

Information

Berlin, Oktober 2007

Glossar Telematik

Die Einführung der elektronischen Gesundheitskarte geht mit diversen neuen und für viele Kollegen völlig fremdartigen Begriffen einher. Was ist Telematik überhaupt? Wie funktioniert ein elektronisches Rezept? Was ist eine Stapelsignatur? Wozu wird ein Konnektor benötigt? Und wozu ein Cross-Zertifikat? Die Gesundheitskarte selbst ist da nur die Spitze des Eisbergs.

Wir bringen Licht ins Dunkel. In diesem Informationsblatt finden Sie die wichtigsten Begriffe erklärt. Die Sortierung ist bewusst nicht alphabetisch sondern inhaltlich angelegt – vom Allgemeinen zum Besonderen.

Telematik

Der Begriff leitet sich aus **Tele**kommunikation und **Informatik** ab. Er beschreibt die Informationsverknüpfung mehrerer elektronischer Datenverarbeitungssysteme (EDV-Systeme) mittels eines Telekommunikationssystems.

Gesundheitstelematik

Im Gesundheitswesen wird die Telematik eingesetzt, um patientenbezogene Daten durch ein digitales Netzwerk zwischen Ärzten, Apothekern und Krankenhäusern schneller austauschen zu können. Beispiele sind die elektronische Patientenakte oder das elektronische Rezept.

Telematikinfrastruktur

Die komplexe elektronische Vernetzung, wie sie in der Gesundheitstelematik realisiert wird, verlangt eine den Anforderungen gewachsene bundesweite Kommunikationsplattform. Diese ist die Grundlage, um auch in der vernetzten Medizin interdisziplinär zusammenarbeiten zu können. Unter dem Begriff der Telematikinfrastruktur werden daher alle Komponenten, Dienste und Kommunikationsdienste zusammengefasst, die im Zuge der Einführung der elektronischen Gesundheitskarte zur Anwendung gebracht werden.

Telemedizin

Die Telemedizin gilt als Teilbereich der Gesundheitstelematik. Der Begriff bezeichnet einen diagnostischen und therapeutischen Vorgang, bei dem Arzt und

Patient räumlich und/oder zeitlich voneinander getrennt sind. Die Kommunikation wird in einem solchen Fall über Telefon oder Internet (E-Mail) hergestellt, für die Diagnose kommen technische Geräte zum Einsatz, die ihre Daten elektronisch verwalten und über das Internet oder andere elektronische Medien übermitteln können.

eHealth

eHealth (oder auch E-Health) ist ein Begriff, der im Allgemeinen das Zusammen-treffen von Internet und Medizin beschreibt. Je nach Kontext wird er für die elekt-ronische Erfassung, Verarbeitung, Speicherung und Übertragung von Daten im Gesundheitswesen verwendet, als Synonym für Telemedizin oder für das Bestreben verschiedener Interessengruppen (Versicherungen, Selbsthilfegrup-pen, Informationsportale), Informationen und Dienstleistungen zum Thema Ge-sundheit im Internet zu dokumentieren.

gematik GmbH

Die **Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH** ist im Januar 2005 mit Sitz in Berlin als Betriebsorganisation von den Spitzenorganisa-tionen des deutschen Gesundheitswesens gegründet worden. Ziel der Gesell-schaft ist die Einführung, Pflege und Weiterentwicklung der Gesundheitskarte und die Entwicklung übergreifender IT-Standards für den Aufbau und den Betrieb der gemeinsamen Telematikinfrastruktur. Im Beirat der gematik GmbH sitzen Vertreter von Patientenverbänden und der Bundesländer sowie Experten aus Wissenschaft und Industrie. Die Gesellschafter – bestehend aus Kostenträgern (Krankenkassen) und den Leistungs-trägern (z.B. Bundesärztekammer, Kassen-ärztliche Bundesvereinigung) – halten jeweils die Hälfte des Gesellschafterkapi-tals.

