ATG

Gesellschaft für
Versicherungswissenschaft
und -gestaltung e.V.

GVG

Management-Papier *„Sicherheitsinfrastruktur“*

Aktionsforum Telematik im Gesundheitswesen

Köln, Mai 2001

Zur Vorlage für den GVG-Ausschuss
„Telematik im Gesundheitswesen“ am 11.06.2001

Kontakt:
Jürgen Dolle (Koordinierung), GVG
mailto: j.dolle@gvg-koeln.de

Autoren-Team:
Dr. Hamid Farroukh, ABDA (*Meilensteine 1-2*)
Harald Flex, ITSG
Reinhold Mainz, KBV
Rudolf Meinert/Jürgen Völlink, DKG
Irmgard Siebert, KZBV
Wolfgang Strobel, AOK-BV

Das Team bedankt sich bei allen Experten, die im Rahmen von Sitzungen des ATG-Plenums, des ATG-Forums oder in Form schriftlicher Stellungnahmen oder Anhörungen wertvolle Kommentare zu Entwürfen abgegeben haben.

Inhaltsverzeichnis

Vorwort

Die das ATG tragenden Organisationen haben es sich zum Ziel gesetzt, durch einen sektorenübergreifenden Einsatz moderner Informationstechnologie (IT) in ausgewählten Bereichen des Gesundheitswesens die Qualität der medizinischen Versorgung zu optimieren, patientenorientierte Angebote zu verbessern und Wirtschaftlichkeitspotentiale im Gesundheitssystem zu erschließen. Hierzu bedarf es übergreifender Vereinbarungen, die den Aufbau einer flächendeckenden Telematikinfrastruktur, die Rahmenbedingungen für informationstechnische Anwendungen und die technisch-organisatorischen Grundlagen für den Einsatz interoperabler Lösungen schaffen. Damit können Verfahrensabläufe und Datenlage aller Beteiligten nachhaltig verbessert werden.

Der Sachverständigenrat für die Konzertierte Aktion im Gesundheitswesen beklagt bereits in seinem Sondergutachten 1997 die derzeitige andauernde Misere:

> *„Das Fehlen flächendeckend akzeptierter Standards und durchgängig kompatibler Kommunikationsprozesse verhindert die Ausschöpfung großer Rationalisierungspotentiale im Gesundheitswesen.“*

Vor diesem Hintergrund wurde 1999 das „Aktionsforum Telematik im Gesundheitswesen“ (ATG) als Initiative der Selbstverwaltung unter dem Dach der „Gesellschaft für Versicherungswissenschaft und –gestaltung e.V.“ (GVG) gegründet. Das ATG findet die Unterstützung u. a. des Bundesministeriums für Gesundheit.

In Auftrag gegebene Managementpapiere zu den Themen

⇒ Elektronisches Rezept

⇒ Elektronischer Arztbrief

⇒ Sicherheitsinfrastruktur

⇒ Europäische und Internationale Perspektiven von Telematik im Gesundheitswesen

liegen inzwischen vor.

Sie zeigen eindrucksvoll die Notwendigkeit einheitlicher Verfahrensnormen, können als Grundlage für verbindliche Beschlüsse der Selbstverwaltungsorgane dienen und Grundlage für politisches Handeln sein. Jeder hier eingesetzte Geldbetrag bewirkt relativ kurzfristig ein Vielfaches an Einsparungen und/oder Verbesserungen in der Prozess- sowie Datenqualität. Mit dem ATG verfolgen die Selbstverwaltungsorganisationen eine Strategie des stufenweisen Vorgehens hinsichtlich von im Konsens erarbeiteten kurz- oder mittelfristigen Aufgabenstellungen. Ziel ist der schrittweise Aufbau einer Telematikplattform.

Das Aktionsforum hat bereits unter Beweis gestellt, dass es interessenübergreifend die Entscheidungsprozesse im nationalen Gesundheitssystem herstellen kann, indem mit den zuständigen Akteuren die optimalen Lösungswege herausgearbeitet und dann als gemeinsame, verbindliche Vorgehensweisen vorgeschlagen werden. Seine Arbeit wirkt dem Auseinanderstreben entstehender informationstechnischer Lösungen entgegen und unterstützt die Beteiligten nachhaltig in ihrem Vorhaben, eine gemeinsame Telematikplattform aufzubauen. Die langfristige Strategie soll ebenfalls im Konsens erarbeitet und festgelegt werden. Dabei wird u. a. auch die Art der Realisierung einer einrichtungsübergreifenden Behandlungsdokumentation (elektronische Patientenakte) als zukünftiges Kernelement einer sektorübergreifenden Kooperation zu diskutieren sein.

Dabei wird sich zeigen, wie wertvoll zentral moderierte Konsenslösungen für alle Beteiligten sind. Voraussetzung ist allerdings, dass sich die Erkenntnis durchsetzt:

> *„Abgesprochene Konzepte, eine gemeinsame Infrastruktur und vereinbarte IT-Standards haben Vorteile für alle Beteiligten!“*

Dr. Herbert Rische, BfA	Dr. Manfred Zipperer	Jürgen Dolle, GVG
Vorsitzender GVG	Vorsitzender ATG	Koordinator ATG

0 Zusammenfassung („Management Summary“)

0.1 Zielgruppe

Die Empfehlungen dieses Papiers richten sich an das Management der Selbstverwaltungen des Gesundheitssystems und an die Regierungen des Bundes und der Länder.

Sie beschreiben die zunächst erforderlichen Maßnahmen zum Aufbau einer Telematikinfrastruktur, hier speziell einer Sicherheitsinfratruktur, als wesentlichem Teil einer Telematik-Plattform und als Basis von Anwendungen.

Insbesondere die Ausführungen in der Anlage und im Anhang geben aber auch interessierten Kreisen konkrete Hinweise auf sinnvolle Formen der Realisierung der untersuchten Anwendungen, ohne bereits ein Konzept vorwegnehmen zu wollen und zu können.

0.2 Vorgehensweise des Teams

Das Team Sicherheitsinfrastruktur hat seine Arbeit aufgebaut auf einer Kommunikationsanalyse für die beiden Anwendungen „Elektronischer Arztbrief“ (eArztbrief) und „Elektronisches Rezept“ (eRezept).

Diese Analyse wurde auftragsgemäß eingeschränkt auf Transportszenarien, d. h. die Betrachtung einrichtungsübergreifender elektronischer Patientenakten (einschließlich einer Dokumentation verordneter und/oder ausgegebener Arzneimittel) und die vertiefte Betrachtung von Statistik-, Abrechnungs- oder Archivierungsdiensten wurde bewusst ausgeklammert.

Durch Verallgemeinerung der untersuchten Szenarien und die Ergänzung allgemeiner Realisierungsaspekte war eine Problemanalyse möglich, deren Ergebnisse auch über die betrachteten Anwendungen eArztbrief und eRezept hinaus gültig sind.

Auf dieser Grundlage wurden Lösungsansätze aufgezeigt und schließlich problembezogene Maßnahmenvorschläge sowie organisationsbezogene Maßnahmenvorschläge gemacht.

0.3 Erkannte Probleme

Die erkannten Problemfelder lassen sich gliedern in

- die Sicherheit der (an öffentliche Netze) angeschlossenen Systeme,
- die vertrauenswürdige, sichere und rechtssichere elektronische Kommunikation zwischen im Gesundheitssystem Tätigen, unterteilt in

  - Kommunikation mit einer bekannten natürlichen Person als Empfänger einer Nachricht,
  - Kommunikation mit einer Organisationseinheit,
  - Kommunikation mit einer natürlichen Person, die erst später vom Patienten bestimmt wird,

- die Kommunikation mit dem Bürger,
- die Anonymisierung oder Pseudonymisierung von Daten.

0.4 Lösungsansätze

Die Sicherheit der an (offene) Netze angeschlossenen Systeme soll bei extern erbrachten Firewall-Services durch Kontrollverfahren garantiert werden.

Die elektronische Kommunikation soll zwischen im Gesundheitssystem Tätigen mittels E-Mail unter speziellen Absprachen für das Gesundheitssystem oder - wenn der Empfänger noch nicht bekannt ist - durch Transport einer Berechtigung in Form eines kryptografischen Datenobjekts (Ticket) auf einem geeigneten, nicht personengebundenen Transportmedium erfolgen. Der Patient – oder ein Beauftragter – übergibt dieses Ticket an einen von ihm bestimmten Empfänger, der damit temporär und verschlüsselt gespeicherte Daten von einem Kommunikationsserver abholen und lokal entschlüsseln kann.

Dies bedingt

- die Ausstattung aller im Gesundheitssystem Tätigen, die elektronisch kommunizieren sollen, mit einer SmartCard („Health Professional Card“), d. h. einer Chipkarte mit elektronischer Ausweisfunktion, kryptografischen Verfahren für Digitale Signatur, Ver- und Entschlüsselung, Authentisierung, einem Lesegerät für SmartCards und geeigneter Kommunikationssoftware,
- die Etablierung einer „Public Key“- Infrastruktur auf der Grundlage einer speziellen, aber einheitlichen Sicherheitspolitik für das Gesundheitssystem unter Verwendung besonderer Attribute, welche die zweifelsfreie Identifizierung von Kommunikationspartnern und ihrer Rolle ermöglicht,
- die Definition geeigneter rechtlicher Rahmenbedingungen für die Ausgabe von „Health Professional Cards“, für die Festlegung von Standards und die Anpassung von Formvorschriften zwecks Zulassung der elektronischen Form.

Im Gesundheitswesen ist zum Schutz der Privatssphäre eine zweckbezogene Anonymisierung und Aggregation oder Pseudonymisierung von patientenbezogenen oder leistungserbringerbezogenen Daten notwendig.

0.5 Nebenaspekte

Da die elektronische Kommunikation bei den betrachteten Anwendungen eArztbrief und eRezept zwischen im Gesundheitssystem Tätigen stattfinden kann, ist eine Ausstattung des Patienten zum Zwecke der elektronischen Kommunikation mit ihm hierbei nicht erforderlich. Sie ist dennoch optional möglich, sofern die entsprechen-

den Standards eingehalten werden. Der – ggf. durch Selbstausstattung – geeignet ausgestattete Patient kann an der elektronischen Kommunikation beteiligt werden.

Hieraus resultiert, dass derzeit keine neue Krankenversichertenkarte für die betrachteten Anwendungen ausgegeben werden muss.

Sofern die zukünftige Ausstattung des Patienten mit einer „Krankenversichertenkarte“ oder „Gesundheitskarte“ geplant ist, sollte dies ebenfalls in Form einer SmartCard erfolgen, die zunächst aber ausschließlich der Identifizierung des Patienten dienen muss. Dem Patienten zugeordnete Daten können dann für Berechtigte aus dem Netz verfügbar gemacht werden. Solange dem Patienten keine für das Gesundheitssystem spezifische, einheitliche und lebenslang eindeutige Kennung zugeordnet werden soll - was bei der Diskussion zu einem Pseudonymisierungskonzept zu erörtern wäre – könnte jede vom Patienten benutzte, geeignet standardisierte SmartCard (z. B. Bankenkarte) zur Identifizierung verwendet werden. Eine spezielle Chipkarte des Gesundheitssystems für den Patienten würde besonders dann Sinn machen, wenn zusätzlich stabile Informationen (z. B. Blutgruppe, Allergien) auf einer solchen Karte untergebracht würden.

0.6 Problembezogene Maßnahmenvorschläge

Folgende Maßnahmen sollten sofort ergriffen werden:

- Erstellung eines Konzepts für eine Kommunikations- und Sicherheitsinfrastruktur,
- Realisierung eines technischen Demonstrators für eine vertrauenswürdige, sichere und rechtssichere elektronische Kommunikation,
- Aufstellung eines Projektplans für den flächendeckenden Aufbau der Infrastruktur einschließlich der Schaffung erforderlicher rechtlicher oder vertraglicher Grundlagen,
- Planung und Beschreibung neuer organisatorischer Aufgaben und gemeinsamer Betriebseinrichtungen zur Etablierung einer „Public Key“- Infrastruktur, für die Ausgabe von „Health Professional Cards“, für die Erarbeitung und Durchsetzung von Standards, für die Überwachung der Softwarequalität und zur Durchführung von Kontrollaufgaben,
- Erstellung zweckgebundener Pseudonymisierungskonzepte.

0.7 Allgemeine Maßnahmenvorschläge

Die nachfolgenden organisatorischen Empfehlungen dienen der erforderlichen Professionalisierung der Umsetzung im Kontext der Empfehlungen der anderen ATG-Teams.

Der Aufbau einer Infrastruktur ist eine gesellschaftliche Aufgabe. Die einmalige Finanzierung des Aufbaus der Infrastruktur sollte durch die Regierungen des Bundes und der Länder gemeinsam geschehen. Die Finanzierung der Anwendungen könnte dann durch die Partner der Selbstverwaltung erfolgen.

Die Realisierung erster Anwendungen zur Nutzung der Infrastruktur sollte durch gemeinsame Projekte mit anteiliger Finanzierung erfolgen.

Für den Betrieb einer (Sicherheits-) Infrastruktur können gemeinsame Betriebseinrichtungen (z. B. die oberste Instanz einer Zertifizierungshierarchie) sinnvoll sein.

Die einzelnen Projekte sollten in Verantwortung der jeweiligen Projektbeteiligten unter der Steuerung eines Lenkungsausschusses durchgeführt werden.

Die koordinierende Begleitung aller Projekte zur Etablierung und Nutzung der Telematik-Plattform kann vom Aktionsforum Telematik im Gesundheitswesen (ATG) übernommen werden.

1 Einleitung

Meilenstein 3

Eine vertrauenswürdige elektronische Kommunikation mit den besonderen Anforderungen des Gesundheitssystems bedarf – da sie einrichtungs-, organisations-, sektor- und grenzüberschreitend stattfinden soll, der Absprachen aller Beteiligten insbesondere zu organisatorischen, technischen, inhaltlichen sowie rechtlichen und vertraglichen Details.

Eine Kommunikationsinfrastruktur einschließlich der bedeutsamen Sicherheitsinfrastruktur muss durch eine Arbeitsgemeinschaft des gesamten Gesundheitssystems – und in Kooperation mit den anderen Staaten der europäischen Gemeinschaft – definiert, aufgebaut und auf Dauer betrieben werden.

Obwohl weitgehend standardisierte Internet-Dienste benutzt werden können, bedarf es dennoch konkretisierender Vereinbarungen; daneben müssen sogar einzelne neue Dienste entwickelt werden.

Für den Betrieb der Infrastruktur sind sowohl neue übergreifende organisatorische Instanzen notwendig, als auch die Übernahme neuer Aufgaben durch bestehende Organisationen.

Aufbau und Betrieb der Infrastruktur als Basis für beliebige Anwendungen sind eine gesamtgesellschaftliche Aufgabe, deren Aufbau deshalb einmalig vom Staat finanziert werden sollte. Ihr erheblicher und dauerhafter Nutzen für alle Bürger schon bei der Betrachtung einiger weniger Anwendungen ist unstrittig. Deutschlands Weg in die Informationsgesellschaft mit den daran geknüpften ökonomischen und gesellschaftlichen Folgen wird stark dadurch bestimmt werden, wie rasch dieser Weg beschritten werden kann.

