Kassenärztliche Bundesvereinigung
Körperschaft des öffentlichen Rechts

Sicheres Netz der KVen

Merkblatt KV-SafeNet-Router

[KBV_SNK_MBEX_KV-SafeNet-Router]

Dezernat 6
Informationstechnik, Telematik und Telemedizin

10623 Berlin, Herbert-Lewin-Platz 2

Kassenärztliche Bundesvereinigung

Version	1.0
Datum:	31.10.2011
Klassifizierung:	Öffentlich
Status:	In Kraft

DOKUMENTENHISTORIE

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	31.10.2011	KBV	Erstellung des Dokuments, QS und Freigabe		

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.

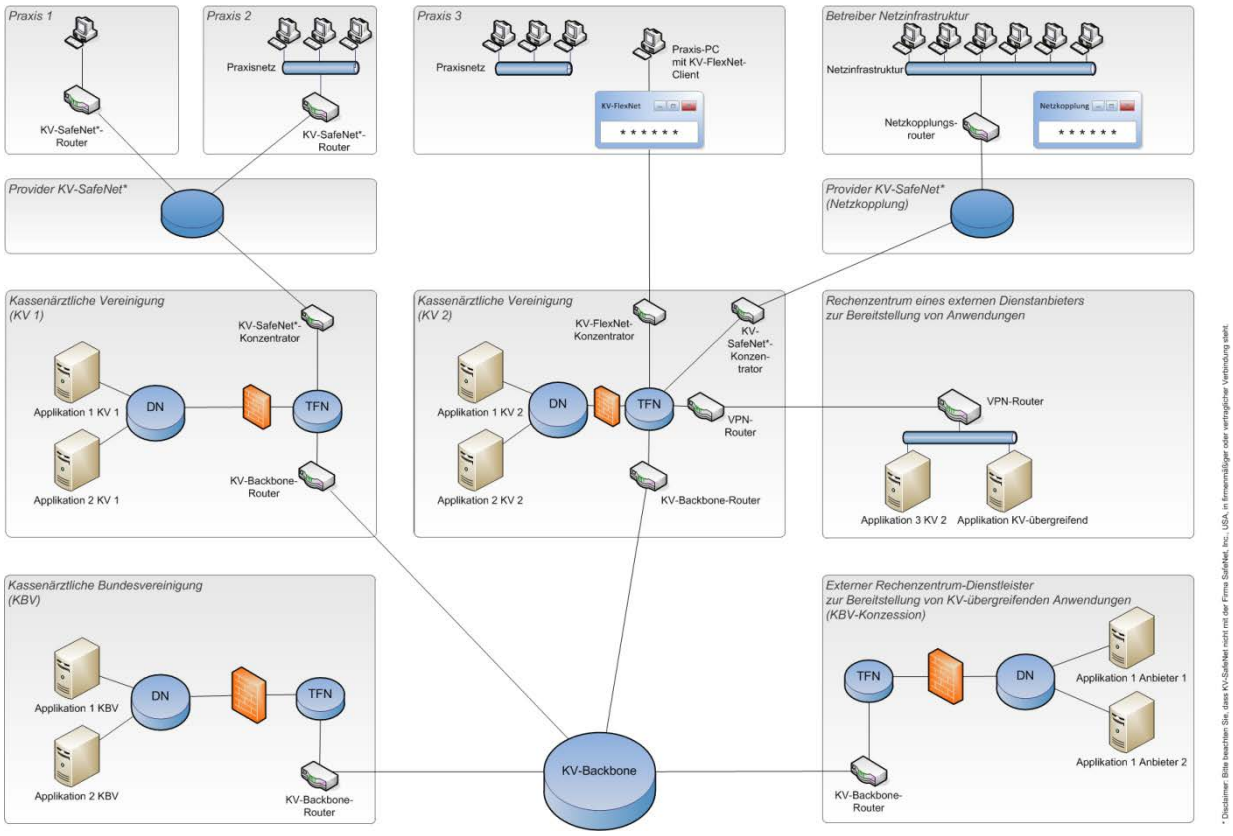

Abbildung 1: Beispielhafte Netztopologie

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

Dieses Merkblatt soll Teilnehmern mit KV-SafeNet-Zugang auf einer technischen, aber verständlichen Ebene erläutern, wie die sichere Kommunikation zum *Sicheren Netz der KVen* aufgebaut ist. Dazu gehören im Einzelnen: eine Darstellung der Kommunikationsendpunkte, der verwendeten kryptographischen Verfahren, sowie eine übersichtliche Erläuterung der technischen und organisatorischen Sicherheit.

Für eine Einführung in das *Sichere Netz der KVen* sei hier auf die Broschüre „KV-Online-Power – Wege zur papierlosen Praxis“[2] verwiesen.

Für eine Darstellung welche Maßnahmen bei Einsatz bestimmter Sicherheitsszenarien umzusetzen sind, kann das Dokument [KBV_SNK_MBEX_Sicherheit_Arbeitsplätze] als Referenz verwendet werden. Insbesondere wenn über den KV-SafeNet-Router auch das Internet genutzt werden soll, klärt das Dokument auf, dass geeignete Schutzmaßnahmen wie Sicherheitsupdates für Betriebssystem- und andere Software, Virenschutz und Firewall auf dem PC installiert werden müssen.