Gesundheitskarte (eGK)

Mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung hat der Gesetzgeber 2004 die Grundlage für die elektronische Gesundheitskarte geschaffen und ihre Einführung verbindlich vorgegeben (§291a, SGB V). Sie ist das zentrale Objekt der Gesundheitstelematik in Deutschland und soll in Zukunft die Krankenversichertenkarte ersetzen. Derzeit wird sie in ausgewählten Testre-gionen erprobt. Ausgestattet mit Lichtbild des Versicherten und einem Mikropro-cessorchip, der administrative Daten wie Name, Geburtsdatum und Versiche-tennummer speichert, ist sie gegen unautorisierte Zugriffe geschützt. Sie dient als Speichermedium des elektronischen Rezepts, gibt Auskunft über den Zuzah-lungsstatus des Patienten und darüber, ob dieser an einem DMP-Programm (**D**i-sease **M**anagement **P**rogrammen für chronisch Kranke) teilnimmt. Über die Speicherung der elektronischen Patientenakte sowie von Verordnungs- und Not-falldaten entscheidet der Patient selbst, diese Angaben sind freiwillig. Des Weite-ren ist geplant, auf der Rückseite der Gesundheitskarte die Europäische Kran-kenversicherungskarte (EHIC) zu integrieren, die den bisher üblichen Auslands-krankenschein ersetzt.

Elektronisches Rezept (eRezept)

Das elektronische Rezept soll das bisherige Papierrezept ersetzen. Der Ablauf bleibt erhalten, allerdings auf elektronischem Wege. Das Rezept wird vom Arzt auf der Gesundheitskarte gespeichert und signiert, in der Apotheke wird es mit speziellen Lesegeräten abgerufen und der Patient erhält seine Medikamente. Dieser Vorgang ist nur in Kombination mit Heilberufsausweisen möglich, mit denen sich z.B. Arzt und Apotheker legitimieren.

Elektronische Patientenakte (ePA)

Die elektronische Patientenakte enthält alle Behandlungsdokumente eines Patienten (Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen) und wird auf der elektronische Gesundheitskarte gespeichert. Diese Anwendung ist freiwillig. Zunächst soll nur innerhalb einer Praxis oder Klinik auf die elektronische Patientenakte zugegriffen werden können. Langfristig ist jedoch eine Ausweitung der Zugriffsrechte geplant, so dass alle Ärzte mit Einwilligung ihrer Patienten schnell Zugriff auf deren Unterlagen haben und Befunde somit unmittelbar am Ort der aktuellen Behandlung verfügbar sind. Zugriff auf die elektronische Patientenakte haben generell nur Inhaber von elektronischen Heilberufsausweisen. Zugriffsrechte des Patienten selbst sind aktuell noch in der Diskussion.

Elektronischer Heilberufsausweis (HBA) / elektronischer Arztausweis (eArztausweis)

Der elektronische Heilberufsausweis ist Bestandteil des Sicherheitskonzepts der Telematikinfrastruktur. Mit ihm müssen sich Mitarbeiter im Gesundheitswesen (Ärzte, Apotheker, Psychotherapeuten usw.) beim Zugriff auf Patientendaten identifizieren. Er erlaubt den Zugriff auf die medizinischen Daten der Gesundheitskarte und ermöglicht es z.B. elektronische Rezepte auszustellen und diese zu signieren.

EHIC

Die Europäische Krankenversichertenkarte (EHIC) ersetzt das bisher übliche Formular E-111 und ermöglicht den Versicherten so die medizinische Behandlung im europäischen Ausland. Es ist geplant, den EHIC auf der Rückseite der Gesundheitskarte zu integrieren.

Digitale Signatur / elektronische Signatur (eSign)

Die digitale Signatur ist eine elektronische Unterschrift, deren Echtheit durch ein Zertifikat bestätigt wird und die Authentizität einer Nachricht (z.B. eines elektronischen Rezepts auf der Gesundheitskarte) nachweist. Sie wird an ein elektronisches Dokument angehängt und enthält verschlüsselte Daten, die ein autorisierter Empfänger (z.B. der Apotheker) entschlüsseln und prüfen kann. Eine derartige digitale Signatur ist rechtsgültig und der persönlichen Unterschrift gleichgestellt. Für die Gesundheitstelematik gewährleistet die digitale Signatur ein hohes Maß an Sicherheit im Umgang mit den elektronischen Patientendaten.