Von Anwendungen des Gesundheitssystems sind alle Bürger betroffen und ohne Infrastruktur werden sie nicht flächendeckend funktionieren können. Neben technischen und organisatorischen Maßnahmen ist dabei eine akzeptanzfördernde begleitende Öffentlichkeitsarbeit notwendig, welche die Bereitschaft zur Nutzung neuer Techniken sowohl bei den Berufen des Gesundheitssystems als auch bei den Bürgern fördert.

Nur durch eine gemeinsame Anstrengung von Forschung, Industrie und den verantwortlichen Organisationen des Gesundheitssystems und durch flankierende Maßnahmen der Regierung kann der Aufbau der notwendigen Infrastruktur in der gewünschten kurzen Zeitperiode durchgeführt werden. Die in diesem Jahr bereitgestellten personellen und finanziellen Ressourcen werden maßgebend dafür sein, wie schnell durch die Selbstverwaltung gestaltete flächendeckende elektronische Anwendungen zum Alltag der Patientenversorgung gehören und dadurch die erwarteten Vorteile wirksam werden lassen.

2 Vorwort und Zielsetzung

Meilenstein 1

Adressat dieses Dokuments sind die Verbände des deutschen Gesundheits- und Sozialsystems und ggfs. der Gesetzgeber.

Von der Basis der Gesundheitsberufe kommen sehr pragmatische Forderungen nach einer Verbesserung der (elektronischen) Kommunikation z. B. zur Unterstützung neuer kooperativer Versorgungsformen, deren Dynamik nicht zu unterschätzen ist.
Da diese Kommunikationsvorgänge vertrauenswürdig sind, ist zu deren elektronischer Realisierung eine Sicherheitsinfrastruktur erforderlich.

Die Akzeptanz der Telematik im Gesundheitswesen wird um so höher sein, je sicherer die technische Ausgestaltung von Anwendungen ist.

Kommunikation im Gesundheitswesen findet organisationsübergreifend statt. Deshalb muss eine Sicherheitsinfrastruktur zur Unterstützung einer elektronischen Kommunikation gemeinsam von allen Partnern des Gesundheits- und Sozialsystems, welche die elektronische Kommunikation aktiv gestalten, vereinbart werden.

Eine organisationsübergreifende elektronische Kommunikation benötigt eine von den Organisationen gemeinsam vereinbarte und verantwortete Sicherheitsinfrastruktur.

Eine Sicherheitsinfrastruktur sollte als Infrastrukturkomponente anwendungsneutral definiert und als Basis für beliebige Anwendungen aufgebaut werden. Diese Sicherheitsinfrastruktur besteht sowohl aus Rahmenbedingungen und Vorgaben als auch- zumindest teilweise - aus Komponenten, welche die Selbstverwaltung bereitstellen muss oder für die ein finanzielles Anreizsystem sinnvoll sein könnte.

Die Sicherheitsinfrastruktur ist eine allgemeine Infrastrukturkomponente, die möglichst anwendungsneutral definiert und als Basis für beliebige Anwendungen aufgebaut werden sollte. Ihr Aufbau stellt sich als Querschnittsaufgabe dar.

Dabei sind Dienste (z. B. Zertifikate, Zeitstempel) zur Unterstützung einer Kommunikations- und Informationsinfrastruktur und deren Zusammenwirken mit Prozessen zu beschreiben. Diese Beschreibung umfaßt auch eine Sicherheitspolitik (Policy), Organisationsstrukturen für Vertrauenswürdige Stellen (Trust Center) und Elemente zur Benutzung der Infrastruktur (z. B. Hard- und Softwarekomponenten).

Ein wesentliches Ziel der Sicherheitsinfrastruktur ist die sichere, rechtssichere und vertrauenswürdige Kommunikation, deren Erfüllung beispielsweise durch die Dienste „Digitale Signatur“ und „Verschlüsselung“ erreicht werden soll.

Wesentliches Ziel der Sicherheitsinfrastruktur ist die Unterstützung einer sicheren, rechtssicheren und vertrauenswürdigen elektronischen Kommunikation und der Schutz der Privatsphäre.

Daneben sind auch Dienste zur Anonymisierung und Pseudonymisierung zu betrachten, die besonders geeignet sind, den Schutz der Privatsphäre zu sichern.

Ziel dieses Managementpapiers ist es,

- den Handlungsbedarf für den Aufbau einer einheitlichen und flächendeckenden Sicherheitsinfrastruktur im Gesundheitswesen aufzuzeigen,
- diese Infrastruktur global zu beschreiben und

ausgehend von den vorhandenen Lösungen und Konzepten Wege für eine Umsetzung aufzuzeigen.

Der Handlungsbedarf und die Handlungsalternativen für den Aufbau einer einheitlichen, flächendeckenden Sicherheitsinfrastruktur als wesentlicher Bestandteil einer Kommunikationsinfrastruktur soll aufgezeigt werden.

3 Definition und Abgrenzung des Themas

Meilenstein 1

Eine Telematik-Infrastruktur (Plattform) besteht in ihren technisch-organisatorischen Kernelementen aus den Komponenten Sicherheitsinfrastruktur, Kommunikationsinfrastruktur und Informationsinfrastruktur. Diese Komponenten bilden eine Gesamtarchitektur für informationstechnische Anwendungen.

0. Sicherheitsinfrastruktur

   Von der Sicherheitspolitik (Policy) bis zur Festlegung der Details von kryptografischen Verfahren müssen verbindliche Regeln abgestimmt werden.

1. Kommunikationsinfrastruktur

   Von einer allgemeinen Dienste-Infrastruktur über abgestimmte Basis-Dienste bis hin zu Verzeichnisdiensten sind verbindliche Definitionen für interoperable Verfahren erforderlich.

2. Informationsinfrastruktur

   Von Minimalanforderungen an die medizinische Dokumentation und die Strukturierung sowie Definition von Basiselementen für die technische Kommunikation bis hin zu technischen Elementen einer transparenten Speicherung und vertrauenswürdigen Verarbeitung sind verbindliche Festlegungen notwendig.

Die hier betrachtete Sicherheitsinfrastruktur dient der Sicherheit und Vertrauenswürdigkeit des Informationsaustausches zwischen den Kommunikationspartnern sowie dem Schutz der Privatsphäre. Dabei ist nicht nur der Kommunikationsvorgang selbst, sondern auch die Sicherheit und Vertrauenswürdigkeit der informationstechnischen Umgebung in die Betrachtung einzubeziehen.

Die informationelle - elektronisch unterstützte - Vernetzung des Gesundheitswesens stellt besondere Anforderungen an die Verfügbarkeit, Integrität, Verbindlichkeit und Vertraulichkeit von Informations- und Kommunikationsvorgängen.

Eine Sicherheitsinfrastruktur stellt organisatorische und technische Elemente und Dienste zur Verfügung, die Sicherheit und Vertrauenswürdigkeit beim Einsatz von Informations- und Kommunikationstechnik gewährleisten sollen.

Neben rein technisch-organisatorischen Aspekten müssen auch rechtliche – insbesondere datenschutzrechtliche – Rahmenbedingungen betrachtet werden, da es auch um die Zulässigkeit bestimmter elektronischer Transaktionen geht. Dieses Dokument beschäftigt sich jedoch schwerpunktmäßig mit den technisch-organisatorischen Aspekten.

Zu den Kernelementen einer Sicherheitsinfrastruktur für das Gesundheitswesenzählen:

- autorisierte organisatorische Stellen zur Ausgabe von elektronischen Ausweisen/ Zertifikaten,
- elektronische Ausweise für die beteiligten Personen (Patienten, "Health Professionals" und andere Beteiligte) einschließlich der Darstellung von deren Organisationszugehörigkeit,
- Verfahren/Regeln zur Authentisierung sowie zur Verschlüsselung und Signierung von Daten,
- Verfahren/Regeln zur Sicherung von Anwendungen und Transportwegen.

Dieses Dokument behandelt ausschließlich Elemente, Dienste und Funktionen einer Sicherheitsinfrastruktur, die einen vertrauenswürdigen und sicheren Informationstransport zwischen Beteiligten im Gesundheitswesen ermöglichen. Hierzu gehören auch Dienste zum Schutz der Privatsphäre, wie Anonymisierung und Pseudonymisierung. Beteiligte an Kommunikationsvorgängen sind dabei natürliche Personen, Organisationen/Institutionen und technische Systemkomponenten.

Die Sicherheit der beteiligten Systeme selbst liegt in der Verantwortung der diese betreibenden Organisationen. Hierfür können lediglich Empfehlungen ausgesprochen werden.

Die Sicherheit der angeschlossenen beteiligten Systeme bedarf einer separaten Betrachtung.

Die Infrastruktur soll - auf der Basis von Standards - für alle zukünftigen Anwendungen geeignet sein, muss jedoch vor allem die mit Priorität geplanten Anwendungen "Rezept" und "Arztbrief" abdecken. Anhand von Szenarien kann geprüft werden, ob sich die Sicherheitsinfrastruktur auch für weitere Anwendungen eignet.

Die Sicherheitsinfrastruktur soll für alle zukünftigen Anwendungen geeignet sein. Allerdings kann der Aufbau stufenweise und in erweiterbarer Weise in der Form erfolgen, dass zunächst die Bedürfnisse prioritärer Anwendungen erfüllt werden.

4 Anforderungen

Meilenstein 1

Damit zukünftige Kommunikationsbeziehungen für organisationsübergreifende Anwendungen miteinander funktionieren, bedarf es einer einheitlichen Plattform.

Als Basisinvestition für zukünftige Anwendungen muss eine einheitliche Infrastruktur aufgebaut werden.

Auf der Grundlage von einheitlichen rechtlichen, organisatorischen und technischen Regeln soll eine interoperable Sicherheitsinfrastruktur für einen übergreifenden, standardisierten Informationstransport bereitgestellt werden.

Zur Ausgestaltung einer problemlosen, organisationsübergreifenden elektronischen Kommunikation sind einheitliche rechtliche, organisatorische und technische Regeln erforderlich.

Diese Infrastruktur soll Regeln umfassen für die Feststellung der Identität/Rolle einer Person oder Organisation (Authentizität) und den sicheren Informationstransport (Integrität, Verbindlichkeit, Vertraulichkeit, Verfügbarkeit, Zugriffsschutz, differenzierte und auftragsbezogene Zugriffsrechte). Eine wesentliche Grundlage einer elektronischen Kommunikation sind dabei Adreßbücher, in denen die Kommunikationspartner sicher identifiziert werden können.

Die bei der traditionellen Informationsübermittlung geltenden Regeln müssen bei einer elektronischen Kommunikation explizit abgebildet werden. Wo die elektronische Kommunikation neue Möglichkeiten schafft, sind auch neue Regeln und Prinzipien zu definieren.

Die Sicherheitsinfrastruktur soll in ihrer Umsetzung in den Bereichen, in denen die Digitale Signatur zum Einsatz kommt, auch die Anforderungen des deutschen Signaturgesetzes erfüllen.

Die Kommunikationsvorgänge sollen in den Bereichen, in denen die Digitale Signatur zum Einsatz kommt, nach den Vorgaben des – derzeit novellierten - Signaturgesetzes abgesichert werden, so dass auch eine rechtssichere elektronische Kommunikation möglich wird.

5 Bestandsaufnahme

Meilenstein 1

5.1 Ist-Situation

5.1.1 Beschreibung der Ist-Situation

Die bestehenden Anwendungen im Gesundheits- und Sozialsystem benutzen derzeit keine organisationsübergreifende, flächendeckende, gemeinsame technische Infrastruktur.

Es gibt derzeit keine flächendeckend von allen Organisationen des Gesundheits- und Sozialsystems benutzte Sicherheitsinfrastruktur für die elektronische Kommunikation.

Allerdings gibt es bereits Anwendungen, die sich einer Sicherheitsinfrastruktur bedienen.

Die Gesetzlichen Krankenkassen, die Sozialversicherungen und die Leistungserbringer tauschen heute Daten in dem jeweils zugelassenen Umfang auf maschinell verwertbaren Datenträgern oder mittels Datenfernübertragung aus. Diese Datenlieferungen bilden die Grundlage u.a. für die Genehmigung und Zahlung von Leistungen. Entsprechende Verträge zwischen den Organisationen regeln den technischen Rahmen und die Verfahren zum Schutz der Datenübertragungen. Darüber hinaus gibt es eine Reihe konzeptioneller Überlegungen und Vorarbeiten zur Migration des bestehenden Verfahrens und Anpassung der Sicherheitsinfrastruktur an die aktuellen Entwicklungen.

Es gibt am Markt und bei einigen Organisationen des Gesundheits- und Sozialsystems grundsätzlich geeignete Sicherheits-infrastrukturen, die zum Teil spezifischen Anwendungen dienen und im Rahmen des Aufbaus einer gemeinsame Infrastruktur auf der Basis von Interoperabilitätsstandards vereinheitlicht werden müssen.

Komponenten einer zukünftigen Sicherheitsinfrastruktur sind in hieran interessierten Kreisen – zum Teil auch bereits im Konsens – beschrieben worden. Auf diesen Arbeiten kann aufgebaut werden. Allerdings liegt der Schwerpunkt nicht auf der Vervollständigung der technischen Arbeiten, sondern bei der Bewertung der Ergebnisse und bei konkreten Festlegungen. Als Beispiele für bereits weithin akzeptierte technische Festlegungen seien zum Zeitpunkt der Erstellung dieser Dokumentation genannt: SSL für die sichere Kommunikation zwischen Anwendungen oder Rechnern, S/MIME als Transportprotokoll für elektronische Post, Triple DES für eine symmetrische Verschlüsselung, RSA mit einer Schlüssellänge von mindestens 1024 Bit für die asymmetrische Verschlüsselung, SHA-1 oder RIPEMD160 als Hash-Verfahren, Zertifikatstrukturen gem. X.509V3, Chipkartenterminals gem. MKT-Spezifikation.

In einigen regionalen Projekten in Deutschland (z. B. Krebsregister Magdeburg, QuasiNiere) wurden exemplarisch Sicherheitsinfrastrukturen implementiert, die als Muster für eine flächendeckende Infrastruktur in die Betrachtungen einbezogen werden können.

Auf nationaler, europäischer und internationaler Ebene wurden in den letzten Jahren eine Vielzahl von Normen und Normentwürfen erarbeitet, die als Grundlage für den Aufbau einer Telematik-Infrastruktur benutzt werden können. Diese Arbeiten sind nicht abgeschlossen.

Erste Vorschläge für Interoperabilitätsstandards existieren. Diese Vorschläge müssen bei der weiteren Arbeit berücksichtigt werden.

Allerdings liegt der Schwerpunkt im Gesundheitssystem nicht auf der Vervollständigung der technischen Arbeiten, sondern bei der Bewertung der Ergebnisse und bei konkreten Festlegungen.