1.3 Klassifizierung und Adressaten des Dokuments

Dieses Dokument ist öffentlich zu verwenden. Es richtet sich vor allem an die Teilnehmer im *Sicheren Netz der KVen*. Dazu gehören die niedergelassenen Ärzte und Psychotherapeuten, die den Online-Zugang zu ihrer KV oder einer Applikation im *Sicheren Netz der KVen* bereits umgesetzt haben oder in ihrer Praxis einrichten wollen und Informationen bezüglich des verwendeten Sicherheitsniveaus beim Einsatz von KV-SafeNet wünschen.

* 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] Siehe: http://www.kbv.de/24874.html

2 Sicherheit am KV-SafeNet-Router

Aufbauend auf der topografischen Netzlandschaft werden die jeweiligen Kommunikationsendpunkte der Netzverbindungen sowie die vereinfachten technischen Erläuterungen der Verschlüsselungsverfahren transparent aufgezeigt und erläutert. Abschließend sollen die Rechte des Teilnehmers und die Kontrollfunktion der KBV/KVen gegenüber den KV-SafeNet-Providern beschrieben werden.

2.1 KV-SafeNet-Zugang

Der KV-SafeNet-Zugang eines Teilnehmers ermöglicht den gesicherten Datenaustausch im *Sicheren Netz der KVen*. In diesem Abschnitt werden die Voraussetzungen der Teilnehmer dargestellt. An Hand eines Schaubilds wird verdeutlicht, zwischen welchen Endpunkten die Datenverbindungen aufgebaut und auf welcher Ebene Daten ausgetauscht werden.

2.1.1 Voraussetzungen

Anbieter die einen Zugang zum *Sicheren Netz der KVen* bereitstellen dürfen, müssen in jedem Fall von der KBV-Prüfstelle zertifiziert sein. Um die entsprechende Zertifizierung zu erhalten, müssen alle Provider der KBV nachweisen, dass ihre technischen und organisatorischen Konzepte den Anforderungen und Sicherheitsstandards der Richtlinie KV-SafeNet [KBV_SNK_RLEX_KV-SafeNet] entsprechen und die gesetzlichen Vorgaben zum Datenschutz erfüllen.

Bei einem zertifizierten KV-SafeNet-Provider darf nun ein Vertragsarzt, -psychotherapeut oder ein anderer nach den Richtlinien der KBV zugelassener Teilnehmer einen Vertrag abschließen. Der Vertrag erlangt jedoch erst Gültigkeit mit der jeweiligen Bestätigung des Antrags durch die zuständige KV. Die KV verifiziert Teilnehmerdaten auf KV-Zugehörigkeit. Ist der Teilnehmer nicht KV-Mitglied, findet der Vertrag keine Anwendung und der Zugang kann nicht installiert werden.

2.1.2 Zugang zum *Sicheren Netz der KVen*

Die Online-Anbindung über KV-SafeNet ähnelt dem Anschluss an das Internet. Der Zugang zum *Sicheren Netz der KVen* erfolgt über einen nicht manipulierbaren KV-SafeNet-Router, der zwischen Telefonanschluss und Praxisrechner, beziehungsweise Praxisnetzwerk geschaltet wird. Der KV-SafeNet-Router baut ein sogenanntes virtuelles privates Netzwerk (VPN) auf. Dieses schottet die Verbindung vom normalen Internet ab und ermöglicht so einen abgesicherten Datenaustausch mit den Rechenzentren der jeweiligen KV und der KBV. Gleichzeitig blockiert der KV-SafeNet-Router den Zugriff von außen auf die angeschlossenen Praxis-PCs und die Daten im Praxis-Netzwerk. Damit ist die gesamte Praxis-EDV geschützt.

Die zertifizierten KV-SafeNet-Provider bieten die folgenden Zugangsvarianten an: ISDN, DSL, UMTS bzw. den VPN-Zugang über einen bereits bestehenden Internetanschluss eines Telekommunikationsproviders.

Daten können dann durch den etablierten VPN-Tunnel zu den im *Sicheren Netz der KVen* angebotenen Applikationen übertragen werden. Der Aufbau des Tunnels erfolgt dabei immer vom Teilnehmer zur KV. Der Tunnelaufbau von der KV zum Teilnehmer ist nicht möglich. Für die zugrundeliegende Sicherheit des Tunnels ist der KV-SafeNet-Provider an dieser Stelle verantwortlich. Die festen Endpunkte des Tunnels liegen beim Teilnehmer und in der KV. Das Öffnen des Tunnels ist dem Provider strikt untersagt und technisch sowie organisatorisch unterbunden.