Komfort- / Stapelsignatur

Komfort- bzw. Stapelsignatur sind Spezialfälle der digitalen Signatur und werden genutzt, um den technischen Vorgang der elektronischen Signatur (in der Regel vollzogen durch die Eingabe einer mindestens 6-stelligen PIN) in der Praxis zu beschleunigen. Bei der Stapelsignatur werden dazu mehrere Dokumente ge-

sammelt (ein Stapel) und dann durch die einmalige PIN-Eingabe gleichzeitig signiert. Die Komfortsignatur ist dagegen ein Verfahren, bei der die PIN einmal eingegeben und die Signatur durch ein anderes Identifikationsmerkmal – wie z.B. den Fingerabdruck – ausgelöst wird. Allerdings ist die technische Umsetzung der Komfortsignatur unter Beachtung der Vorschriften zur Erstellung von qualifizierten elektronischen Signaturen sehr komplex und dieses Verfahren durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch nicht zugelassen, so dass der Zeitpunkt einer Realisation noch nicht sicher ist.

Zertifikat

Zertifikate sind elektronische Bescheinigungen, die von einer Zertifizierungsinstanz ausgestellt bzw. signiert werden. Mit ihnen werden dem Zertifikatsinhaber bestimmte Informationen zugeordnet. Man unterscheidet zwischen verschiedenen Formaten:

- Ein **Public-Key-Zertifikat** (der Begriff wird in der Regel als Synonym für Zertifikat verwendet) weist nach, dass der öffentliche Schlüssel eines asymmetrischen Verschlüsselungsverfahrens zu der Person, Firma oder Institution gehört, die ihn verwendet. In Form eines Datensatzes informiert das Zertifikat über den Namen des Inhabers, dessen öffentlichen Schlüssel, über die Seriennummer und Gültigkeitsdauer des Zertifikats sowie über den Namen der Zertifizierungsstelle. Diese Daten sind mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Damit wird die Echtheit einer digitalen Signatur bestätigt, mit der sich z.B. der Arzt mittels seines Arztausweises innerhalb der Telematikinfrastruktur im Gesundheitswesen authentifizieren und elektronische Dokumente sowie E-Mails verschlüsseln kann.
- Ein **Attributzertifikat** dagegen enthält selbst keinen öffentlichen Schlüssel, sondern verweist lediglich in eindeutiger Weise auf ein Public-Key-Zertifikat. Es wird verwendet, um einem Public-Key-Zertifikat weitere Daten (Attribute) zuzuweisen, also z.B. dass der Zertifikatsinhaber Arzt ist.

Qualifiziertes Zertifikat

Ein qualifiziertes Zertifikat ist ein Zertifikat, das von einem Zertifizierungsdienstanbieter gemäß Signaturgesetz (SigG) für natürliche Personen ausgestellt wird. Die detaillierten Inhalte eines qualifizierten Zertifikats ergeben sich aus § 7 SigG. Insbesondere muss die Identifizierung eines Signaturschlüsselinhabers anhand eines amtlichen Ausweises erfolgen.

Cross-Zertifikat

Ein Cross-Zertifikat ist ein Zertifikat, das eine Zertifizierungsinstanz für eine andere Zertifizierungsinstanz ausstellt.

Zertifikatsinfrastruktur

Synonym für Public-Key-Infrastruktur.

Zertifizierungsdienstanbieter (ZDA) / Zertifizierungsinstanz / Zertifizierungsstelle / CA (Certification Authority) / Trustcenter

Zertifizierungsdienstanbieter sind im Bereich des Signaturgesetzes (SigG) vertrauenswürdige Instanzen, die Zertifikate z.B. für elektronische Arztausweise ausgeben, mit denen elektronische Dokumente (z.B. das elektronische Rezept digital signiert werden können. In Deutschland unterliegt die Ausgabe von qualifizierten Zertifikaten der Überwachung einer zuständigen Behörde, der Bundes-

netzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Hier muss sich jeder Zertifizierungsdienstanbieter akkreditieren lassen.