5.1.2 Bewertung der Ist-Situation

Heute wird im Gesundheitssystem bereits umfangreich und teilweise ohne die rechtlich erforderliche und technisch mögliche Sicherheit elektronisch kommuniziert. Diese Situation bedarf dringend einer Änderung.

Zur Herstellung der rechtlich gebotenen vertrauenswürdigen und sicheren elektronischen Kommunikation sind Maßnahmen erforderlich.

Zum Aufbau einer gemeinsamen Sicherheitsinfrastruktur sind Vereinbarungen zur interoperablen Verbindung von separaten Sicherheitsinfrastrukturen erforderlich.

Beispiele für möglicherweise geeignete Sicherheitsinfrastrukturen existieren in einigen Projekten.

Diese Vereinbarungen und die Anforderungen aus neuen Anwendungen haben die Anpassung und Erweiterung vorhandener Sicherheitsinfrastrukturen zur Folge.

Vorhandene Sicherheitsinfrastrukturen der Selbstverwaltung bedürfen der Anpassung.

Die beteiligten Organisationen müssen die Benutzung der Sicherheitsinfrastruktur daneben in einem Rahmenwerk beschreiben.

Die Verwendung der Sicherheitsinfrastruktur ist organisationsspezifisch in einem Rahmenwerk zu beschreiben.

Für die Benutzung einer einheitlichen Infrastruktur und für interoperable Verfahren bedarf es vor allem vereinbarter Standards für eine offene, übergreifende elektronische Kommunikation. Diese Standards sollten grundsätzlich auf der Basis von (internationalen) Normen, können aber auch auf der Basis von Normentwürfen oder auf der Grundlage allgemein akzeptierter Firmenstandards festgelegt werden. Normen oder Industriestandards stehen jedermann zur Anwendung frei. Es sei denn, Normen sind, z. B. durch einen Vertrag oder durch ein Gesetz, verbindlich gemacht worden. Auch Normen oder Standards definieren häufig nur einen allgemeinen Rahmen, der eine Reihe von Optionen beinhaltet. Dies bedeutet, dass bezüglich dieser Optionen Festlegungen getroffen werden müssen.

Aus (kommerziell) verfügbaren Sicherheitslösungen und auf der Grundlage von Arbeiten interessierter Kreise und von Standardisierungseinrichtungen können interoperable Sicherheitsinfrastrukturen aufgebaut werden, die durch gemeinsame Absprachen eine übergreifende Sicherheitsinfrastruktur bilden.

Bei jeder notwendigen Festlegung ist im Einzelfall zu prüfen, welche relevanten Normen oder Standards in die Überlegungen einbezogen werden sollten.

Noch ausstehenden Standardisierungsarbeiten muss ein erheblicher Stellenwert eingeräumt werden.

Auf der Grundlage existierender Normen und Standards oder auf der Basis von Entwürfen müssen jeweils eine konkrete Auswahl und konkrete Festlegungen nach einer solchen Auswahl getroffen werden, um wirklich zu einer gemeinsam nutzbaren Infrastruktur und zu interoperablen Verfahren zu kommen. Diese Festlegungen müssen ggf. in Verträgen der Selbstverwaltung für solche Anwendungen verbindlich gemacht werden, für die die Selbstverwaltung verantwortlich ist.

5.2 Rahmenbedingungen

Die besonders sensiblen Informationen (z. B. personenbezogene Gesundheitsdaten), die im Gesundheits- und Sozialsystem elektronisch kommuniziert werden sollen, bedürfen höchster Anstrengungen zur Gewährleistung der Sicherheit und Vertraulichkeit von auf ihnen beruhenden Kommunikationsvorgängen.

Die Infrastruktur muss grundsätzlich ein Sicherheitsniveau gewährleisten, dass den hohen Ansprüchen an den Schutz von personenbezogenen Gesundheitsdaten gerecht wird, wenn auch nicht alle Anwendungen ein gleich hohes Niveau benötigen.

Wegen der organisationsübergreifenden Kommunikationsvorgänge ist eine einheitliche Infrastruktur erforderlich; sie kann nur gemeinsam von allen Beteiligten definiert und aufgebaut werden. Hierzu besteht ein allgemeiner Konsens. Neben den rechtlichen, organisatorischen und technischen Fragen ist auch ein Finanzierungsmodell für gemeinsame Maßnahmen und Strukturelemente erforderlich.

Die Bereitstellung einer einheitlichen Sicherheitsinfrastruktur ist eine gemeinsame Aufgabe aller Organisationen des Gesundheits- und Sozialsystems.

Die Realisierung einer Sicherheitsinfrastruktur dient der Bereitstellung einer organisatorisch-technischen Plattform. Sie verändert keine bestehenden Strukturen oder Geschäftsprozesse, schafft aber eine Voraussetzung zu ihrer Anpassung und Weiterentwicklung. Sie dient zur Realisierung beliebiger Anwendungen und trägt hierdurch indirekt zur Veränderung von Prozessen der Gesundheitsversorgung bei.

Die Implementierung der Sicherheitsinfrastruktur kann nur im zeitlichen Zusammenhang mit einigen Anwendungen durchgeführt werden, die geeignet sind, die Infrastruktur zu finanzieren. Besonders geeignet sind solche Anwendungen, die dem gestiegenen Informationsbedürfnis bei kooperativen Versorgungsformen gerecht werden.

Die Sicherheitsinfrastruktur ist Voraussetzung für viele Anwendungen und muss deshalb für deren Realisierung bereitgestellt werden.

5.2.1 Rechtliche Dimension

Die Neufassung des Signaturgesetzes (z. Zt. erfolgt, nachdem Bundestag und Bundesrat zugestimmt hatten,die Prüfung auf Konformität zur entsprechenden EU-Richtlinie durch die Europäische Kommission) eröffnet die Möglichkeit zur Gleichstellung elektronischer Unterschriften mit eigenhändigen.

Eine verbindliche elektronische Kommunikation wird in absehbarer Zeit durch die Gleichstellung Digitaler Signaturen mit eigenhändigen Unterschriften sowohl im privaten Recht als auch im öffentlichen Recht ermöglicht.

Darüber hinaus können zur Umsetzung des Signaturgesetzes im öffentlichen Bereich zusätzliche Voraussetzungen an die Sicherheitsinfrastruktur gestellt werden (z. B. Akkreditierung der Zertifizierungsstelle). Unklar ist, ob und in wieweit das Gesundheits- und Sozialsystem zusätzlichen Anforderungen unterliegen soll.

Das Signaturgesetz ermöglicht dem öffentlichen Bereich, zusätzliche Anforderungen an die Sicherheitsinfrastruktur zur Erzeugung Digitaler Signaturen zu stellen. Es ist – im europäischen Kontext – zu prüfen, ob und welche derartigen zusätzlichen Anforderungen sinnvoll sind. Im europäischen Rahmen ist die „Reichweite“ von Rahmenbedingungen und Lösungen zu beachten.

Die Regelungen zur Sicherheit und zu den Verfahren in der Telekommunikation im Sinne der regelhaften Berufsausübung sind u. a. Gegenstand der Arbeit der zuständigen Berufsorganisationen (z. B. Kammern) auf der Leistungserbringerseite.

Deshalb wird konkret zu prüfen sein, ob und welche neuen/ergänzenden berufsrechtlichen und anderen rechtlichen Regelungen begleitend zum Aufbau einer Sicherheitsinfrastruktur erforderlich sind. Als maßgebliche „Rechtskreise“ sind insbesondere das allgemeine Gebot der Schweigepflicht für Heilberufe und die Datenschutzgesetze zu beachten (Fragen der Zulässigkeit, Anforderungen an technische und organisatorische Maßnahmen der Datensicherheit, z. B: „10 Gebote“ des § 9 BDSG i. V. mit der Anlage hierzu).

Die Sicherheitsinfrastruktur bedarf unter Umständen rechtlicher Regelungen, z. B. auf der Ebene der Berufsordnungen der Leistungserbringer.

5.2.2 Organisatorisch-technologische Dimension

Für den Aufbau einer Sicherheitsinfrastruktur gibt es heute bereits eine Reihe von Definitionen, Standards, etablierten Verfahren und Mechanismen, deren Nutzung im Hinblick auf nationale und internationale Interoperabilität unumgänglich ist.

Die Sicherheitsinfrastruktur soll deshalb zur Herstellung einer umfassenden Interoperabilität auf der Grundlage von internationalen Normen realisiert werden. Die optionalen Parameter müssen dabei zwischen allen Vertragspartnern durch konkrete und einheitliche Absprachen festgelegt werden.

Noch ausstehenden Standardisierungsarbeiten muss ein hoher Stellenwert eingeräumt werden.

Bei der Realisierung der technischen Elemente einer Sicherheitsinfrastruktur können neben kommerziellen - zum Signaturgesetz konformen - Einrichtungen auch bestehende organisatorische und technische Einrichtungen des Gesundheits- und Sozialsystems genutzt werden, sofern sie die Anforderungen an die Sicherheitsinfrastruktur erfüllen.

Organisatorische Aufgaben einer Sicherheitsinfrastruktur müssen teilweise auch von Organisationen des Gesundheits- und Sozialsystems selbst wahrgenommen werden (z. B. Ausgabe von elektronischen Ausweisen).

Aufgaben einer Sicherheitsinfrastruktur müssen zum Teil selbst wahrgenommen werden, für andere können Dienstleister in Anspruch genommen werden.

Die Benutzung einer einheitlichen Sicherheitsinfrastruktur bedarf vertraglicher Vereinbarungen aller Beteiligter, damit die erforderlichen Festlegungen verbindlich werden.

Die konkrete Ausgestaltung einer einheitlichen Infrastruktur bedarf der Absprachen zwischen allen Vertragspartnern, auch zu organisatorischen und technischen Details. Dabei geht es weniger um die technischen Definitionen als vielmehr um verbindliche Entscheidungen für deren Einsatz und um Festlegungen, wo es einen Entscheidungsspielraum gibt.

Von der Einführung einer Sicherheitsinfrastruktur sind nicht nur die Organisationen des Gesundheits- und Sozialsystems, sondern vor allem die Nutzer von Anwendungen (z. B. Ärzte, Zahnärzte, Apotheker, Angestellte in Versicherungen) einschließlich der Patienten/Versicherten betroffen.

Dabei bedürfen die elektronischen Hilfsmittel zur Ausgestaltung/Sicherung des informationellen Selbstbestimmungsrechts einer besonderen Betrachtung.

Von einer Sicherheitsinfrastruktur im Gesundheits- und Sozialwesen sind möglicherweise alle Bürger betroffen. Die Ausgestaltung ihrer Beteiligung in elektronischen Verfahren bringt neue Anforderungen mit sich.

Die derzeit vorhandene EDV-Infrastruktur muss in bezug auf die Fähigkeit zur Integration in eine Sicherheitsinfrastruktur überprüft und angepaßt werden.

Der Aufbau einer flächendeckenden Sicherheitsinfrastruktur wird daher nicht kurzfristig zu bewerkstelligen sein.

Die vorhandene informationstechnische Infrastruktur – insbesondere bei einzelnen Beteiligten (z. B. kleine Arztpraxen) – wird nur mit Schwierigkeiten in eine neue Sicherheitsinfrastruktur eingebunden werden können. Deshalb ist von Übergangszeiten auszugehen.

6 Analyse, Lösungsansätze, Realisierungsaspekte

Meilenstein 2

Damit eine Sicherheitsinfrastruktur beschrieben werden konnte, hat das Team zunächst eine Kommunikationsanalyse durchgeführt, deren Ergebnis im Anhang zur Anlage 1 zu finden ist. Sodann wurde versucht, aufgrund der konkreten Anforderungen aus den Anwendungen „Elektronischer Arztbrief“ und „Elektronisches Rezept“ und einer nachfolgenden Abstraktion den Rahmen für eine Sicherheitsinfrastruktur zu beschreiben und die erforderlichen Aktivitäten zu deren Aufbau zu analysieren. Die Ergebnisse dieser Betrachtung findet man in Anlage 1.

Wenn man spezielle Anforderungen an Anwendungslösungen ausklammert, kann das elektronische Rezept – auf seinem Transportweg – als Sonderform des elektronischen Arztbriefs betrachtet werden.

Das E-Rezept ist auf dem Transportweg eine Sonderform des E-Arztbriefs.

Als Ergebnis der Analyse wird folgendes festgestellt:

1. Ein besonderes Problem im Gesundheitssystem ist, dass in vielen Fällen (Einweisung, Überweisung, Rezept) der Empfänger einer Nachricht im Vorhinein nicht feststeht und erst durch den Patienten ausgewählt wird.

   Deshalb kann in diesen Fällen ein Informationsobjekt auf einem (temporären) Datenträger mitgegeben werden. Eine Verschlüsselung des Informationsobjekts auf dem temporären Datenträger erscheint nicht notwendig – analog zur heutigen Lesbarkeit des Papierrezepts, der Einweisung oder Überweisung.

Für im Vorhinein nicht feststehende Empfänger kann der Patient Daten oder eine Zugangsberechtigung zu Daten auf einem geeigneten Trägermedium mitnehmen.

Daten werden mittels E-Mail oder auf einem (temporär benutzten) Datenträger (z. B. Chipkarte) transportiert. Daneben können sie von einem Server abgeholt werden.

2. Der Transport von Daten kann mittels Standard-Protokollen des Internet erfolgen, z. B. E-Mail.

   Allerdings sind ergänzende Absprachen notwendig, die folgende Aspekte betreffen:

   Bestehende E-Mail-Lösungen müssen ergänzt werden.

   - Welche Verschlüsselungs- und Signaturverfahren - und deren Ausprägungen im Detail bis hin zu Inhalten und deren Darstellung in Sicherheits-Zertifikaten – werden verwendet?

     Auch hierbei kann zwar auf Standardverfahren zurückgegriffen werden, allerdings müssen ergänzende Absprachen bis hin zur Festlegung optionaler Elemente getroffen werden.

     Interoperabilität auf der Grundlage allgemeiner (generischer) Standards lässt sich nur durch zusätzliche Absprachen erreichen (Auswahl von Optionen, Definition erlaubter Ergänzungen - sog. Profilbildung).

   - Wie können Absender und Empfänger in elektronischen Adressbüchern einwandfrei identifiziert werden?

     Inhalte von Adressbüchern und Adressschemata müssen – als Teil eines Datenmodells – im Detail festgelegt werden.

   - Wie kann der Empfang einer Nachricht zuverlässig bestätigt werden?

   - Welche zusätzlichen Informationen müssen in standardisierter Form mitgegeben werden, damit eine vertrauenswürdige Zustellung elektronischer Nachrichten innerhalb einer adressierten Organisation oder Organisationseinheit in automatisierter Form erfolgen kann? Welche Informationen zur Organisationszugehörigkeit, Rolle und Vertretungsmacht müssen in einem elektronischen Adressbuch verfügbar sein?

     Die Zugehörigkeit von Personen zu Organisationseinheiten und ihre Vertretungsmacht muss in einem elektronischen Adressbuch definiert sein. Rechtssichere Kommunikationsvorgänge finden immer zwischen Personen statt, die ggfs. Organisationen (Institutionen) vertreten.