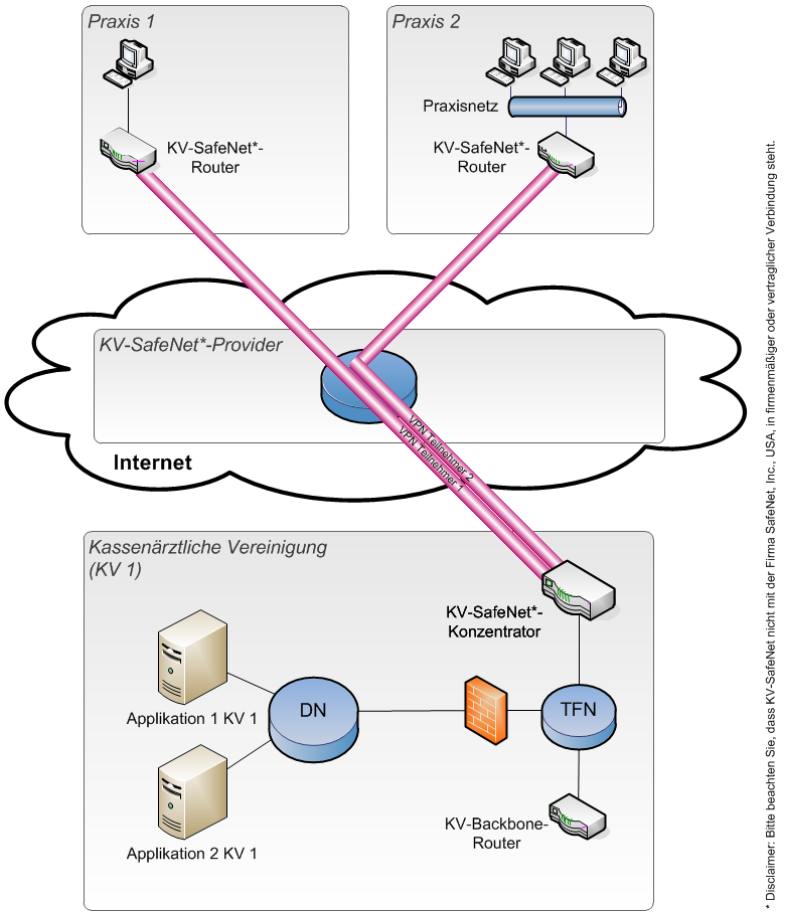

Abbildung 2: Schematische Darstellung des Zugangs

Diese Abbildung verdeutlicht den durchgehenden Tunnel vom Teilnehmer in die KV. Werden beispielsweise Abrechnungsdaten übertragen, so wird die Vertraulichkeit auf mehreren Ebenen gewährleistet:

1. mit Hilfe des etablierten VPN-Tunnels zur KV und schließlich
2. über das abgesicherte Mitgliederportal der KV, an dem sich der Teilnehmer mit seinen persönlichen Zugangsdaten anmeldet.

Wie die einzelnen Sicherheitsmechanismen zusammenwirken und die Daten des Teilnehmers schützen, soll im Weiteren erläutert werden.

Zu den zwei genannten Ebenen kann je Dienst und dessen besonderen Anforderungen an die Datensicherheit ein weitere hinzukommen. Für die besonders sensiblen Daten, die im Rahmen der ***Online-Abrechnung*** übertragen werden erfolgt zum Beispiel eine zusätzliche Verschlüsselung mit dem *KBV-Kryptomodul*. Dabei werden die Daten zuerst durch das verwendete Praxisverwaltungssystem und das dort eingesetzte Verschlüsselungsmodul der KBV bereits auf dem Rechner des Teilnehmers verschlüsselt.

Datenschutz und Datensicherheit der Übertragung erfolgt dann in drei Ebenen:

1. Verschlüsselung durch das in die Praxissoftware integrierte KBV-Kryptomodul.
2. Schutz der Daten durch VPN-Kanal bei der direkten Übertragung zur KV.
3. Verschlüsselung des Mitgliederportals der jeweiligen KV.

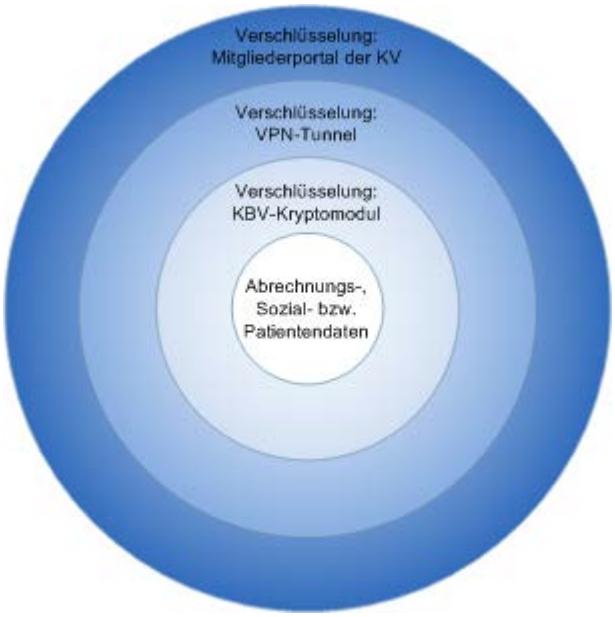

Abbildung 3: Ebenen der Verschlüsselung im Rahmen Online-Abrechnung

2.1.3 Darstellung der Kommunikation

Der nicht manipulierbare KV-SafeNet-Router wird zwischen den Netzwerkanschluss der Praxis und den Praxisrechner, beziehungsweise das Praxisnetzwerk geschaltet. Der KV-SafeNet-Router blockiert mit Hilfe einer integrierten Firewall den Zugriff von außen auf die angeschlossenen Praxis-PCs und dortigen Daten. Angriffe aus dem Internet auf die Arztpraxis werden somit unterbunden.