Bundesnetzagentur (BnetzA)

Die Bundesnetzagentur ist die Rechtsnachfolgerin der Regulierungsbehörde für Telekommunikation und Post (RegTP). Sie ist in Deutschland für die Überwachung der Ausgabe von qualifizierten Zertifikaten zuständig und akkreditiert Zertifizierungsdienstanbieter. Dazu betreibt sie eine nationale Wurzelzertifizierungsstelle (Root-CA). Diese Root-CA stellt der Bundesnetzagentur nur Zertifikate für akkreditierte Anbieter von qualifizierten Zertifikaten aus.

RegTP

Siehe Bundesnetzagentur.

Root-CA

Eine Root-CA (oder auch Root bzw. Root-Instanz) ist die so genannte Wurzel- bzw. oberste Zertifizierungsinstanz. Der Begriff setzt sich zusammen aus Root (englisch für Wurzel, steht hier für die oberste Zertifizierungsinstanz in einer PKI-Hierarchie) und CA, der Abkürzung für **C**ertification **A**uthority, zu deutsch Zertifizierungsinstanz. In Deutschland wird sie für das Gesundheitswesen von der Bundesnetzagentur betrieben und überwacht.

Root-Infrastruktur

Synonym für Public-Key-Infrastruktur.

Registrierungsinstanz / Registrierungsstelle

Vertrauenswürdige Stelle, die die Identität eines Antragstellers für Zertifikate nach festgelegten Regeln prüft und die Daten an den Zertifizierungsdienstanbieter (ZDA) weiterleitet.

Signaturgesetz (SigG)

Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001 (letztmalig geändert am 26. Februar 2007). Es regelt den rechtlichen Rahmen der Anwendung von elektronischen Signaturen.

Verzeichnisdienst

Ein Verzeichnisdienst ist Bestandteil einer Public-Key-Infrastruktur (PKI). Hier werden die öffentlichen Schlüssel aller zertifizierten Teilnehmer online zur Verfügung gestellt, um die Authentizität des Absenders einer verschlüsselten Nachricht feststellen zu können.

Versichertenstammdatendienst (VSDD)

Der Versichertenstammdatendienst ist ein zentraler Bestandteil der neuen Telematikinfrastruktur. Er organisiert rund um die Uhr den Datenabgleich innerhalb des gesamten Systems. Somit bleiben die Stammdaten der Versicherten immer auf dem aktuellen Stand. Wenn sich künftig z.B. die Adresse ändert oder sich ein Patient in ein Versorgungsprogramm seiner Krankenkasse einschreibt, muss die Gesundheitskarte nicht ausgetauscht werden, stattdessen wird der Datensatz online aktualisiert.

Verschlüsselung / Entschlüsselung

Dokumente zu verschlüsseln dient dem Schutz vor unautorisierten Zugriffen. Dabei werden die Daten durch Algorithmen bearbeitet (z. B. können die Buchstaben um eine bestimmte Anzahl Stellen im Alphabet verschoben werden, bei der Entschlüsselung wird dieser Vorgang rückwärts vollzogen). Abhängig davon, wie sicher die Übertragung der Daten sein soll, sind zwei verschiedene Verschlüsselungsarten möglich:

- Verwenden Sender und Empfänger denselben Schlüssel bzw. Algorithmus zum Ver- und Entschlüsseln, spricht man von **symmetrischer Verschlüsselung**. Der Nachteil liegt darin, dass Sender und Empfänger eine vor Dritten sichere Möglichkeit haben müssen, sich auf den gemeinsamen Schlüssel zu verständigen. Diese Möglichkeit existiert aber in der Regel so nicht.
- Von **asymmetrischer Verschlüsselung** spricht man, wenn mittels eines Computers zwei Schlüssel generiert werden – einer zum Ver- und einer zum Entschlüsseln. Beide stehen in einer mathematischen Beziehung zueinander, aus einem allein lässt sich der andere aber nicht ableiten. Interessant ist hierbei vor allem der Algorithmus zur Entschlüsselung: Wird der Algorithmus zum Verschlüsseln häufig vom Empfänger öffentlich zur Verfügung gestellt (ein so genannter öffentlicher Schlüssel = *Public Key*), so muss der Algorithmus zum Entschlüsseln (der private Schlüssel = *Private Key*) gut geschützt sein – er erst ermöglicht es, die Daten wieder lesbar und somit nutzbar zu machen. Diese Form der Verschlüsselung wird auch Public-Key-Kryptografie genannt.