   - Wie kann für Absender und Empfänger ein eindeutiger Fallbezug oder Bezug zum Patienten hergestellt werden, welche Informationen sollten hierzu in standardisierter Form mitgegeben werden?
   - Welches Format und welche Bedeutung haben mitgelieferte Daten?

3. Es kann – z. B. wegen des Umfangs der Daten oder weil keine personenbezogenen sensiblen Daten auf einem Datenträger transportiert werden sollen – sinnvoll sein, einem Empfänger von Daten lediglich eine Berechtigung zum Abholen dieser Daten zuzusenden oder – bei zuvor noch nicht feststehendem Empfänger - auf einem Trägermedium (auch Papier) zu übergeben. Diese Berechtigung kann in Form eines sog. elektronischen Tickets gestaltet werden, die es - abgesichert durch kryptografische Verfahren – ausschließlich dem Besitzer des Tickets gestattet, bereitgestellte Informationen (z. B. einmalig) – von einem Server im Internet – abzurufen und lokal mittels des Tickets zu entschlüsseln. Derartige Tickets und Abrufverfahren sind zwar in Forschungsprojekten realisiert worden, sind aber derzeit nicht Teil von Standard-Kommunikationsverfahren im Internet.

Statt des Transports von Daten oder ergänzend dazu kann ein kryptografisch gesichertes Ticket übermittelt werden, welches den (einmaligen) Abruf von Daten und deren lokale Entschlüsselung gestattet.

Ein derartiges Abrufverfahren (Ticketverfahren) muss definiert, realisiert und als Standard-Internet-Verfahren propagiert werden.

4. Informationsobjekte können auf Servern (im Internet) auch für eine spätere Abholung durch eine jeweils festgelegte Gruppe von Berechtigten (z. B. Fachärzte für Urologie in einem Krankenhaus) abgelegt werden. Allerdings können diese dann lediglich mit einem großen Gruppen von Berechtigten verfügbaren Schlüssel verschlüsselt werden, so dass sich ein derartiges Verfahren nur als Übergangslösung bis zur Realisierung eines Ticket-Verfahrens (vgl. Nummer 3) eignet. Die Berechtigung zum Abholen könnte anhand sogenannter Attribut-Zertifikate auf einem elektronischen Ausweis (vgl. Nummer 5) geprüft werden. Gegenüber Missbrauchsversuchen müssten in diesem Falle geeignete Kontrollverfahren etabliert werden.

5. Die vertrauenswürdige – flächendeckend mögliche – elektronische Kommunikation erfordert es, dass alle potentiellen Kommunikationspartner – und das sind alle Beschäftigten im Gesundheitssystem – mit kryptografischen Werkzeugen ausgestattet werden. Das sind nach Stand der Technik SmartCards (Chipkarten als elektronische Ausweise), zugehörige Lese- und ggfs. Schreibgeräte und Kommunikationssoftware, die mittels dieser Werkzeuge eine vertrauenswürdige, interoperable elektronische Kommunikation gestattet. Zwar können hierfür grundsätzlich Standard-Werkzeuge verwendet werden, allerdings kann die Interoperabilität nur durch zusätzliche Absprachen garantiert werden.

Alle Beschäftigten im Gesundheitssystem, die an der elektronischen Kommunikation teilnehmen, benötigen eine SmartCard als kryptografisches Werkzeug. Zur ihrer Benutzung muss eine Infrastruktur aus Lese-/Schreibgeräten, geeigneter Kommunikationssoftware und organisatorischen Einrichtungen für die Ausgabe und Verwaltung von Werkzeugen und Zertifikaten vorhanden sein.

6. Da die Kommunikation im Gesundheitssystem in der Regel zwar über den Patienten aber zwischen Beschäftigten des Gesundheitssystems erfolgt, ist eine Ausstattung des Patienten - jedenfalls bei den betrachteten Anwendungen – nicht zwingend notwendig. Sie ist jedoch sinnvoll, da dann der Patient selbst Teilnehmer an der elektronischen Kommunikation sein kann.

Der Patient kann optional vom Gesundheitssystem (den Krankenkassen) mit einer kryptografischen SmartCard ausgestattet werden, sofern eine flächendeckende Infrastruktur zum Lesen solcher SmartCards und geeignete Kommunikationslösungen existieren.

Hierzu stellt sich die Frage, ob es Angelegenheit des Patienten ist, sich selbst auszustatten (Bürgerkarte?, eine seiner Bankenkarten?).

Alternativ kann der Patient sich selbst ausstatten (z. B. geeignete Bankenkarte), wenn die verwendete Karte den vorgegebenen Standards entspricht.

Die derzeitige Krankenversichertenkarte könnte z. B. dadurch abgelöst werden, dass ein Patient über seine SmartCard identifiziert wird und die notwendigen Angaben entweder in Sicherheits-Zertifikaten oder auf Servern bereitgestellt werden. Allerdings würde dies voraussetzen, das alle Stellen im Gesundheitssystem mit geeigneten Lesegeräten ausgestattet sind (eine nach Auffassung des Teams allerdings ohnehin notwendige Maßnahme).

Die einwandfreie Identifizierung eines Patienten über sein kryptografisches Werkzeug (SmartCard) gestattet die Zuordnung von Daten im Netz.

Da die Ausstattung des Patienten kein Pflicht-Bestandteil der ersten Stufe einer Sicherheitsinfrastruktur ist, wurde die Ablösung der heutigen Krankenversichertenkarte nicht weiter betrachtet, Lösungen hierfür könnten jedoch ad hoc aufgezeigt werden.

Die Ausstattung des Patienten mit einer SmartCard ist in der ersten Stufe einer Sicherheitsinfrastruktur optional.

7. Wesentlicher Bestandteil einer Sicherheitsinfrastruktur ist eine sogenannte „Public Key“-Infrastruktur.

Die Sicherheitsinfrastruktur ist eine Basis-Infrastruktur für alle (elektronischen) Kommunikationsbeziehun-- gen und Teil einer Kommunikationsinfra-- struktur.

Hierunter versteht man organisatorische und technische Maßnahmen, welche die sichere und vertrauenswürdige Verwendung eines kryptografischen Schlüsselpaars – bestehend aus einem öffentlichen und einem privaten (geheimen) Schlüssel – garantieren. Der Eigentümer dieses Schlüsselpaars wird durch eine vertrauenswürdige dritte Stelle (Zertifizierungsstelle) in einem elektronischen Zertifikat bestätigt. Zertifizierungsstellen erhalten ihrerseits Zertifikate, so dass – ausgehend von einer definierten Wurzelinstanz – eine Zertifizierungshierarchie entsteht.

Eine „Public Key“ Infrastruktur gemäß Signaturgesetz muss auf der Grundlage einer spezifischen Sicherheitspolitik für das Gesundheitssystem in einer speziellen Zertifizierungshierarchie realisiert werden, die technisch abgebildet wird, deren Wurzelinstanz aber auch organisatorische Funktionen wahrzunehmen hat.

Hierzu zählen z. B. die Anerkennung fremder (ausländischer) Sicherheitspolitiken und Zertifikate und der Abgleich von Anforderungen innerhalb der Europäischen Union sowie die Vorgabe von Interoperabilitätsstandards und –profilen.

Zertifizierungsstellen für „Public Key“-Infrastrukturen im Gesundheitssystem sollen einer Sicherheitspolitik gem. Signaturgesetz unterliegen, damit eine elektronische Kommunikation rechtssicher durchgeführt werden kann.

Zusätzlich sind jedoch weitere Anforderungen des Gesundheitssystem in einer speziellen Sicherheitspolitik festzulegen (z. B. keine Pseudonyme, festgelegte Verschlüsselungsverfahren, bestimmte zusätzliche Inhalte in Zertifikaten).

Aus diesem Grunde muss für das Gesundheitssystem eine eigene Zertifizierungshierarchie aufgebaut werden und es muss festgelegt werden, unter welchen Bedingungen Zertifikate aus einer fremden Zertifizierungshierarchie, die unter einer anderen Sicherheitspolitik herausgegeben wurden, anerkannt werden können. Neben der Sicherheitspolitik sind auch zur „Public Key“-Infrastruktur Absprachen notwendig, die eine Interoperabilität der sie nutzenden Verfahren garantieren.

8. Neben der Sicherheit und Vertrauenswürdigkeit der Datenübertragung muss auch die Sicherheit der an der Kommunikation beteiligten Systeme betrachtet werden. Hierzu sind Vorgaben erforderlich, die als Empfehlungen für die Kommunikationsbeteiligten gelten und in Zusammenarbeit mit der Industrie umzusetzen sind.

   Wenn kleine Organisationen des Gesundheitssystems (z. B. Arztpraxen) Firewallsysteme oder Systeme mit vergleichbaren Funktionen von Dritten betreiben lassen, stellt sich die Frage der Kontrolle dieser Dritten, die kleinen Organisationen wegen des oft fehlenden Know-How nicht zugemutet werden kann. Deshalb scheint es notwendig, hierfür Kontrollmechanismen zu definieren.

Die Kontrolle von extern erbrachten (Intranet-) Services und die Verschlüsselung von außerhalb der ärztlichen Kontrolle gespeicherter personenbezogener medizinischer Daten erfordert besondere Maßnahmen. Hiezu zählt insbesondere die Kontrolle von Firewall-Services oder „Intrusion Detection“-Services.

7 Bewertung, Empfehlungen und Maßnahmenvorschläge

Meilenstein 3

Die nachfolgend dargestellten **speziellen Maßnahmen**empfehlungen betreffen die Komponenten der aufzubauenden Kommunikations- und Sicherheitsinfrastruktur, während die **generelle**n **Maßnahmen**vorschläge sich mit den erforderlichen Begleitaktivitäten zur Durchführung (Projektorganisation, Finanzierung, etc.) beschäftigen.

Der Aufbau einer Kommunikations- und Sicherheitsinfrastruktur sollte in Form einer Arbeitsgemeinschafterfolgen, unter deren Dach gemeinsame Projekte von Mitgliedern durchgeführt werden können.

Alle beschriebenen **Maßnahmen können nur bewältigt werden, wenn es zu einer mit ausreichenden Ressourcen ausgestatteten Arbeitsgemeinschaft aller Beteiligten kommt**, die Projekte auch in Form von Aufträgen nach außen betreut und begleitet.

Infrastrukturaufgabe

Aufbau und Betrieb einer Kommunikations- und Sicherheitsinfrastruktur für informationstechnische Anwendungen ist eine alle Partner des Gesundheitssystems betreffende gemeinsame Infrastrukturaufgabe (gesellschaftliche Aufgabe), da es **nur auf der Basis einer abgesprochenen und vereinbarten Infrastruktur zu einer funktionierenden, sicheren, rechtssicheren und vertrauenswürdigen elektronischen Kommunikation im Gesundheitswesen kommen kann**.

Die Bereitstellung einer Infrastruktur ist eine gesellschaftliche Aufgabe und eine gemeinsame Aufgabe der Selbstverwaltung des Gesundheitssystems. Infrastruktur und geeignete Rahmenbedingungen ermöglichen erst das sinnvolle selbständige Handeln einzelner Akteure.

Wegen der gravierenden **Auswirkungen** einer funktionierenden elektronischen Kommunikation und Informationsbereitstellung **auf das Gesundheitswesen und** auf **die** die Technik (und teilweise Organisation) liefernde **Informatikindustrie ist** auch **das finanzielle Engagement der Regierung** zum Aufbau einer Infrastruktur **sinnvoll**.

Die Kosten-Nutzen-Relation einer Infrastrukturaufgabe ergibt sich aus der Betrachtung der Vielzahl aller (denkbaren) Anwendungen. **Es besteht** dabei **die berechtigte Vermutung**, **dass** alleine schon die beiden konkret betrachteten Anwendungen **„Elektronisches Rezept“ und „Elektronischer Arztbrief“ den Aufbau der Infrastruktur rechtfertigen**.

Die Kosten-Nutzen-Relation einer Infrastrukturaufgabe ergibt sich aus der Betrachtung aller (denkbaren) Anwendungen.

Empfehlung 1:

Die Regierung (Bundeskanzleramt, BMWi, BMBF, BMG) **wird aufgefordert**, **den Aufbau der Infrastruktur** als innovatives Projekt und **als gesellschaftliche Aufgabe innerhalb des Wandels zur Informationsgesellschaft zu verstehen**. Sie wird wird gebeten, die Infrastruktur einmalig finanziell zu fördern. In einer Voruntersuchung, mit der eine Unternehmensberatung von ATG und BMG gemeinsam beauftragt wird, wird die Höhe der erforderlichen Mittel geschätzt.

Die Regierung wird gebeten, den Aufbau der Infrastruktur zu finanzieren, da es sich um eine gesamtgesellschaftliche Aufgabe handelt und damit das Gesundheitssystem den Weg in die Informationsgesellschaft zum Wohle aller Bürger zügig gehen kann.

Erprobung von Technik und Organisation ist erforderlich

Die für den Aufbau einer Sicherheitsinfrastruktur erforderliche Technik ist in wesentlichen Teilen am Markt verfügbar. Allerdings gibt es noch **Probleme hinsichtlich** des Zusammenwirkens (**der Interoperabilität**) **von Komponenten verschiedener Lieferanten** und von Diensten und Anwendungen. Des weiteren ist zu berücksichtigen, dass die besonderen Anforderungen des Gesundheitssystems, die ja zum Teil erst noch definiert werden, erstmalig auf der Grundlage verfügbarer Technik zu implementieren wären. Deshalb kann und sollte nicht unmittelbar mit der Implementierung einer Sicherheitsinfrastruktur begonnen werden. Statt dessen **sollte die bereits begonnene konzeptionelle Arbeit zu Ende geführt werden.** Parallel dazu **sollte die Erprobung von Technik und neuer organisatorischer Funktionen in Form von Demonstrationsprojekten oder von Modellversuchen durchgeführt werden**.

Geeignete Technik zum Aufbau einer Sicherheitsinfrastruktur ist im wesentlichen verfügbar, bedarf aber der Anpassung, Ergänzung und Erprobung.

Diese Modellversuche können anwendungsbezogen für die Themen „Elektronisches Rezept“ und „Elektronischer Arztbrief“ stattfinden; denn für beide Szenarien wird eine vollständig funktionie-

rende Kommunikations- und Sicherheitsinfrastruktur benötigt.

Neben der Durchführung der Modellversuche sollte die **Bildung** als notwendig erkannter **neuer organisatorischer Instanzen** unmittelbar erfolgen.

Eine Sicherheitsinfrastruktur besteht auch aus organisatorischen Instanzen, die neu gebildet werden müssen. Hierzu sind gemeinsame Aktivitäten der Selbstverwaltung und möglicherweise auch gesetzliche Lösungen notwendig.

Empfehlung 2:

Es werden **Modellprojekte für die Anwendungen „Elektronischer Arztbrief“ und „Elektronisches Rezept“** durchgeführt, **die auf den Ergebnissen eines Demonstratorprojekts für sichere und vertrauenswürdige** elektronische Kommunikation beruhen.

In diesen Modellprojekten soll auch die Akzeptanz alternativer Lösungen bei den Beteiligten untersucht werden.