Beim Zugang zum *Sicheren Netz der KVen* baut der Router einen VPN-Tunnel auf. Das VPN schottet die Verbindung vom Internet ab und gewährleistet einen sicheren Datenaustausch mit dem Rechenzentrum der jeweiligen KV. Die Daten werden durch den VPN-Tunnel auf direktem Weg in das Rechenzentrum der KV übertragen. Die fest definierten Tunnel-Endpunkte sind dabei einerseits der KV-SafeNet-Router beim Teilnehmer und andererseits der sogenannte Konzentrator im KV-Rechenzentrum. Die weitere Verarbeitung der Daten erfolgt in der jeweiligen KV unter Einhaltung der gesetzlichen Vorgaben zu Datenschutz und Datensicherheit.

Der KV-SafeNet-Router wird ausschließlich von durch die KBV zertifizierten Providern angeboten. Diese Provider verpflichten sich u. a. zur Einhaltung der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] und gewährleisten, dass die hohen Sicherheitsstandards eingehalten werden.

Sowohl der Konzentrator als auch die KV-SafeNet-Router ignorieren alle Protokollanfragen auf TCP/IP Ebene aus dem Internet. Ein potentieller Angreifer erhält somit keine Information, die er für einen Angriff nutzen könnte.

2.2 Technische Sicherheit

Damit bei der Übertragung der Informationen eine hohe Sicherheit gewährleistet werden kann, müssen die folgenden drei Anforderungen für die Übertragung von Daten erfüllt werden:

- Vertraulichkeit der Daten, so dass kein Unbefugter Zugriff auf die gesendeten Informationen hat
- Integrität der Daten, damit diese vor unautorisierter Veränderung (Manipulation) geschützt sind
- Authentizität des Senders der Daten, dass nachweisbar und verifizierbar ist, wer zu welchem Zeitpunkt die Daten übermittelt hat

Um diese Schutzziele zu erreichen werden im *Sicheren Netz der KVen* VPN-Verbindungen verwendet. Diese besondere Art der Netzwerke wird im Folgenden beschrieben.

2.2.1 Erläuterung der VPN Technologie

Über ein VPN kann ein privates Netzwerk etabliert werden, das als Basis ein beliebiges Trägernetz, z. B. das Internet, nutzt. Das VPN sorgt für die sichere Übertragung der Daten und gewährleistet dabei immer die Einhaltung der drei bereits erwähnten Sicherheitsziele: Vertraulichkeit, Integrität und Authentizität.

Vertraulichkeit fordert die Geheimhaltung der Daten und wird durch die Verschlüsselung der Daten gewährleistet. Somit können unberechtigte Dritte keine Kenntnis von den Daten erlangen. Die eingesetzte Verschlüsselung der Netzwerkkommunikation verhindert, dass Nichtbeteiligte dritte Parteien Zugriff auf das sichere Netzwerk bekommen.

Integrität bedeutet, dass Daten bei der Übertragung nicht modifiziert werden. Dies wird erreicht, indem die zu übertragenden Pakete mit Prüfsummen versehen werden, die dann zusammen mit dem Paketinhalt verschlüsselt übertragen werden. Beim Empfänger wird euneut eine Prüfsumme gebildet und mit der übertragenen verglichen. Stimmen die Prüfsummen überein, kann eine Modifizierung der übertragenen Daten ausgeschlossen werden.

Durch *Authentizität* wird sichergestellt, da keine unberechtigten Benutzer über das VPN auf das lokale Netzwerk zugreifen können und da eingehende Daten tatsächlich von der angemeldeten Gegenstelle kommen und nicht von einer anderen Quelle. Somit ist der Sender einer Nachricht nachweislich verifizierbar. Die notwendige Authentisierung wird über den KV-SafeNet-Router realisiert, der den zugehörigen Teilnehmer eindeutig identifiziert.

Aktuelle Umsetzungen von VPN gewährleisten immer eine starke Authentisierung, sowie den Schutz von Vertraulichkeit und Integrität der übertragenen Daten.

