Die Entsperrung kann entweder durch den Provider erfolgen oder durch den Teilnehmer.

Wenn die Entsperrung durch den Provider vorgenommen wird, muss der Prozess der Erzeugung und Versendung der Berechtigungsnachweise äquivalent zum initialen Prozess durchgeführt werden.

Wenn die Entsperrung durch den Teilnehmer vorgenommen wird, müssen als gesonderter Prozess der Authentisierung weitere Benutzerdaten abgefragt werden. Die abzufragenden Benutzerdaten dürfen nicht leicht ableitbar sein (z. B. Name des Teilnehmers, Geburtsdatum).

Wiederholte fehlerhafte Passworteingaben für eine Benutzerkennung oder unzulässige Verbindungsversuche sollen zu einer unverzüglichen Warnung des Systems an den Provider führen. Die Schwellwerte hierzu sind im Rahmen eines Incident Management Systems des Providers vom Provider selbständig festzulegen und entsprechende Maßnahmen zu treffen. Dies ist im Rahmen der Zertifizierung nachzuweisen.

Änderungen an Benutzerdaten und Berechtigungsnachweisen sind durch den Verzeichnisdienst zu protokollieren.

7.1.2.4 Protokollierung der Teilnehmerzugriffe

Teilnehmerzugriffe auf das SNK sind im rechtmäßigen Rahmen zu protokollieren. Änderungen der gesetzlichen Vorgaben müssen vom Provider unverzüglich umgesetzt werden.

Die folgenden Absätze dieses Abschnittes sind im Rahmen der rechtmäßigen Protokollierung der Teilnehmerzugänge umzusetzen.

Für jeden erfolgreichen Verbindungsaufbau und -abbau und für jeden abgewiesenen Verbindungsaufbau muss eine Protokollierung vorgenommen werden.

Zu protokollieren sind:

- das identifizierende Merkmal des Teilnehmers, z. B. die Teilnehmerkennung
- Datum und Zeit des Verbindungsaufbaus, sowie die Verbindungsdauer

Die eingesetzten Verfahren zur Protokollierung müssen dem Stand der Technik entsprechen und können den vom BSI herausgegebenen Maßnahmen (Protokollierung der Sicherheitsgateway-Aktivitäten) entnommen werden.

7.1.2.5 Verschlüsselung

Die Verbindung zwischen Netzkopplungsrouter und VPN-Konzentrator muss durch einen verschlüsselten Hardware-VPN-Tunnel äquivalent zum KV-SafeNet-Anschluss geschützt sein. Das Verschlüsselungsverfahren hat dabei dem Stand der Technik zu entsprechen.

Ergänzend gilt folgende Regelung:

Die von den Teilnehmern übermittelten Daten zur Authentisierung müssen vor einem Zugriff Dritter durch eine Verschlüsselung geschützt sein.

7.1.3 Datendurchleitung und zu unterstützende Protokolle

Der Netzkopplungsrouter muss sicherstellen, dass die zwischen dem PC-Arbeitsplatz und den Anwendungen im SNK stattfindende Datenkommunikation mindestens für Webanwendungen mit den Protokollen HTTP und HTTPS unterstützt wird. Eine SSL/TLS-Verschlüsselung zwischen dem PC- Arbeitsplatz und den Anwendungen im SNK darf hierbei nicht aufgebrochen werden.

7.1.4 Verhinderung des Zugriffes von nicht berechtigten Netzwerken

Es muss technisch und organisatorisch sichergestellt werden, dass ausschließlich Personen aus der Organisation bzw. Institution des Betreibers der anzuschließenden Netzinfrastruktur Zugang zum Netzkopplungsrouter erlangen können. Personen außerhalb der Organisation, z. B. aus anderen angeschlossenen Netzinfrastrukturen oder außerhalb des Gebietes der Bundesrepublik Deutschland, dürfen keinen Zugang zum Netzkopplungsrouter erhalten.