Gemeinsam verantwortete und finanzierte Projekte zum Aufbau der Infrastruktur sind erforderlich.

7.1 Spezielle Maßnahmen

Spezielle Kommunikationsverfahren/-standards

Sowohl für die Übermittlung von Informationen als auch für deren Bereitstellung und Abruf auf/von Servern sollen wo immer möglich standardisierte Internet-Protokolle eingesetzt werden. **Sicherheitsaspekte als auch Aspekte der Interoperabilität haben** jedoch **zur Folge, dass** zusätzlich **konkrete Absprachen zur Nutzung optionaler Funktionen und** ggfs. auch **Ergänzungen erforderlich sind**. Dies führt zu speziellen Kommunikationsverfahren und -standards für das Gesundheitssystem, die unter den potentiellen Kommunikationspartner verbindlich vereinbart werden müssen, **damit** überhaupt **eine flächendeckend funktionierende** sichere **elektronische Kommunikation zustande kommen kann**.

Die Ansprüche an Sicherheit und Interoperabilität bedingen, dass hinsichtlich der Nutzung standardisierter Internet-Protokolle zusätzliche Absprachen erforderlich sind, die im Ergebnis zu einem spezifischen Kommunikationsstandard für das Gesundheitswesen führen.

„Public Key"- Infrastruktur (PKI)

Wesentlicher Bestandteil einer Sicherheitsinfrastruktur ist eine „Public Key"-Infrastruktur (PKI).

Die Definition einer gemeinsamen Sicherheitspolitik und die Etablierung einer Zertifizierungshierarchie für das deutsche Gesundheitswesen **sind** dabei wichtige **organisatorische Aufgaben**.

Daneben ist es erforderlich, alle organisatorischen und technischen Aspekte der Etablierung und Nutzung einer Sicherheitsinfrastruktur in einem Rahmenwerk zu beschreiben, auf dessen Grundlage individuelle Ausgestaltungen erfolgen können. Ein derartiges Rahmenwerk beschreibt auch die Absprachen zur Nutzung von Standards, damit interoperable Lösungen – auch grenzüberschreitend - möglich werden.

Zusätzlich sind Vereinbarungen zur gegenseitigen Anerkennung von Sicherheitspolitiken (z. B. Verbot zur Benutzung von Pseudonymen für „elektronische Identitäten", Verbot des Mitlesens von elektronischen Nachrichten des Gesundheitssystems durch staatliche Stellen) und zur Anerkennung von Zertifikaten (Inhalt, Format, ausstel-

lende Stelle) - auch mit ausländischen Gesundheitssystemen - erforderlich.

Zur Erledigung gemeinsamer organisatorischer und technischer Aufgaben einer PKI, d. h. zum Aufbau und zum Betrieb einer gemeinsamen Sicherheitsinfrastruktur für das deutsche Gesundheitssystem, ist die **Bildung einer zentralen organisatorischen Einheit** notwendig. Sie bildet eine (**virtuelle**) **Zertifizierungsstelle für das deutsche Gesundheitswesen als Wurzelinstanz** in **einer Zertifizierungshierarchie**.

Eine gemeinsame org.-technische Instanz als oberste Instanz (Wurzel) einer „Public Key" Infrastruktur für das deutsche Gesundheitssystem sollte gebildet werden.

Anerkennung ausländischer Sicherheitspolitiken

Eine weltweite patientenbezogene elektronische Kommunikation bedingt konkrete **Absprachen mit ausländischen Gesundheitssystemen zur Sicherheitspolitik**, zur Anerkennung von Sicherheitszertifikaten **und zur Konstruktion** sicherer und rechtssicherer **interoperabler Verfahren**.

Zur grenzüberschreitenden interoperablen elektronischen Kommunikation sind Absprachen zur Sicherheitsinfrastruktur mit ausländischen Gesundheitssystemen zur Etablierung interoperabler Kommunikationsverfahren erforderlich.

Register

Die Ausgabe von prozessorgestützten Chipkarten „Health Professional Cards: HPC) als wichtigem Werkzeug einer Sicherheitsinfrastruktur und die Erstellung elektronischer Zertifikate durch berechtigte Stellen zur Identifizierung aller im Gesundheitswesen tätigen Personen „in der elektronischen Welt" setzt voraus, dass alle an der elektronischen Kommunikation beteiligten Personenkreise „erreicht" werden. Dies ist für Angestellte großer Organisationen des Gesundheitssystems und für verkammerte Berufe, die Berufsregister führen, gegeben, nicht dagegen ohne weiteres für die übrigen nicht verkammerten Heilberufe (z. B. Hebammen).

Alle im Gesundheitssystem tätigen Personen müssen grundsätzlich in Berufsregistern oder organisationsspezifischen Registern erfaßt sein.

Ein **Berufsregister für die übrigen Heilberufe** könnte die oben beschriebenen Aufgaben übernehmen, die organisatorisch zum Aufbau einer flächendeckenden Infrastruktur notwendig sind.

Register müssen im Zusammenhang mit dem Betrieb einer Sicherheitsinfrastruktur neue Aufgaben übernehmen.

Diese **Register sollten** auch **Teilaufgaben einer „Public Key"- Infrastruktur (PKI) übernehmen**. Alternativ zur Bildung eines Berufsregisters für sonstige Heilberufe könnte diese Aufgabe von einer Arbeitsgemeinschaft der Krankenkassen für die sonstigen Leistungserbringer übernommen werden.

Dazu gehört die Ausstellung und Verwaltung von sog. Attribut-Zertifikaten, die Ausgabe von Chipkarten für Digitale Signatur, Verschlüsselung und Authentisierung sowie die Pflege von elektronischen Adreßbüchern.

Adressbuch

Die Berufsregister oder sonstigen Register stellen eine wichtige Grundlage für den **Aufbau eines** allgemeinen und **sicheren elektronischen Adressbuchs** für das deutsche Gesundheitswesen dar.

Wesentlicher Bestandteil einer gemeinsamen Kommunikations- und Sicherheitsinfrastruktur ist ein gemeinsames elektronisches Adressbuch, dessen Pflege in Zusammenarbeit mit den Registern geregelt werden muss.

Ein derartiges Adressbuch kann als Nebeneffekt dazu benutzt werden, Patienten den Zugang zu Informationen über Dienstleistungen des Gesundheitssystems zu ermöglichen.

Zum Aufbau einer Sicherheitsinfrastruktur ist ein sicheres Adressbuch unbedingte Voraussetzung, da hiermit notwendige Verzeichnisdienste einer „Public Key"- Infrastruktur (PKI) verbunden sind, wie beispielsweise die Bereitstellung eines kryptografischen Schlüssels zur Verschlüsselung von Nachrichten an einen Adressaten.

Ein derartiges Adressbuch kann von Patienten auch für den Zugang zu Informationen benutzt werden („Gelbe Seiten" des Gesundheitssystems).

„Health Professional Card“ (HPC)

Ein wichtiges Element einer Sicherheitsinfrastruktur ist eine **prozessorgestützte Chipkarte** (z. B. HPC) **für alle im Gesundheitssystem tätigen Personen, die an der elektronischen Kommunikation teilnehmen**. Ein geeignetes Muster bietet die vorliegende Spezifikation des Elektronischen Arztausweises. Allerdings müssen die Überlegungen zur Darstellung der Organisationszugehörigkeit der Personen und von deren Rolle im Gesundheitssystem und deren Vertretungsmacht noch vertieft werden.

Für eine rechtssichere Kommunikation müssen alle im Gesundheitswesen tätigen Personen mit einer SmartCard ausgestattet werden. Die Ausgabe von derartigen SmartCards geschieht in Zusammenarbeit mit Berufsregistern bzw. verantwortlichen Organisationen.

Kontrolle der Sicherheitsmaßnahmen für an offene Netze angeschlossene Systeme

Die **Kontrolle von Sicherheitsmaßnahmen für den Zugang zu offenen Netzen** (Internet), kann kleinen Organisationen (z. B. Arztpraxen) des Gesundheitssystems nicht zugemutet werden, da Ihnen das hierfür erforderliche Wissen fehlt. Extern kontrollierte Sicherheitsservices könnten eine geeignete Lösung darstellen.

Kleinen Organisationen des Gesundheitssystems, z. B. Arztpraxen, kann nicht zugemutet werden, selbst für die Sicherheit der an öffentliche Netze angeschlossenen Systeme verantwortlich zu sein.

Pseudonyme

Für personenbezogene Daten sind rückführbare und nicht rückführbare **zweckgebundene Pseudonyme** erforderlich. Diese Pseudonyme sollten zum frühest möglichen Zeitpunkt in **zweckgebundene Datenflüsse** integriert werden. Dadurch werden anonymisierte Statistiken für definierte Zwecke ermöglicht. Pseudonyme für Patienten und für im Gesundheitssystem Tätige sind eine gute **Voraussetzung zur Gewinnung von Transparenzdaten**.

Pseudonyme sind eine Voraussetzung für einrichtungsübergreifende und lebenslange prinzipiell personenbeziehbare Statistiken.

Änderung von Gesetzen

Alle **Gesetze** des öffentlichen Rechts für das Gesundheitswesen **müssen** – analog zur Änderung des BGB - dahingehend **angepaßt werden,** dass Digitale Signaturen als gleichwertig zur eigenhändigen Unterschrift angesehen werden und die **Schriftform durch eine elektronische Form ersetzt werden kann**.

Die Anerkennung der Digitalen Signatur und der elektronischen Form kann durch die Anpassung gesetzlicher Regelungen – analog zur vorgesehenen Ergänzung des BGB - erfolgen.

Weiterhin müssen Formvorschriften in Gesetzen, Verordnungen und Verträgen angepasst werden.

Zusätzlich ist zu **prüfen, ob die gesetzlichen Grundlagen zur Ausgabe von elektronischen Ausweisen (HPCs) ausreichen** oder ob es in Teilbereichen für eine flächendeckende Ausstattung von im Gesundheitswesen tätigen Personen mit einem kryptografischen Werkzeug einer besonderen gesetzlichen Regelung bedarf.

Daneben stellt sich die Frage, ob es ausreichende **Rechtsgrundlagen** gibt, **um die Interoperabilität einer elektronischen Kommunikation** im Gesundheitswesen „**erzwingen**“ **zu können**.

Um eine das gesamte Gesundheitssystem umfassende interoperable elektronische Kommunikation zu etablieren, bedarf es möglicherweise weiterer gesetzlicher Grundlagen.

Empfehlung 3:

Es soll ein Projekt unter Beteiligung von Industrie und Forschung durchgeführt werden, in dem die vertrauenswürdige und interoperable elektronische Kommunikation nach den Vorstellungen dieses Papiers demonstriert wird (Empfehlung 3.1: **Demonstratorprojekt**). Die Vorgaben hierzu werden von einem ATG-Team erarbeitet. Neben der Ende-zu-Ende-Transportsicherheit ist auch ein sicherer Kanal zwischen den Kommunikationspartnern und der sichere Zugang zu offenen Netzen (Internet) Inhalt des Demonstratorprojekts.

Da eine funktionierende Kommunikations- und Sicherheitsinfrastruktur die Grundlage für anwendungsbezogene Modellprojekte darstellt, soll hierfür zunächst ein Demonstratorprojekt durchgeführt werden.

Eswird angestrebt, in Zusammenarbeit mit dem Projekt Telematikplattform für medizinische Forschungsnetze (TMF) eine Teilfinanzierung durch das BMBF zu erreichen.

In diesem Demonstratorprojekt werden alle noch fehlenden Festlegungen entwickelt und erprobt. Die Anforderungen an Kommunikationssoftware und Werkzeuge zur Erreichung der Interoperabilität werden beschrieben.

Zusätzlich ist das **Konzept einer Sicherheitsinfrastruktur** im Detail zu beschreiben und ein **Projektplan zum Aufbau der Infrastruktur** vorzulegen (Empfehlung 3.2: Projektplan).

Ergänzend soll das Konzept für eine Sicherheitsinfrastruktur inklusive eines Projektplans für deren Aufbau und dauerhaften Betrieb soll erstellt werden.

Folgende Details sind notwendiger Bestandteil dieser Arbeiten:

- Die organisatorischen Details und die jeweils Verantwortlichen für die Ausgabe von „Health Professional Cards“ (HPCs) werden festgelegt.
- Die Funktionen und Inhalte eines elektronischen Adressbuchs für das Gesundheitssystem werden entworfen. Daneben ist darzustellen, durch wen und in welcher Weise die ständige Aktualisierung des elektronischen Adressbuchs erfolgt.
- Methoden, Verfahren und organisatorische Grundlagen einer vertrauenswürdigen externen Sicherheitskontrolle für Firewallsysteme o. ä. werden dargestellt.
- Es wird aus juristischer Sicht untersucht, welcher gesetzliche Änderungsbedarf für die Etablierung einer Infrastruktur besteht.

Eine Prüfung der gesetzlichen Grundlagen für den Aufbau der Infrastruktur ist notwendig.

Geschätzter Mittelbedarf für vorbereitende Projekte zwecks Aufbau einer Kommunikations- und Sicherheitsinfrastruktur: ca. **1,3 Millionen DM (einmalig).**

Empfehlung 4:

Unter der Federführung des BMG und unter Beteiligung aller Organisationen des ATG sollte eine Arbeitsgruppe eingerichtet werden, die zunächst ein **Konzept zur Pseudonymbildung** im Gesundheitssystem vorzulegen hat. Dieses Konzept stellt einen wesentlichen Baustein zur Gewinnung von Transparenzdaten dar.

Unter Federführung des BMG sollte ein Konzept zur Pseudonymbildung entworfen werden.

7.2 Generelle Maßnahmen

Professionelle Projektorganisation mit Teilprojekten

Die Realisierung einer gemeinsamen Kommunikations- und Sicherheitsinfrastruktur bedarf eines gemeinsamen **Projektmanagement**s aller Beteiligten. Hierzu sind **Ressourcen** in Form von Personal, Sachmitteln und Geld bereitzustellen. Wegen des Umfangs und der Komplexität der Aufgabenstellung ist eine Unterteilung in Teilprojekte sinnvoll.

Der Aufbau einer Telematik-Infrastruktur für das Gesundheitssystem ist eine gesellschaftliche Aufgabe, die im wesentlichen der gemeinsamen Selbstverwaltung des Gesundheits- und Sozialsystems obliegt.

Sie kann allerdings nur in enger Zusammenarbeit mit Wissenschaft und Industrie und mit Unterstützung der Regierung erfolgreich gelöst werden.

Zum Aufbau einer Telematik-Infrastruktur müssen gemeinsam gelenkte und finanzierte Projekte durchgeführt werden.