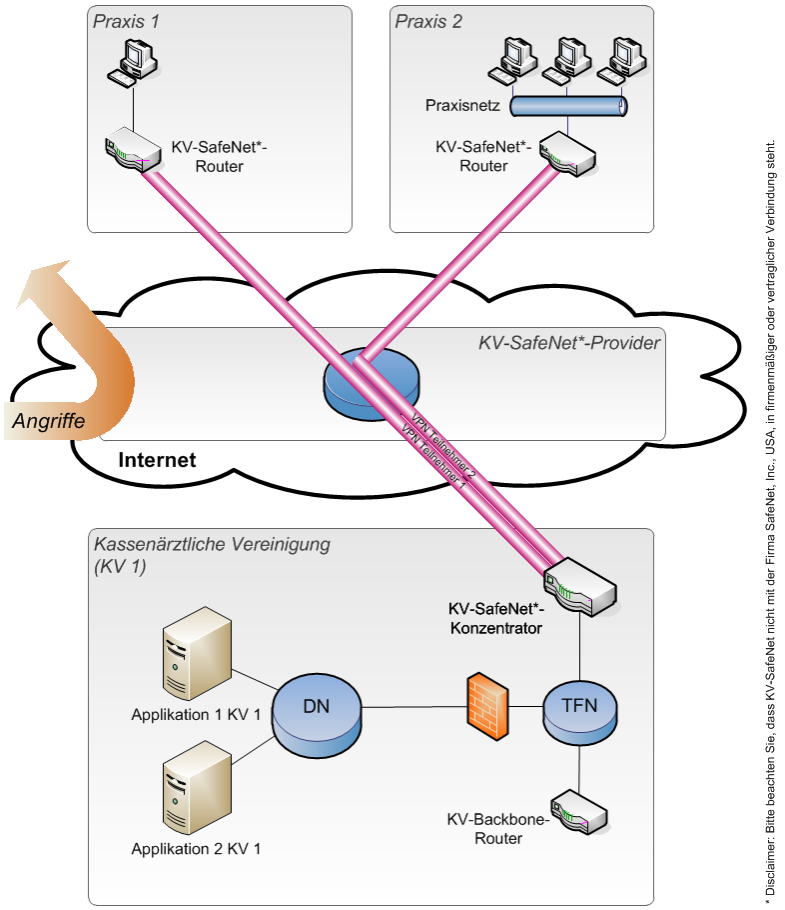

Abbildung 4: Sicherer Datenaustausch über VPN

2.2.2 Angewandte VPN-Verfahren

Für den Aufbau einer sicheren Verbindung werden aufeinander aufbauend die folgenden drei Schritte durchlaufen:

1. Authentifikation der Kommunikationspartner, d.h. Identifikation der Benutzer mit Hilfe eines asymmetrischen Verfahrens oder durch den Einsatz von Zertifikaten,
2. Vereinbarung eines symmetrischen Schlüssels, der dazu dient die Vertraulichkeit der zu übertragenden Daten durch Chiffrierung bzw. Kodierung zu schützen und
3. Austausch dieser Schlüssel, die den Schutz der Kommunikation gewährleisten.

Bei den Kommunikationspartnern aus Schritt eins handelt es sich um den Teilnehmer und um die KV, in der der Einwahlknoten des KV-SafeNet-Providers aufgestellt ist. Der VPN-Tunnel existiert nur zwischen diesen authentifizierten Kommunikationspartnern. Kein KV-SafeNet-Provider und kein anderer Teilnehmer im *Sicheren Netz der KVen* haben auf die über diesen VPN-Tunnel übertragenen Daten Zugriff.

Nach erfolgreicher Authentisierung der Kommunikationspartner einigen sich beide Parteien auf ein Verschlüsselungsverfahren. Dabei wählt der Konzentrator (Server) aus einer durch den KV-SafeNet-Router (Client) zur Verfügung gestellten Liste von unterstützten Verfahren eines für die Sitzung aus.

Für eine ausführlichere Darstellung und weitere Referenzen für die Umsetzung von VPN-Verfahren sei hier auf den Anhang A.1: „VPN auf dem ISO/OSI Schichtmodell“ verwiesen.

2.2.3 Angewandte Verschlüsselungsverfahren

Bei der Zertifizierung der KV-SafeNet-Provider richtet sich die KBV nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI), insbesondere nach der Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI – Technische Richtlinie TR-02102“[3] und nach den Maßnahmen zum IT-Grundschutz zur Auswahl eines geeigneten kryptographischen Verfahrens (M 2.164[4]).

Zertifizierte KV-SafeNet-Provider[5] müssen bei dem Einsatz von Verschlüsselungsmechanismen und -verfahren immer die aktuellen Vorgaben des BSI beachten.

Eine ausführlichere Betrachtung und weitere Quellen sind im Anhang A.2: „Aktuelle Verschlüsselungsverfahren“ hinterlegt.

2.3 Organisatorische Sicherheit

Zusätzlich zur grundlegenden technischen Sicherheit wird für den Teilnehmer mit KV-SafeNet auch organisatorisch Sicherheit gewährleistet. Dies geschieht vor allem in Form von Zertifizierungen und Überprüfungen der KV-SafeNet-Provider durch die KBV und durch die Gewährleistung und Prüfung der Rechte im Teilnehmervertrag. Zudem hat der Teilnehmer die Möglichkeit zur Kontrolle des KV-SafeNet-Providers in Bezug auf dessen Wartungsaktivitäten. Diese Maßnahmen und deren Umsetzung werden im folgenden Abschnitt erläutert.

2.3.1 Zertifizierung und Überprüfung der KV-SafeNet-Provider

Im Rahmen des Zertifizierungsprozesses durch die KBV erkennt der Provider die Richtlinie [KBV_SNK_RLEX_KV-SafeNet] ohne Einschränkungen an und verpflichtet sich somit zur vollständigen Umsetzung.