Das erfolgt mittels einer Zugriffssteuerungsliste (Access Control List) auf dem Netzkopplungsrouter. Der Betreiber der angeschlossenen Netzinfrastruktur benennt dem Provider die erlaubten Netzwerke bzw. Netzbereiche, der Provider richtet die Regeln entsprechend im Netzkopplungsrouter ein.

7.1.5 Unbefugter Zugriff

Die bezüglich unbefugter Zugriffe definierten Regelungen der zum Zeitpunkt der Zertifizierung gültigen Fassung der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet], gelten entsprechend auch für die Richtlinie KV-SafeNet (Netzkopplung). Das in der Richtlinie KV-SafeNet definierte Teilnehmernetz entspricht im Rahmen der Netzkopplung der angeschlossenen Netzinfrastruktur. Die Regelungen sind äquivalent umzusetzen.

7.1.6 Betrieb und Standort des Netzkopplungsrouters

Der Netzkopplungsrouter bzw. die einzelnen Komponenten des Netzkopplungsrouters dürfen ausschließlich durch den Provider betrieben werden.

Die Routing-Komponente darf ausschließlich innerhalb der angeschlossenen Netzinfrastruktur betrieben werden.

Der Authentisierungs- und Verzeichnisdienst darf betrieben werden:

- innerhalb der angeschlossenen Netzinfrastruktur als separate Komponente
- innerhalb der angeschlossenen Netzinfrastruktur als gemeinsame Komponente mit der Routing-Komponente
- als separate Komponente im Providernetz

Der Authentisierungs- und Verzeichnisdienst darf nicht innerhalb des KV-Backbones, dem Transfernetz oder dem Dienstnetz betrieben werden.

Der Authentisierungs- und Verzeichnisdienst kann für jede angeschlossene Netzinfrastruktur separat oder zentral betrieben werden.

In jedem Fall hat der Provider sicherzustellen, dass die Kennungen der Teilnehmer einer angeschlossenen Netzinfrastruktur gegen Zugriffe von nicht berechtigten Teilnehmern aus anderen angeschlossenen Netzinfrastrukturen abgesichert sind.

7.2 OPTIONALE ANFORDERUNGEN

Ein zur Zertifizierung eingereichtes Konzept muss mindestens die Basisanforderungen des Abschnitts 7.1 erfüllen.
In Abhängigkeit von den zu nutzenden Anwendungen und von der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur sind verschiedene Lösungskonzepte separat zertifizierungsfähig. Dieser Abschnitt beschreibt spezifische Anforderungen, die in Abhängigkeit von den zu nutzenden Anwendungen und der IT-Infrastruktur des Betreibers der anzuschließenden Netzinfrastruktur optional umzusetzen sind.

7.2.1 Datendurchleitung und zu unterstützende Protokolle

Zusätzlich zu den in den Basisanforderungen definierten und zwingend zu unterstützenden Protokollen kann der Netzkopplungsrouter weitere Protokolle unterstützen, z. B. FTP, SMTP, Pop3, IMAP usw. oder auch proprietäre Protokolle spezifischer Anwendungen mit auf dem PC-Arbeitsplatz installierten Client-Komponenten.
Die Datendurchleitung ist aus Teilnehmer- und Applikationssicht transparent.

7.2.2 Terminalserver-Umgebungen

Im Falle des Einsatzes von Multi-User-Umgebungen (z. B. Terminalserver) auf Seiten des Betreibers der anzuschließenden Netzinfrastruktur muss das zur Zertifizierung eingereichte Konzept zwingend sicherstellen, dass Teilnehmer auf Basis von Teilnehmersitzungen und nicht ausschließlich auf Basis von IP-Adressen am Netzkopplungsrouter authentisiert werden.

8 ORGANISATORISCHE ANFORDERUNGEN AN DEN PROVIDER

Die folgenden, in der aktuell gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] definierten Regelungen bezüglich der organisatorischen Anforderungen an den Provider sind entsprechend für die Richtlinie KV-SafeNet (Netzkopplung) gültig:

- Mindestumfang des Angebotes
- Transparenz des Angebotes
- Installation und Betrieb
- Support und Wartung
- Ausschluss des Supports durch die KV/KBV
- Sicherheit der Zugangsdaten
- Teststellungen der angebotenen Anbindungsvarianten
- Missbrauch der Anbindung
- Vorbehalt bei übermäßiger Belastung des KV-Backbones

Notwendige Ergänzungen oder Abweichungen für den Anwendungsbereich der Netzkopplung werden in den folgenden Abschnitten definiert.