Public Key (Öffentlicher Schlüssel)

Der so genannte öffentliche Schlüssel wird bei der asymmetrischen Verschlüsselung eingesetzt. Er ist ein Bestandteil des Schlüsselpaares. Im Gegensatz zu dem privaten Schlüssel – dem anderen Schlüssel – muss dieser nicht geheim gehalten werden und wird zum Beispiel im Zertifikat des Eigentümers verbreitet.

Private Key (Privater Schlüssel)

Der private Schlüssel ist der Teil eines kryptografischen Schlüsselpaares, auf den nur der Inhaber des Schlüsselpaares zugreifen kann. Er wird z.B. auf dem elektronischen Arztausweis gespeichert und verwendet, um digitale Signaturen zu erstellen bzw. Daten zu entschlüsseln.

Public-Key-Infrastruktur (PKI) / Zertifikatsinfrastruktur / Root-Infrastruktur

Unter diesen Begriff fällt all das, was nötig ist, um kryptografische Schlüsselpaare (private und öffentliche Schlüssel) zu verwalten. Zu den wesentlichen Kernkomponenten einer PKI zählen die Registrierungsinstanz, die Zertifizierungsinstanz und der Verzeichnisdienst.

Public-Key-Kryptografie

Synonym für die asymmetrische Verschlüsselung.

Public-Key-Zertifikat

Siehe Zertifikat.

X.509

International standardisiertes Format für Zertifikate.

Anonymisierung

Bei der Anonymisierung – einem Verfahren zum Datenschutz – werden personen-bezogene Daten derart verschlüsselt, dass ein Rückschluss darauf, zu welcher Person diese Daten ursprünglich gehören, nicht mehr möglich ist. Die Anonymisierung kommt zum Beispiel für Statistiken zum Einsatz.

Pseudonymisierung

Die Pseudonymisierung ist ein Verfahren zum Datenschutz, das personenbezo-gene Daten ähnlich wie bei der Anonymisierung so verändert, dass nicht ersicht-lich ist, zu welcher Person diese Daten gehören. Jedoch kann durch die Vergabe eines Pseudonyms (z.B. einer eindeutigen ID-Nummer) die Zuordnung unter bestimmten Voraussetzungen später wieder hergestellt werden. Generell aber darf bei der Pseudonymisierung die Zugehörigkeit von Daten, Pseudonym und natürlicher Person für Unbefugte praktisch nicht nachvollziehbar sein.

Authentifizierung*

Authentifizierung bezeichnet den Vorgang, die Identität einer Person (oder auch eines Rechnersystems) an Hand eines bestimmten Merkmals zu überprüfen. Die Authentifizierung stellt die Frage: Ist das die Person, die sie vorgibt zu sein? Dies geschieht in der Regel durch die digitale Signatur. Synonym: Identitätsüberprü-fung.

Authentisierung*

Dies ist ein Verfahren zum Nachweis einer Identität (Beispiel: Passwortabfrage beim Starten des). Die Authentisierung beantwortet die Frage: Bin ich die Per-son, die ich vorgebe?

Identifizierung

Bei diesem Verfahren wird geprüft, ob personenbezogene Daten (z.B. auf der elektronischen Gesundheitskarte) mit einer natürlichen Person übereinstimmen.

Interoperabilität

Interoperabilität beschreibt die Fähigkeit verschiedener Systeme und/oder Tech-nologien zusammenzuarbeiten. Das verlangt notwendig die Einhaltung gemein-samer Standards, etwa den DICOM-Standard bei bildgebenden medizinischen Geräten. In der Gesundheitstelematik garantiert die Interoperabilität der verwen-deten Systeme einen reibungslosen Daten- und Informationsfluss zwischen den beteiligten Ärzten, Apothekern usw.