Im Zertifizierungsverfahren werden die technischen Konzepte der einzelnen Zugangsvarianten und -geräte überprüft. Dazu zählen nicht nur die technischen Beschreibungen der Geräte, sondern auch die Erläuterungen zu den Schutzmaßnahmen, die dazu führen, dass der Zugang zum *Sicheren Netz der KVen* mittels KV-SafeNet das lokale Netzwerk des Teilnehmers vor Angriffen aus dem Internet ebenso schützt wie die Übertragung der Daten. Gemäß Richtlinie [KBV_SNK_RLEX_KV-SafeNet] werden immer alle Zugangsgeräte eines Providers überprüft. Setzt ein Provider ein neues Gerät ein, ist das nur nach erfolgreicher Prüfung durch die KBV möglich.

Andererseits werden auch die organisatorischen Betriebsprozesse des Providers begutachtet. Dazu zählen die Maßnahmen zur Einhaltung und Umsetzung der Service- und Supportprozesse bezüglich des Konzentrators in der KV und des KV-SafeNet-Routers beim Teilnehmer. Ebenso wird geprüft, ob der Provider seine Mitarbeiter zur Einhaltung des Datenschutzes und der Verschwiegenheit verpflichtet (Verpflichtung bezogen auf § 5 Bundesdatenschutzgesetz sowie § 88 Telekommunikationsgesetz).

Die KBV hat nach erfolgreicher Zertifizierung immer ein Überprüfungsrecht des KV-SafeNet-Providers. Gemäß Richtlinie [KBV_SNK_RLEX_KV-SafeNet] erfolgt die Überprüfung von Providern auf organisatorischer und auf technischer Ebene.[6] Zum einen werden Überprüfungen der Einhaltung organisatorischer Maßgaben dieser Richtlinie durchgeführt, sogenannte Audits. Diese Audits beinhalten eine Vor-Ort-Prüfung beim Anbieter sowie eine Prüfung ausgewählter Dokumente. Zum anderen werden ein durch die KBV ausgewählter KV-SafeNet-Router und ein Konzentrator einer sicherheitstechnischen Überprüfung unterzogen, einem sogenannter Penetrationstest.

[3] Siehe Technische Richtlinie TR-02102 https://www.bsi.bund.de.
[4] Siehe Maßnahme M 2.164: https://www.bsi.bund.de.
[5] Gültig für KV-SafeNet-Provider, die nach der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] Version 3.0 oder höher zertifiziert sind.
[6] Gültig für KV-SafeNet-Provider, die nach der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] Version 3.1 oder höher zertifiziert sind.

2.3.2 Rechte des Teilnehmers

Durch Umsetzung der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] ergeben sich für den Teilnehmer unter anderem im Teilnehmervertrag das Kontrollrecht über die fortlaufende Einhaltung der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] sowie ein außerordentliches Kündigungsrecht aus wichtigem Grund. Ebenso muss der Vertrag eine Vertragsstrafe des Providers in festgelegter Höhe aufgrund nicht eingehaltener Wiederherstellungszeiten enthalten.

Bezüglich der Wartungszugänge des KV-SafeNet-Routers hat der Teilnehmer immer die Möglichkeit dem Wartungszugang grundsätzlich zu widersprechen bzw. den Zeitpunkt der Wartung zu steuern und zu autorisieren. Des Weiteren hat der Teilnehmer ein Informationsrecht über alle durchgeführten Wartungs- und Administrationszugriffe auf den KV-SafeNet-Router.

2.3.3 Wartungszugang und Konfiguration der Zugangsgeräte

Um eine Manipulation der Konfiguration des KV-SafeNet-Routers zu verhindern, wird dieser durch geeignete Sicherheitsmaßnahmen, z. B. Änderung der Zugangsdaten zur Administrationsoberfläche des Routers, geschützt. Zudem wird durch die vom Provider einzuhaltenden und durch die KBV zertifizierten Maßnahmen der Richtlinie [KBV_SNK_RLEX_KV-SafeNet] ein Zugriff vom Internet auf den KV-SafeNet-Router und somit auf das dahinterliegende Praxisnetzwerk verhindert.

2.4 Fazit und Schlussbetrachtung

Der KV-SafeNet-Router realisiert ein hardwarebasiertes VPN. Dies ist nach Auffassung der Datenschutzbeauftragten der Länder und des Bundes die sicherste Variante zur Datenübertragung.

Mit dem KV-SafeNet-Zugang zum *Sicheren Netz der KVen* werden Vertraulichkeit, Integrität und Authentizität gewährleistet. Die angewandten Verfahren (VPN-Technologie, Verschlüsselungsmethodik) orientieren sich an den Maßgaben des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) und entsprechen dem Stand der Technik.

KV-SafeNet-Provider und deren eingesetzte KV-SafeNet-Router unterliegen einem strengen Zertifizierungs- und Überprüfungsverfahren der KBV, das die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherheit gewährleistet.

Die KBV prüft zudem die Musterverträge zwischen Provider und Teilnehmer und achtet auf die Wahrung der Rechte der Teilnehmer zur Kontrolle der Provider.