8.1 SCHUTZ DER ANBINDUNG

Ergänzend dazu gelten im Rahmen der Netzkopplung folgende Regelungen:

Bei Angriffsversuchen oder sonstigen Sicherheitsvorfällen, die durch den Teilnehmer, den Betreiber der angeschlossenen Netzinfrastruktur, die KBV oder eine KV festgestellt und gemeldet werden, ist der Provider verpflichtet durch geeignete Maßnahmen den Angreifer ausfindig zu machen und angemessene Gegenmaßnahmen einzuleiten – die datenschutzrechtlichen Regelungen müssen eingehalten werden.

Angemessene Gegenmaßnahmen bei Missbrauch, festgestellten Angriffsversuchen oder sonstigen Sicherheitsvorfällen, die durch einen Teilnehmer verursacht worden sind, müssen mindestens Folgendes einschließen:

- Deaktivierung des Teilnehmers im Netzkopplungsrouter.
- Meldung des Vorfalls an die KBV. Die KBV informiert andere Provider über den Vorfall, sodass ggf. der Teilnehmer auch in anderen Netzkopplungsroutern anderer Provider deaktiviert werden kann.
- Unterstützung bei der Untersuchung der Aktivitäten des Teilnehmers und der Schadensanalyse, z. B. durch Bereitstellung von Log-Dateien.

Angemessene Gegenmaßnahmen bei Missbrauch, festgestellten Angriffsversuchen oder sonstigen Sicherheitsfällen, die durch den Betreiber der angeschlossenen Netzinfrastruktur verursacht worden sind, müssen Folgendes einschließen:

- Deaktivierung der Anbindung des Betreibers der angeschlossenen Netzinfrastruktur und damit aller darüber angeschlossenen Teilnehmer.
- Meldung des Vorfalls an die KBV.
- Unterstützung bei der Schadensanalyse, z. B. durch Bereitstellung von Log-Dateien.

9 BERICHTSWESEN

Notwendige Ergänzungen oder Abweichungen zur gültigen Version der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] für den Anwendungsbereich der Netzkopplung werden in diesem Kapitel definiert.

Um das in dieser Richtlinie definierte Verfahren der Teilnehmerzulassung zum SNK durchführen zu können, muss der Provider alle Teilnehmer an die KVen melden. Diese Meldung hat sowohl bei der erstmaligen Einrichtung der Teilnehmer als auch unverzüglich bei jeder Änderung oder Erweiterung des Teilnehmerkreises zu erfolgen. Die KVen können ein Vetorecht gegenüber einzelnen Teilnehmern ausüben.

Der Provider stellt hierzu den KVen bei erstmaliger Einrichtung der Teilnehmer, regelmäßig monatlich zum 15. des Folgemonats und ansonsten unverzüglich bei Änderungen oder Erweiterungen des Teilnehmerkreises eine Auflistung der in den Netzkopplungsroutern eingerichteten Teilnehmer zur Verfügung.

Die Aufstellung hat pro KV zu erfolgen und ist ausschließlich an die betreffende KV zu melden und enthält die folgenden Informationen:

- Nachname und Vorname des Teilnehmers
- Gebiet der KV-Zugehörigkeit des Teilnehmers
- Lebenslange Arztnummer (LANR) des Teilnehmers
- Betriebsstättennummer (BSNR) des Teilnehmers
- zu nutzende Anwendungen oder Begründung für den Zugang zum SNK

Da die KVen den Teilnehmerkreis bestimmen, sind diese auch in der Pflicht, den Teilnehmerkreis zu prüfen. Diese Prüfung sollte regelmäßig bei Änderung des Teilnehmerkreises durchgeführt werden, mindestens aber jährlich.

Das Datenformat zur Übermittlung der Statistiken wird von der KBV festgelegt.