Konnektor

Ein Konnektor steuert den Datenaustausch zwischen der Software einer Arztpra-xis (dem so genannten „Primärsystem des Leistungsträgers“) und der Telematik-infrastruktur des Gesundheitswesens. Mit seiner Hilfe werden die Zugriffe auf die elektronische Gesundheitskarte und den elektronischen Arztausweis über die Kartenterminals koordiniert sowie die Netzanbindung zur Verfügung gestellt. Der Konnektor stellt außerdem sicher, dass von Seiten der Telematikinfrastruktur auf das lokale Netzwerk des jeweiligen Primärsystems (z.B. Arztpraxis, Apotheke usw.) kein Zugriff erfolgen kann. Das heißt, er baut keine Verbindungen auf, die nicht durch einen lokalen Zugriff angestoßen worden sind (einseitige Zugriffs-

* Im Englischen werden die beiden Begriffe nicht unterschieden.

möglichkeit ausschließlich berechtigter Personen). Damit sind die Patientendaten vor möglichen illegalen Zugriffen (z.B. von Hackern) zusätzlich geschützt.

Smart Card

Smart Card ist ein anderer Begriff für „Chip-Karte“ oder „Integrated Circuit Card“ (ICC). Eine solche Karte (oder auch Card) besteht aus Kunststoff und ist mit einem Chip ausgerüstet, auf dem z.B. persönliche Daten des Besitzers gespeichert werden können. Sie sind bereits heute in Form von Telefon-, Kunden- und EC-Karten ein täglicher Begleiter. Die Gesundheitskarte wird es in Zukunft sein.

Kartenterminal

Technische Apparatur zum Kontaktieren der im System verwendeten Chipkarten.

Schnittstelle

Eine Schnittstelle ist die Verbindung zweier Systeme oder Systemkomponenten, die der gemeinsamen Kommunikation dient. In der Gesundheitstelematik sind die so genannten Softwareschnittstellen von Bedeutung: Sie ermöglichen es, Befehle und Daten zwischen verschiedenen Programmen oder Datenträgern auszutauschen. Zu den allgemein verbreiteten Softwareschnittstellen gehören ODBC, Twain oder CORBA.

DICOM

Digital **I**maging and **C**ommunications in **M**edicine (DICOM) ist ein weltweit offener Standard zum Austausch von digitalen Bildern in der Medizin. Das betrifft sowohl das Format zur Speicherung als auch das Kommunikationsprotokoll zum Austausch von Bilddaten. Die meisten Hersteller von medizinisch bildgebenden Systemen wenden für ihre Geräte den DICOM-Standard an. Dadurch wird im klinischen Umfeld Interoperabilität zwischen medizinischen Systemen verschiedener Hersteller erreicht.

PACS

PACS steht für **P**icture **A**rchiving and **C**ommunication **S**ystem und bezeichnet ein in der Medizin verwendetes Bildarchivierungs- und Kommunikationssystem. Die Abkürzung „Pacs“ wird inzwischen wie ein eigenes Wort verwendet. Pacs-Systeme erfassen vor allem Bilddaten aus der Radiologie und der Nuklearmedizin, grundsätzlich kommen aber auch Bilder aus anderen Bereichen (z.B. Endoskopie, Kardiologie, Pathologie, Mikrobiologie) für die Pacs-Verarbeitung in Frage. Die Bilder werden zusammen mit Informationen zur Identität des Patienten sowie zur klinischen Fragestellung und den durchgeführten Untersuchungen auf einem zentralen Serversystem gespeichert. Alle modernen Systeme arbeiten mit standardisierten Kommunikationsprotokollen und Speicherformaten (DICOM), wodurch verschiedene Pacs-Komponenten und Diagnosegeräte herstellerunabhängig genutzt werden können. Für die Gesundheitstelematik bedeutet dieses Verfahren einen schnellen und unkomplizierten Bilddatentransfer zwischen verschiedenen Einrichtungen mit eindeutiger Zuordnung zum Patienten.

© Hartmannbund

Verband der Ärzte Deutschlands e. V.
Schützenstraße 6a
10117 Berlin

Ansprechpartner: Katja Kraher

Telefon (030) 20 62 08 – 0

Telefax (030) 20 62 08 – 29

E-Mail hb-info@hartmannbund.de

Internet www.hartmannbund.de