3 Glossar

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

Begriff	Erklärung
Servicenetz	Siehe Dienstenetz.
Sicheres Netz der KVen	Das *Sichere Netz der KVen* ist eine von der KBV und den KVen bereitgestellte Infrastruktur, bestehend aus einem vollvermaschten VPN-Netzwerk (KV-Backbone), im Netzwerk befindlichen Diensten und Anwendungen (KV-Apps) und den definierten Anbindungsmöglichkeiten an das Netzwerk (KV-SafeNet und KV-FlexNet). Diese Infrastruktur trägt den Anforderungen an Datenschutz und Datensicherheit Rechnung und ist für die Übermittlung von Sozialdaten geeignet.
Teilnehmer	Ein Teilnehmer ist ein Vertragsarzt, -psychotherapeut oder ein anderes nach den Richtlinien der KBV zugelassenes Mitglied des *Sicheren Netzes der KVen*.
Teilnehmernetz	Die untereinander lokal vernetzten Teilnehmercomputer bilden das Netzwerk des Teilnehmers. Hier können sich weitere vernetzte Endsysteme (z.B. Server, Drucker, Kartenleser) befinden.
Transfernetz (TFN)	Das Transfernetz dient der Weiterleitung der Datenpakete vom Teilnehmer zu den Applikationsservern und zurück. Es wird durch den KV-Backbone-Router realisiert. Die Organisation des Transfernetzes liegt in Verantwortung des KV-Backbone-Betreibers.
Tunnel / VPN-Tunnel	Für die Kommunikation des zugeordneten Netzes mit einem seiner VPN-Partner werden am VPN-Gateway die ursprünglichen Netzwerkpakete in ein VPN-Protokoll gepackt. Daher spricht man bei VPN vom Tunnel.
Zertifizierung	Prozess in dem explizit nachgewiesen wird, wie der Antragsteller die in der Richtlinie geregelten Anforderungen umsetzt. Wird dieses Verfahren erfolgreich abgeschlossen, erhält der Antragsteller eine Konformitätserklärung.
Zugangsnetz	Dazu gehören Netzelemente und Vermittlungsstellen, die Grundlagen der techn. Infrastruktur zwischen Anbieter- und Teilnehmeranschluss schaffen.

4 Referenzierte Dokumente

Referenz	Dokument
[KBV_SNK_RLEX_KV-SafeNet]	Richtlinie KV-SafeNet
[KBV_SNK_LFEX_Zert_Provider]	Leitfaden Zertifizierung Provider
[KBV_SNK_MBEX_ Sicherheit_Arbeitsplätze]	Merkblatt Sicherheitsanforderungen an KV-SafeNet-Arbeitsplätze

ANHANG

A Anhang: Technische Grundlagen

A.1 VPN auf dem ISO/OSI Schichtmodell

Der virtuelle Tunnel entsteht dadurch, dass die zu übertragenden IP-Pakete verschlüsselt und in ein neues IP-Paket platziert werden. Dabei setzt sich ein IP-Paket immer aus dem IP-Header (Ziel- und authentifizierte Absender Adresse des Pakets) und den Nutzdaten zusammen.

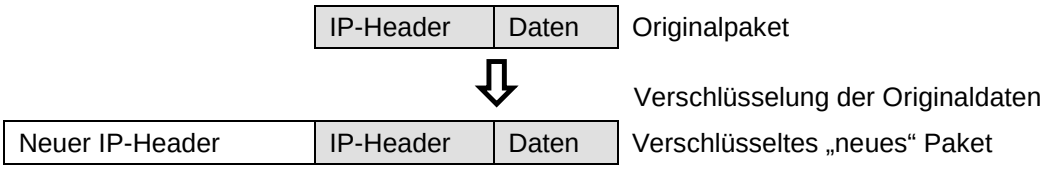

Abbildung 5: Aufbau eines IP-Pakets im VPN-Tunnel

Somit sind Ziel- und Absender-IP-Adresse, sowie die Daten aus dem Originalpaket im neuen IP-Header durch die Verschlüsselung und die Authentizität im VPN-Tunnel geschützt und verborgen. Die Umsetzung des VPN-Tunnels ist auf drei verschiedenen Ebenen möglich:

ISO/OSI Schicht[7]		VPN-Protokoll	Anschauliche Darstellung/Beschreibung
7	Anwendungsschicht		Anwendungsebene: ermöglicht den Zugriff auf Daten und gibt die Kommunikation zwischen zwei Anwendungen wieder
6	Darstellungsschicht		
5	Sitzungsschicht		
4	Transportschicht	SSL, TLS	Transport: Ende-zu-Ende Kontrolle durch Segmentierung der Datenströme
3	Vermittlungsschicht	IPSec	Internet: Leitungsorientierte Vermittlung der Pakete auf Netzwerkebene
2	Sicherungsschicht	L2TP, CHAP	Netzzugang: phys. Ebene (mechanisch, elektrisch), Übertragung einzelner Bits
1	Bitübertragungsschicht		

Tabelle 1: Platzierung von VPN auf ISO/OSI Schichtmodell

Die benannten Verfahren eines VPN Protokolls sollen im Folgenden kurz anhand ihrer technischen Eigenschaften erläutert und verglichen werden.