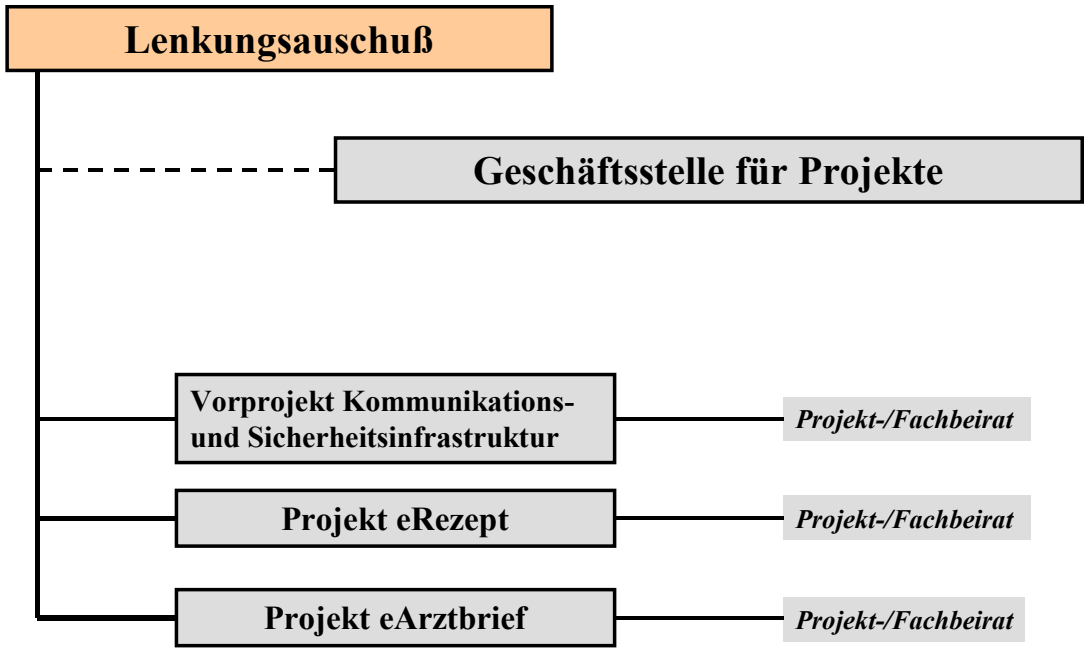
Empfehlung 5:

Es wird ein Rahmenprojekt zur **Koordinierung aller Teilprojekte** durchgeführt. Für dieses Rahmenprojekt (**Arbeitsgemeinschaft**) wird eine Geschäftsstelle und ein Lenkungsausschuß eingerichtet, der das Mandat haben muss, alle erforderlichen Entscheidungen zu treffen und deshalb mit Entscheidungskompetenz ausgestattet sein muss (z. B. Vorstände). Das ATG wird gebeten, einen Vorschlag zur personellen Besetzung und zum prinzipiellen Finanzierungsschema vorzulegen. Die Projektgeschäftsstelle, die von einem Fachbeirat unterstützt wird, hat die Aufgabe, die fachliche Erstellung von Konzepten und deren dauerhafte Weiterentwicklung zu betreiben einschließlich der notwendigen Qualitätskontrolle, auf der Grundlage von Konzepten Ausschreibungen durchzuführen und Realisierungsprojekte zu überwachen und zu kontrollieren.

Der Aufbau der Telematik-Infrastruktur soll durch eine gemeinsam - gemäß eines prinzipiell gebilligten Finanzierungsschlüssels – finanzierte Arbeitsgemeinschaft erfolgen, die durch einen Lenkungsausschuß gesteuert wird. Der Lenkungsausschuß wird von einer Geschäftsstelle unterstützt. Die Arbeitsgemeinschaft vergibt separat finanzierte Teilprojekte zur Realisierung der Infrastruktur und von Anwendungen nach entsprechender Konzepterstellung und Ausschreibung.

Geschätzte organisatorische Kosten für die Projektgeschäftsstelle: ca. 700.000 DM jährlich.

Organigramm für Telematikprojekte

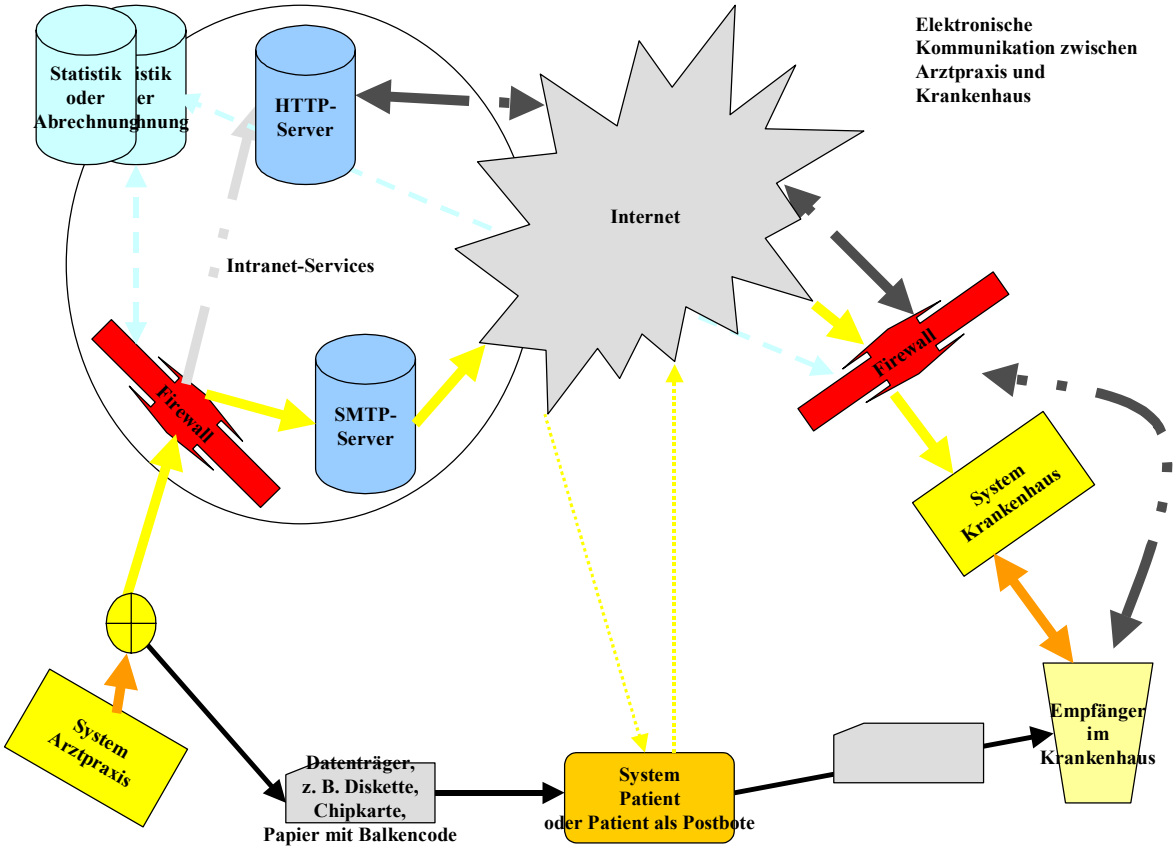


Anlage 1: Beschreibung von Realisierungsaspekten

Kommunikationsbedürfnis und Transparenzbedürfnis

Bezogen auf die im Gesundheitssystem anfallenden Daten kann grundsätzlich zwischen einem Kommunikationsbedürfnis hinsichtlich derartiger Daten etwa zur Mit- und Weiterbehandlung von Patienten und der Sammlung von Daten aus einem individuellen oder globalen Transparenzbedürfnis heraus unterschieden werden. Aus diesen beiden sehr unterschiedlichen Bedürfnissen resultieren auch unterschiedliche Anforderungen an eine Sicherheitsinfrastruktur.

Kommunikationsbedürfnis und Transparenzbedürfnis führen zu unterschiedlichen Anforderungen an eine Sicherheitsinfrastruktur.



Die Anforderungen, die aus dem Kommunikationsbedürfnis entstehen, wurden an den konkreten Anwendungen (Szenarien) „Elektronisches Rezept“ und „Elektronischer Arztbrief“ untersucht. Dabei wurde auf die Ergebnisse der entsprechenden ATG-Teams zurückgegriffen.

Die Verallgemeinerung der Kommunikationssituation führt im Ergebnis dazu, dass die Anforderungen aus den beiden oben genannten Anwendungen prinzipiell gleich behandelt können.

Die verschiedenen denkbaren Kommunikationsbeziehungen wurden in das hier oben dargestellte Diagramm eingezeichnet, so dass hieraus ein allgemeines Kommunikationsdiagramm für das Gesundheitssystem entstand.

In einer Abwägung zwischen Abstraktion und noch leicht verständlicher Konkretisierung wurden die denkbaren Kommunikationsbeziehungen am Beispiel der Kommunikation zwischen einer Arztpraxis als Sender und einem Krankenhausarzt als Empfänger dargestellt. Daneben wurde in dieser Darstellung angenommen, dass die Arztpraxis bestimmte Intranet-Services als Dienstleistung bezieht, während das Krankenhaus diese Dienste selbst betreibt. Die Entscheidung über ein „Outsourcing“ von technisch-organisatorischen Diensten liegt dabei jedoch beim jeweilgen Systembetreiber.

Eine detaillierte Darstellung der Kommunikationsanalyse findet man im Anhang zu dieser Anlage.

Die Ergebnisse der Kommunikationsanalyse münden nachfolgend in Anforderungen an die Sicherheitsinfrastruktur, teilweise sogar in allgemeine Anforderungen an eine Kommunikationsinfrastruktur.

Der Inhalt der Datenübermittlung spielt für die nachfolgende Betrachtung nur insoweit eine Rolle, als es um die Bewertung des Sicherheits- und Schutzbedürfnisses geht, eine größere Rolle spielen formale Aspekte, wie Adreßangaben, evtl. Angaben zum Inhalt der Sendung (Meta-Informationen) und die „sicherheitstechnische Verpackung“.

Kommunikationsbeteiligte

Kommunikationsbeteiligte im Gesundheitssystem sind alle dort tätigen Personen und Organisationen und damit verknüpfte Bereiche (z. B. Arbeitgeber).

Kommunikationsbeteiligte sind Organisationen, Personen, Anwendungen und Rechner (Betriebssysteme).

Die Kommunikation findet in der Regel durch im Gesundheitssystem tätige Personen statt. Die Kommunikation ist dabei meist patienten- oder versichertenbezogen.

Die Kommunikation findet in der Regel patientenbezogen und durch im Gesundheitswesen tätige Organisationen statt. Der Kommunikationsvorgang wird dabei durch eine Person veranlaßt und verantwortet, Empfänger ist dagegen in der Regel eine Organisation.

An der elektronischen Kommunikation nehmen aber auch Anwendungen (Software) und Rechner (Hardware bzw. Betriebssysteme) teil. Dies ist aus dem Blickwinkel einer Sicherheitsinfrastrukturbetrachtung deswegen interessant, weil sich derartige Kommunikationsbeziehungen separat absichern lassen und so einen „sicheren Kanal“ für die benutzerorientierte Kommunikation anbieten.

Übermittlung von Nachrichten

Die besonderen Anforderungen des Gesundheitssystems beim elektronischen Versand von Daten führen dazu, dass ein spezielles „E-Mail-Protokoll“ erforderlich ist, welches jedoch auf den Standard-Internet-Protokollen beruhen sollte. Die Nutzung einer „Health Professional Card“ (HPC) und von „Public Key Infrastructure“- (PKI-) Diensten unter einer festgelegten Sicherheitspolitik, die Nutzung spezieller Inhalte eines Adressbuchs, eine möglicherweise standardmäßige Empfangsbestätigung und die Option zur getrennten Lieferung von Daten und zugehörigen Personenangaben erfordert konkrete Absprachen, wie – das heißt mit welchen Ausprägungen - vorhandene Standard-Dienste des Internet genutzt werden sollen.

Die elektronische Übermittlung von Nachrichten im Gesundheitssystem bedarf spezieller Vereinbarungen für die Nutzung von Internet-Diensten.

Das Adressbuch für Personen und Organisationen

Für die elektronische Übermittlung von Nachrichten an Personen, Personen in Organisationen oder Organisationen ist ein elektronisches Adressbuch sinnvoll, das alle Adressierungsinformationen inkl. der öffentlichen Schlüssel für eine geeignete Verschlüsselung liefert.

Ein allgemeines elektronisches Adressbuch für das Gesundheitssystem mit Angaben zu Organisationen und Personen sollte aufgebaut werden.

Zusätzlich muss dieses Adressbuch die Funktionen eines Verzeichnisdienstes für eine „Public Key Infrastructure“ bieten, damit die Informationen aus Zertifikaten zur Verfügung stehen und geprüft werden können.

Besonders wichtig sind in einem derartigen Adressbuch Angaben zu Organisationen oder zur Organisationszugehörigkeit von Personen, da ja in der Regel Organisationen adressiert werden und wegen der Verschlüsselungsproblematik (z. B. Vertretersituation) auch adressiert werden sollten. Zusätzlich ist die Vertretungsmacht, Rolle oder Funktion von Personen in einer Organisation zu beschreiben.

Ein Adressbuch für das Gesundheitssystem eignet sich daneben als Einstiegspunkt für informationssuchende Patienten.

Als Nebeneffekt kann ein derartiges Adressbuch zugleich den Zugang zu Information über angebotene Dienstleistungen für Patienten ermöglichen („Gelbe Seiten“ des Gesundheitssystems).

Organisation als Adressat oder Sender und Betrachtung des Vertretungsproblems. Die Verschlüsselungsproblematik

Zunächst wird festgestellt, dass eine Kommunikation im Gesundheitssystem in der Regel zwischen Organisationen (Arztpraxis, Station eines Krankenhauses, Abteilung einer Krankenkasse, usw.) stattfindet. Diese Überlegung ist bedeutsam, da eine sichere Datenübermittlung nach Stand der Technik einhergeht mit einer Verschlüsselung, die es lediglich dem Adressaten gestattet, die Sendung zu öffnen. Damit es aber bei Abwesenheit einer bestimmten Person etwa in Vertretungssituationen nicht zu nicht tolerierbaren organisatorischen Problemen kommt, sollte in der Regel eine Kommunikation zwischen Organisationseinheiten stattfinden. Dies ist u. a. auch wichtig bei Rückantworten auf Nachrichten, bei denen technisch betrachtet die E-Mail-Adresse einer Einzelperson benutzt wurde. Geht die Rückantwort an diese Adresse (als Reply-Adresse) kann dies für die eigentlich adressierte Organisation zu nicht lösbaren Problemen führen. Selbstverständlich verhindert dieser grundsätzliche Ansatz nicht die Versendung persönlicher und vertraulicher Nachrichten in verschlüsselter Form an Einzelpersonen oder die Beifügung von für Einzelpersonen verschlüsselten Anhängen.

Kommunikationsteilnehmer im Gesundheitssystem sind grundsätzlich Organisationseinheiten. Diese Überlegung ist bedeutsam, da entscheidend ist, für wen verschlüsselt wird. Die Entscheidung darüber liegt allerdings beim Sender von Daten.

Die korrekte Zustellung innerhalb einer Organisation

Die Übermittlung von Nachrichten von Absenderorganisation zu Empfängerorganisation kann im Sinne einer Ende-zu-Ende-Transportsicherung sicher gestaltet werden. Die korrekte und sichere Zustellung einer Nachricht innerhalb einer Empfängerorganisation (durch deren „Poststelle“) liegt dagegen in der Verantwortung und Organisationshoheit des Empfängers. Analog zur „Papierwelt“ wird ein korrektes Verhalten aufgrund einer nur implizit definierten „Adressierungspolicy“ erwartet. Damit allerdings in einer „elektronischen Welt“ eine voll automatisierte interne Zustellung von Nachrichten an die eigentlichen Empfänger überhaupt möglich wird –so dass etwa keine Notwendigkeit besteht, dass Menschen entschlüsselte Nachrichten vor der Weiterleitung lesen müssen -, sollten neben der E-Mail-Adresse der Empfängerorganisation weitere Adressierungsinformationen in standardisierter Weise mitgesendet werden.

Mittels derartiger Informationen ist eine regelbasierte, automatisierte organisationsinterne Wieterleitung oder Bereitstellung von Nachrichten denkbar. Beispielsweise könnten im - nicht verschlüsselten - Betreff einer E-Mail Institutionskennzeichen und Versichertennummer des Patienten in formatierter Form „als Fallkennzeichen“ angegeben werden. (Beispielsweise könnte die Nachricht innerhalb eines Krankenhauses sofort an die Station weitergeleitet werden, auf die der Patient mittlerweile verlegt wurde.)

Einbeziehung des Patienten in die Kommunikation

Ob die Ausstattung des Patienten mit Werkzeugen der Sicherheitsinfrastruktur bei Einbeziehung des Patienten in die Nachrichtenübermittlung notwendig ist, bedarf einer besonderen Betrachtung. Soll der Patient lediglich temporäre Daten auf einem Datenträger transportieren, benötigt er nicht notwendigerweise Sicherheitswerkzeuge, da er den Datenträger sicher aufbewahren kann. Nimmt der Patient dagegen an einer E-Mail-Kommunikation teil, benötigt er zum Entschlüsseln und zur Prüfung der Digitalen Signatur des Senders kryptografische Werkzeuge. Da der Patient jedoch nicht notwendigerweise in die Kommunikation einbezogen wird, kann ihm die Ausstattung mit geeigneten Werkzeugen grundsätzlich selbst auferlegt werden. Es mag im Wettbewerb der Krankenkassen untereinander z. B. eine geeignete Marketingmaßnahme sein, Patienten mit Krankenversichertenkarten neuen Typs auszustatten, die zugleich kryptografische Funktionen ermöglichen.

Die Einbeziehung des Patienten in die elektronische Kommunikation und dessen Ausstattung mit geeigneten Werkzeugen bedarf einer besonderen Betrachtung. In der Regel kann erwartet werden, dass sich ein Patient selbst mit geeigneten Werkzeugen ausstattet, wenn er in die elektronische Kommunikation einbezogen werden möchte.

Diese Überlegung ist wegen der entstehenden Kosten für die generelle Ausstattung von Patienten und den damit verbundenen Eingriff in einen Markt bedeutsam.

Wären Patienten generell geeignet ausgestattet, könnten allerdings Informationsobjekte für erst später vom Patienten festgelegte Empfänger auf Servern (im Internet) für den Patienten abrufbar verschlüsselt hinterlegt werden – eine Alternative zum hiernach geschilderten Ticketverfahren. Hierbei ist jedoch eine Mitwirkung des Patienten unerläßlich.

Abruf von Nachrichten

Im Gesundheitswesen kommt es häufig zu Situationen, in denen ein Versand von Informationen an den Empfänger nicht möglich ist, da dieser erst später vom Patienten festgelegt wird.

Die von einem noch unbekannten Empfänger benötigten Daten können für eine spätere Abholung bereitgestellt werden.

Daneben ist ein Abrufverfahren deswegen sinnvoll, weil die Menge der mittels E-Mail übertragbaren Daten vielfach beschränkt ist.

Damit ein Abruf-Verfahren im gesamten Gesundheitssystem funktioniert, sind sowohl hinsichtlich der zu benutzenden Grundfunktionen des Internet als auch hinsichtlich der Übermittlung von Informationen, die dem Empfänger den Abruf gestatten, konkrete und spezifische Absprachen erforderlich.

Es ist also ein spezielles „Abruf-Protokoll“ erforderlich, dessen Einzelheiten noch festzulegen sind.

Einzelheiten eines Abrufverfahrens (Ticket-Verfahrens) für bereitgestellte Daten sind noch festzulegen.

Denkbar ist beispielsweise die Übermittlung eines Internet-Links (URL) und zugehöriger Zugangsberechtigungsinformationen (HTTPS).

Derartige Informationen könnten den Patienten auf einer Chipkarte mitgegeben werden.

Der vom Patienten bestimmte Empfänger von Informationen kann vom Patienten Zugangsinformationen/-berechtigungen zum Abruf von Informationen erhalten.

Obwohl es in der Entscheidung des Bereitstellers solcher Informationen liegt, so zu verfahren, muss es zu einer allgemeinen Vereinbarung zur Etablierung eines flächendeckenden Verfahrens kommen, weil ansonsten der ausgewählte Empfänger möglicherweise nicht in der Lage ist, die bereitgestellten Informationen abzurufen.

Ein allgemein vereinbartes Abruf-Verfahren für Daten setzt eine geeignete Ausstattung mit Hard- und Software bei allen potentiellen Empfängern voraus, während der Sender darüber bestimmt, ob er Daten zum Abruf bereitstellt.

Temporär auf einem Server bereitgestellte Informationen können so verschlüsselt werden, dass ein Schlüssel zum Entschlüsseln zugleich die Berechtigung zum (ggfs. einmaligen) Abruf darstellt. Die Entschlüsselung muss erst lokal erfolgen.

Sichere Bereitstellung von Informationsobjekten für noch nicht exakt feststehende Empfänger

Die Übermittlung von Nachrichten an einen noch nicht feststehenden Empfänger kann durch Übergabe eines Datenträgers an den ausgewählten Empfänger erfolgen und/oder durch gesicherte Bereitstellung der Daten auf einem Rechner. Damit bereitgestellte Daten nur von dem ausgewählten Empfänger abgeholt werden können, benötigt der Empfänger Informationen, die ihm die Abholung ermöglichen. Nach Stand der Technik könnte das Informationsobjekt verschlüsselt auf einem Internet-Server bereitgestellt und nach einer Berechtigungsprüfung freigegeben, transportiert und lokal entschlüsselt werden. Der Empfänger benötigt dann für die Abholung der Daten den Schlüssel zum Entschlüsseln und z. B. Benutzerkennung und Paßphrase und Server-Adresse, idealerweise in Form eines sogenannten (kryptografischen) Tickets. Diese Informationen könnten auf einem Trägermedium (z. B. Chipkarte oder Papier) übergeben werden und nur zu einem einmaligen Abholen berechtigen (z. B. als „Kopierschutz“ beim elektronischen Rezept). Einzelheiten eines derartigen Verfahrens wären noch festzulegen. Dabei würde ein Authentisierungsverfahren für den Abrufer mittels HPC die Sicherheit des Verfahrens noch weiter erhöhen. Ein Verfahren, in dem eine Autorisierung zum Abholen von Daten anhand der Angaben auf einer HPC (Attribute in den Zertifikaten) erfolgen würde, kann lediglich als Einstiegslösung betrachtet werden.

Anforderungen an eine sichere Kommunikation

Firewalls oder Schleusen

Die Absicherung der an öffentliche Netze zum Zwecke der elektronischen Kommunikation angeschlossenen Systeme gegenüber Eindringversuchen bedarf einer gesonderten Betrachtung. Zunächst liegt die Verantwortung zum Schutz der eigenen Systeme bei der diese Organisationen betreibenden Organisationen.

Die Verantwortung zum Schutz der eigenen Systeme vor Eindringversuchen liegt beim Betreiber

Allerdings bereitet diese Überlegung insofern Sorgen, als nach dem derzeitigen Stand der technischen Entwicklung sog. Firewallsysteme in der Regel nicht verantwortlich von kleinen Organisationen des Gesundheitssystems (z. B. Arztpraxen) konfiguriert und betrieben werden können. Die Verantwortung für die korrekte Funktionsweise kann aber auch nicht dem Lieferanten derartiger Systeme übertragen werden, da diesem dann ja „Tür und Tor offen stehen“ würde, um an sensible Daten von Patienten zu gelangen. Im Sinne einer Fürsorgepflicht in derartigen Situationen muss deshalb überlegt werden, ob etwa durch Stichproben-Kontrollen vertrauenswürdiger Stellen die notwendige Sicherheit geschaffen werden könnte.

Allerdings stellt sich die Frage, ob kleine Organisationen (z. B. Arztpraxen) Hilfestellung zum konkreten Betrieb von Firewallsystemen benötigen In dem beispielsweise Stichproben-Kontrollen durch bestimmte vertrauenswürdige dritte Stellen durchgeführt werden.

Sichere Online-Verbindung zwischen Rechnern und zwischen Anwendungen

Für die Absicherung des Transportweges (zwischen Rechnern oder zwischen Anwendungen) kann als Internet-Standard eine „Secure Socket Layer“ (SSL)-Verbindung benutzt werden. Verbunden damit ist neben einer Verschlüsselung aller Übertragungen auch die Authentisierung der beteiligten Systemkomponenten. SSL-Verbindungen nutzen Dienste einer „Public Key“- Infrastruktur (PKI).

Zur Absicherung der Verbindung zwischen Rechnern bzw. Anwendungen (Herstellung eines sicheren Kanals) werden die Dienste einer „Public Key“ Infrastruktur (PKI) benötigt.

Sicherer Ende-zu-Ende Transport

Eine sichere, rechtssichere und vertrauenswürdige benutzerorientierte Übermittlung von Daten über öffentliche Netze ist gem. Stand der Technik zum einen mit einem geeigneten E-Mail-Protokoll (zu untersuchen wären z. B. MailTrusT (Projekt des TeleTrusT e. V.) und HCPP (Projekt von Ärztekammer und Kassenärztlicher Vereinigung Bayerns), zum anderen mit einem gesicherten Zugang zu einem Internet-Server (HTTPS) möglich. Die sendende Person sollte dabei die Dienste einer „Public Key"- Infrastruktur durch Einsatz einer „Health Professional Card" (HPC) benutzen. Die Prüfung und Entschlüsselung bei einer Organisation eingehender Nachrichten kann automatisiert (z. B. per Software) erfolgen.

Ein sicherer Ende-zu-Ende Transport zwischen Absender und Empfänger setzt vereinbarte (standardisierte) Verfahren für die Nachrichtenübermittlung voraus, die auf der Basis von Standard-Internet-Protokollen festgelegt werden können.

Ein sicherer Ende-zu-Ende Transport von Daten kann mit einem geeigneten E-Mail-Protokoll geschehen. Derartige Protokolle werden z. Zt. entwickelt und müssen hinsichtlich ihrer Eignung und Interoperabilität untersucht werden, um sie ggfs. als Standard im Gesundheitswesen zu vereinbaren.

Langlebige Sicherungsverfahren beim Transport über öffentliche Netze

Bei einem nach Stand der Technik sicheren Transport von Nachrichten über öffentliche Netze besteht die Gefahr des unerlaubten und heimlichen Anfertigens von Kopien (vgl. 17. Tätigkeitsbericht 1997 – 1998 des Bundesbeauftragten für den Datenschutz).

Der Gefahr des in einigen Jahren möglichen Lesens derartiger Kopien könnte dadurch begegnet werden, dass die Übermittlung von Daten und zugehörigen Personenangaben auf getrenntem Wege geschieht oder das für den späteren Datenaustausch ein Fallkennzeichen oder ein Pseudonym vereinbart wird. Dies ist mit heute verfügbaren Standardtechniken möglich, erhöht allerdings den technischen Aufwand zumindest beim Sender. Nach einer Bewertung des Sicherheitsrisikos im Verhältnis zum Aufwand wird der Sender zu entscheiden haben, ob derartige Techniken für den Versand sensibler Nachrichten im Gesundheitssystem genutzt werden sollen. Konkret könnte die Trennung von Personenangaben und zugehörigen Daten dadurch geschehen, das ein Teil der Information per E-Mail übermittelt wird, für den anderen Teil der Information eine Internet-Adresse (URL). Noch mehr Sicherheit bietet die Verwendung von zuvor vereinbarten Pseudonymen, z. B. Fallkennzeichen.

Die getrennte Übermittlung von Daten und zugehörigen Personenangaben erhöht die Datensicherheit. Es ist zu prüfen, ob auf der Grundlage verfügbarer Technik diese Form der Übermittlung generell oder als Option genutzt werden soll.

Sichere Identifizierung von Teilnehmern

Die Teilnehmer an einer elektronischen Kommunikation im Gesundheitssystem müssen zweifelsfrei ermittelbar sein. Nach den Regeln einer „Public Key"- Infrastruktur für Digitale Signaturen erhält der Teilnehmer eine „elektronische Identität" in Form eines kryptografischen Schlüssels (Schlüsselpaars), nachdem eine vertrauenswürdige Instanz seine Identität festgestellt hat.

Die Zuordnung einer Person zu ihrer „elektronischen Identität" geschieht mittels einer „Public Key" Infrastruktur (PKI).

Die Verbindung zwischen dem Namen einer Person und seiner „elektronischen Identität" wird in einem elektronischen Zertifikat bescheinigt.

Zusätzlich können weitere Eigenschaften und Rechte der Person in einem Zertifikat bescheinigt werden. Solche Zertifikate oder aus ihnen gewonnene Adressbucheinträge in einem sicheren Adressbuch gestatten die Authentisierung von Absender und Empfänger in einer „elektronischen Welt" und die Zuordnung von Rechten an Informationsobjekten.

Innerhalb einer PKI fallen organisatorische Aufgaben an, die zum Teil von den Organisationen des Gesundheitssystems selbst wahrgenommen werden müssen.

Die Authentisierung

Authentisierungsverfahren dienen der Zuweisung von Rechten. Diese können sich auf Einzelpersonen beziehen, aber auch auf deren Zugehörigkeit zu einer Organisation und deren Funktion, Rolle und Vertretungsmacht. Daneben sind Authentisierungsverfahren für Rechner und Anwendungen sinnvoll. Diese Verfahren können analog zur elektronischen Unterschrift betrachtet werden.

In einer Sicherheitsinfrastruktur kann neben der Authentisierung von Personen und deren Organisationszugehörigkeit auch die Authentisierung von Rechnern und/oder Anwendungen verlangt werden.

Die Digitale Signatur

Separat von der Betrachtung des Authentisierungs- und Verschlüsselungsproblems muss die rechtssichere Übermittlung von Nachrichten durch Nutzung der Digitalen Signatur betrachtet werden. Gemäß der Diktion des deutschen Signaturgesetzes wird eine Digitale Signatur immer von einer natürlichen Person geleistet. Die Zugehörigkeit dieser Person zu einer Organisation und ihre Vertretungsmacht ergibt sich aus Signaturschlüssel-Zertifikaten oder zugehörigen Attribut-Zertifikaten. Im Ergebnis bedeutet dies, dass eine von einer Organisation versendete Nachricht von einer Einzelperson digital signiert wird. Die Zugehörigkeit zu einer Organisation und weitere Angaben, aus denen Rechte abgeleitet werden können, ergeben sich aus einem Zertifikat oder einem (sicheren) Adressbuch.