1. L2TP (Layer 2 Tunneling Protocol, vgl. RFC 2661[8]): der Einsatz von L2TP ist nur auf Einwahlverbindungen beschränkt. Hier wird der komplette Kanal verschlüsselt und nicht die einzelnen Datenpakete. Als Authentifizierung dient CHAP (Challenge Handshake Authentication Protocol).
2. Das Sicherheitsprotokoll IPSec (Internet Protocol Security, vgl. RFC 4301[9]) schützt die übertragenen Daten (IP Pakete) bereits auf der Vermittlungsschicht. Dabei wird das

[7] Siehe auch: http://de.wikipedia.org/wiki/OSI-Modell
[8] Online unter: http://tools.ietf.org/html/rfc2661
[9] Online unter: http://tools.ietf.org/html/rfc4301

vollständige Datenpaket verschlüsselt, dennoch bleibt die Quelle der Daten authentifizierbar und die Integrität des Pakets wird gewährleistet. Die Vertrauensbeziehung wird in einem Schlüsselaustauschverfahren zwischen den beiden vorkonfigurierten Endpunkten hergestellt.

3. Das Verschlüsselungsprotokoll TLS (Transport Layer Security, vgl. RFC 5246 für TLS Version 1.2[10]) wurde auf Basis der SSL-Spezifikation (Secure Socket Layer) entwickelt und wird sehr verbreitet für Online-Banking verwendet. TLS hat die Eigenschaft, dass sich beide Parteien vor Beginn der Kommunikation auf einen gemeinsamen Schlüssel einigen können, um so die Daten und deren Übertragung abzusichern.

Da der Einsatz des L2TP nur über Einwahlverbindungen möglich ist, werden bei der Übertragung von Daten im *Sicheren Netz der KVen* hauptsächlich VPN Verbindungen auf Grundlage der IPSec und der SSL/TLS Technologien hergestellt. Beide Verfahren sind durch das BSI für den authentisierten und verschlüsselten Austausch von Informationen über ein nicht vertrauenswürdiges Netzwerk (Internet) anerkannt.

A.2 Aktuelle Verschlüsselungsverfahren

Die folgende Tabelle listet eine Übersicht über die aktuell einzusetzenden Verfahren im Rahmen von KV-SafeNet-Zugängen:

Art des verwendeten Schlüsselverfahrens	Verschlüsselungs-algorithmus und -länge	Bemerkung / Einsatz des Verfahrens
Asymmetrisch	RSA: 2048 Bit	Zertifkate, die zur Authentisierung und zum Schlüsselaustausch verwendet werden
Symmetrisch	AES: 128,192 und 256 Bit 3DES: 168 Bit[11]	Schlüsselverfahren zur eigentlichen Verschlüsselung der Daten
Hashing	SHA-1: 160 Bit[12] SHA-2: 256, 384 und 512 Bit	Berechnung einer Prüfsumme zur Authentisierung der übermittelten Daten

Tabelle 2: Verwendete Verschlüsselungsverfahren und –längen im *Sicheren Netz der KVen*

Asymmetrische Verfahren verschlüsseln die Daten dabei mit dem öffentlichen Schlüssel des Empfängers. Dieser kann die Daten anschließend ausschließlich mit seinem privaten Schlüssel dechiffrieren und erhält somit den Klartext. Gleichzeitig bieten diese Verfahren die Möglichkeit den Sender der Daten anhand einer eingefügten Signatur zu verifizieren, die im verschlüsselten Bereich der Daten integriert wird. Ein typisches im KV-SafeNet verwendetes Verfahren ist die Verschlüsselung mittels RSA. Der Name RSA steht dabei für die Anfangsbuchstaben der Familiennamen der drei Kryptologen Ronald L. Rivest, Adi Shamir und Leonard Adleman die dieses Verfahren am MIT 1977 entwickelt haben.

[10] http://tools.ietf.org/html/rfc5246
[11] Dieses Verfahren bietet selbst bei erfolgreichen Angriffen eine Sicherheit von 112 Bit.
[12] Der Einsatz von SHA-1 ist nur bei der Verwendung in HMAC-basierten Verfahren (SSL/TLS) als unkritisch zu bewerten.

Symmetrische Verfahren haben den großen Vorteil, dass sie wesentlich schneller als asymmetrische Verfahren arbeiten, da sie lediglich mit einem Schlüssel die Daten chiffrieren. Dabei haben sie den großen Nachteil, dass ein Austausch des Schlüssels immer über einen sicheren Kanal geschehen muss. Zu diesen Verfahren zählen einerseits der von der US-Regierung verbreitete und bewährte Data Encryption Standard (3DES), sowie der neuere Advanced Encryption Standard (AES), der sukzessive 3DES ablösen wird.

Beide Verfahren werden ergänzt durch kryptologische Hashing Verfahren. Dies betrifft hier insbesondere den Secure Hashing Algorithm (SHA). Diese Verfahren dienen zur Berechnung eindeutiger Prüfsummen für zu übermittelnde Informationen, um anschließend den Ursprung einer Nachricht identifizieren zu können.