Die gesetzeskonforme elektronische Unterschrift (Digitale Signatur) unter einer Nachricht/einem Informationsobjekt wird immer von einer natürlichen Person geleistet. Die Zugehörigkeit zu einer Organisation/Organisationseinheit und damit verbundene Rechte ergibt sich aus einem Zertifikat bzw. Adressbuch.

Sichere Identifizierung des Patienten

Die sichere Übermittlung von Daten im Gesundheitssystem bedeutet auch, dass es nicht zu Verwechslungen hinsichtlich der Identität des Patienten kommen darf. Angaben, wie Name, Vorname, Geburtsdatum, sind nicht eindeutig genug. Allerdings werden im Gesundheitssystem eindeutige Kennzeichen benutzt, wie z. B. die Angaben zu Krankenkasse und Versichertennummer oder eine Fallnummer, die eine zweifelsfreie Zuordnung von Daten gestatten.

Da derartige Kennzeichen jedoch wechseln können (beim ersten angeführten Beispiel durch Wechsel der Krankenkasse), bedarf die Frage, ob ein lebenslang gültiges identifizierendes Kennzeichen für den Patienten sinnvoll ist, einer besonderen Analyse. Aus den konkret diskutierten Anwendungen „Elektronisches Rezept“ und „Elektronischer Arztbrief“ ergibt sich keine Notwendigkeit hierzu.

Aus den Anwendungen „Elektronisches Rezept“ und „Elektronischer Arztbrief“ ergibt sich keine zwingende Notwendigkeit zur Einführung eines lebenslang identifizierenden Kennzeichens für den Patienten.

Zeitstempel

Die rechtssichere Übertragung elektronischer Nachrichten wirft die Frage auf, ob eine elektronischer Zeitstempel generell verwendet werden soll oder lediglich empfohlen werden soll. Die möglichen Beweismittel der „Papierwelt“ für Ort und Zeitpunkt einer Unterschrift versagen in der „elektronischen Welt“ weitgehend. Die Anbringung elektronischer Zeitstempel verursacht Aufwand in Form lokaler Hardware oder durch die Notwendigkeit zu einer Online-Verbindung zu einem Zeitstempeldienst. Im Zusammenhang mit der Möglichkeit der Quittierung des Eingangs von elektronischen Nachrichten ist die Notwendigkeit zur Anbringung von Zeitstempeln weiter zu untersuchen. Entscheidungen hierzu können anwendungsabhängig getroffen werden. Daneben besteht die Möglichkeit, dem Sender von Daten die Entscheidung über die Verwendung von elektronischen Zeitstempeln zu überlassen.

Die Rechtssicherheit einer Nachricht/eines Dokuments kann durch Zeitstempel oder Empfangsquittungen erhöht werden.

Es ist zu untersuchen, in welchen Fällen derartige Dienste verpflichtend sein sollen oder ob sie in das Belieben des Senders gestellt werden.

Anonymisierung und Pseudonymisierung

Aus Gründen der Transparenz der Versorgungssituation im Gesundheitssystem besteht das Bedürfnis zu statistischen Analysen. Diese Analysen sollen einen bestimmten Zweck erfüllen und können anonymisiert durchgeführt werden.

Die zweckbezogene Anonymisierung von Daten sollte zum frühestmöglichen Zeitpunkt erfolgen.

Hierzu muss der Datenfluß zweckbezogen organisiert werden.

Für Langzeitanalysen ist es dabei sinnvoll, wenn ein „Fall“ verfolgt werden kann, für den zu unterschiedlichen Zeiten und von unterschiedlichen Stellen Leistungen des Gesundheitssystems erbracht wurden. Auf der Grundlage eines Statistik-Konzepts sollte deshalb die zweckbezogene Anonymisierung bzw. Bildung von Fallkenzeichen zum frühestmöglichen Zeitpunkt erfolgen.

Durch ein standardisiertes und vereinbartes Verfahren können jeweils zweckbezogen und daher unterschiedliche Fallkennzeichen gebildet und der Datenfluß zweckbezogen organisiert werden. Ein einheitliches zweckgebundenes „Fallkennzeichen“ läßt sich jedoch nur dann erreichen, wenn von allen Stellen das selbe vereinbarte standardisierte Verfahren benutzt wird.

Verfahren zur Bildung übergreifender Fallkennzeichen oder Pseudonyme müssen allgemein vereinbart sein.

Sicherheitsinfrastruktur

Vorbemerkungen

Für die Realisierung konkreter Anwendungen soll – wo immer möglich – auf Standarddienste und –komponenten zurückgegriffen werden soll.

Dabei sollen die Anforderungen aus Anwendungen wiederum so abstrahiert werden, dass sie durch - ggfs. auch neu definierte - standardisierte Dienste abgedeckt werden können.

Da sich Sicherheitsbedürfnisse nie zu 100 Prozent erfüllen lassen, ist die Realisierung von Sicherheitsmaßnahmen immer abhängig von der Bewertung von Bedrohungsszenarien und von Aufwand und Wirkung einer Maßnahme.

Die Realisierung von Sicherheitsmaßnahmen hängt von Aufwand und Wirkung einer Maßnahme ab.

Der Aufwand ist immer dann gering, wenn marktgängige und übliche Dienste, Werkzeuge und Mechanismen verwendet werden können.

Marktgängige Dienste, Werkzeuge und Mechanismen führen zu einem vertretbaren Aufwand (Stand der Technik).

Wesentlicher Bestandteil einer Sicherheitsinfrastruktur ist eine „Public Key“- Infrastruktur (PKI), die i. w. elektronische Identitäten vertrauenswürdig zur Verfügung stellt.

Wesentlicher Bestandteil einer Sicherheitsinfrastruktur ist eine „Public Key“ Infrastruktur (PKI), wie sie z. B. für Digitale Signaturen zugrunde gelegt wird.

Erforderliche Bestandteile der Sicherheits-infrastruktur

Eine flächendeckende Infrastruktur kann nur durch eine geeignete und standardisierte Ausstattung aller Kommunikationsteilnehmer mit geeigneten Werkzeugen aufgebaut werden.

Bestandteile einer Sicherheitsinfrastruktur sind

- Dienste
- Werkzeuge
- Datenobjekte und
- Mechanismen.

Sie tragen zur Sicherung der Kommunikations-dienste bei.

Die verwendeten Datenobjekte, Mechanismen und Dienste müssen ebenfalls auf der Grundlage technischer Standards konkret vereinbart werden.

Kommunikationsdienste werden in einer Sicherheitsinfrastruktur gem. Stand der Technik von sicheren Internet-Diensten und „Public Key“- Infrastruktur“ (PKI)-Diensten unterstützt. Derartige Kommunikationsdienste sind

- Sicherer Versand eines Informationsobjekts
- Sichere Bereitstellung eines Informationsobjekts für spätere Abholung
- Sichere Abholung eines bereitgestellten Informationsobjekts und
- Sicherer Zugang zu Informationssystemen.

Wesentlicher Bestandteil einer Sicherheitsinfrastruktur ist eine „Public Key“ Infrastruktur (PKI), die sich nicht nur zur Erzeugung Digitaler Signaturen eignet, sondern ebenfalls die Dienste Verschlüsselung und Authentisierung für Personen, deren Organisationszugehörigkeit, Rechner und Anwendungen und deren Kommunikationsverbindungen zur Verfügung stellt.

Dienste

Eine Sicherheitsinfrastruktur stellt folgende Dienste zur Verfügung:

- Basisdienste

  Zugriffskontrolle, Authentisierung, Vertraulichkeit, Integrität, Empfangsbestätigung

- Infrastrukturdienste

  Identifizierung und Registrierung, Namenszuordnung, Personalisierung, Zertifizierung, Verzeichnisdienste, Schlüsselverwaltung

- Mehrwertdienste

  Attributzuordnung, Anonymisierung, Pseudonymisierung, Zeitstempel.

Die entsprechenden Dienste werden anwendungsunabhängig bereitgestellt.

Beispielsweise soll die Sicherstellung der Integrität eines Dokumentes unabhängig davon sein, ob es sich bei diesem Dokument um ein elektronisches Rezept oder einen elektronischen Arztbrief handelt. Unterschiedliche Anwendungen werden von denselben Diensten bedient.

Unterschiedliche Anwendungen können von den selben Diensten einer Sicherheitsinfrastruktur bedient werden.

Basisdienste

Hierunter versteht man die fundamentalen Sicherheitsdienste, die für die sichere Kommunikation direkt eingesetzt werden. Hierzu zählen Integrität, Authentifizierung, Zugriffskontrolle, Vertraulichkeit und Empfangsbestätigung. Die Basisdienste werden durch Mechanismen realisiert, die auf entsprechenden mathematischen Algorithmen beruhen. Zum Beispiel wird die Sicherstellung der Integrität durch den Mechanismus Digitale Signatur realisiert und dieser beruht auf dem RSA-Algorithmus.

Basisdienste werden durch Sicherheitswerkzeuge, wie eine „Health Professional Card“ (HPC) ermöglicht.

Infrastrukturelle Dienste

Diese Dienste ermöglichen die sichere Kommunikation in einem offenen System. Dies bedeutet, dass Benutzer miteinander sicher kommunizieren können, die sich nicht kennen und daher auch nicht unbedingt vertrauen. Hierzu zählen Registrierung, Namensgebung, Schlüsselverwaltung, Kartenpersonalisierung, Zertifizierung und Führung von entsprechenden Verzeichnissen.

Infrastrukturdienste und Mehrwertdienste werden vor allem durch organisatorische Instanzen erbracht.

Mehrwertdienste

Hierbei handelt es sich um Dienste, die sich aus der Geschäftslogik ergeben und durch entsprechende Vereinbarungen bzw. Regelungen erforderlich werden können. Hierzu gehören zum Beispiel die Bescheinigung beruflicher Attribute, die Anonymisierung von Patientendaten sowie die Zeitstempelung von elektronischen Dokumenten.

Während die Basisdienste mittels entsprechend geeigneter Sicherheitswerkzeuge, wie Smartcards, ermöglicht werden, sind für die Erbringung von infrastrukturellen Diensten und Mehrwertdiensten geeignete organisatorische Strukturen (Instanzen) erforderlich.

Werkzeuge einer Sicherheitsinfrastruktur sind

- Smartcards (z. B. „Health Professional Card“ (HPC))
- Lese-/Schreibgeräte für Smartcards
- Spezielle Kommunikationssoftware und
- Software zur Zugangssicherung (z. B. Firewall).

Technische Elemente der Sicherheitsinfrastruktur, die sie äußerlich kennzeichnen, sind Chipkarten für kryptografische Verfahren, elektronische Zertifikate und Verzeichnisdienste (Adreßbücher, Zertifikat-Sperrlisten).

Datenobjekte einer Sicherheitsinfrastruktur sind

- (elektronische) Zertifikate
- (kryptografische) Schlüssel
- Verzeichnisse und
- Zeitstempel.

Mechanismen einer Sicherheitsinfrastruktur sind

- Digitale Signatur
- Ver-/Entschlüsselung
- Authentisierung
- Bereitstellung von Adressen und öffentlichen Schlüsseln
- Prüfung der Gültigkeit von Zertifikaten
- Pseudonymisierung bzw. Anonymisierung für personenbezogene Daten.

Technische Ausstattung

Wichtigste Werkzeuge sind vor allem „Smart-cards“ als „elektronischer Ausweis“ für Heilberufe und alle anderen im Gesundheitswesen tätigen Personen („Health Professional Card“ (HPC)), Lese- und Schreibgeräte für eine HPC und Kommunikationssoftware (und/oder –hardware), welche die Dienste des Internet und die einer „Public Key“- Infrastruktur (PKI) benutzen.

Ein wichtiges Werkzeug einer Sicherheitsinfrastruktur ist eine „Smartcard“ (HPC) für alle im Gesundheitswesen tätigen Personen.

Zu einer technischen Sicherheitsinfrastruktur gehört die Ausstattung aller Kommunikations-partner mit geeigneter Hard- und Software, also mit Werkzeugen.

<u>Alle</u> Kommunikationspartner müssen mit geeigneter Hard- und Software ausgestattet sein.

Aufbau einer „Public Key“- Infrastruktur (PKI)

Der Aufbau einer Sicherheitsinfrastruktur besteht aus organisatorischen Maßnahmen, dem Einsatz ausgewählter Technik und der Festlegung auf bestimmte Verfahren.

Wesentlicher Bestandteil einer Sicherheitsinfrastruktur gem. Stand der Technik ist eine „Public Key“- Infrastruktur (PKI) gem. den Anforderungen des Signaturgesetzes (SigG) und der zugehörigen Verordnung. Diese PKI eignet sich jedoch nicht nur zur Erzeugung Digitaler Signaturen; die gleichen Methoden und Verfahren eignen sich ebenfalls für die Verschlüsselung von Nachrichten bzw. Informationsobjekten und die Authentifizierung von Personen, deren Organisationszugehörigkeit, Rechnern und Anwendungen.

Eine Sicherheitsinfrastruktur wird aus organisatorischen Stellen und technischen Elementen gebildet.

Nur einige organisatorische Funktionen und technische Dienstleistungen können auf Dienstleister (Rechenzentren, Zertifizierungsdienste-anbieter) übertragen werden.

Definition eines Rahmenwerks und einer Sicherheitspolitik

Bei der „Kopplung“ mehrerer Sicherheitsinfrastrukturen zu einer gemeinsamen (virtuellen) Sicherheitsinfrastruktur für das Gesundheitssystem sind Vereinbarungen über die gegenseitige Anerkennung der zugrunde liegenden Sicherheitspolitik (Policy) einschließlich der Verfahren und der Zertifikate notwendig. Alternativ ist die Vereinbarung einer gemeinsamen Policy möglich.

Aufgaben und Obliegenheiten aller beteiligten Stellen müssen in einem Rahmenwerk beschrieben werden.

Die zugrunde liegende Policy wird in den ausgestellten Zertifikaten angegeben und im Internet veröffentlicht.

Zusätzlich sind Standardisierungsabsprachen erforderlich, um das technische Zusammenwirken zu garantieren.

Grundzüge für ein gemeinsames Rahmenwerk

Wesentliche Inhalte eines Rahmenwerks zur Beschreibung der Sicherheitsinfrastruktur sind organisatorische Funktionen, die damit zusammenhängenden Aufgaben und Obliegenheiten und die technischen Dienstleistungen zur Unterstützung der organisatorischen Funktionen einschließlich der Sicherstellung der Interoperabilität verschiedener Sicherheitsinfrastrukturen durch Absprachen zur Benutzung von Standards.

Bestandteil eines Rahmenwerks ist eine Sicherheitspolitik, in der Garantien für die Benutzer der Sicherheitsinfrastruktur übernommen werden.

Die organisatorischen Funktionen betreffen vor allem die Identifizierung der Teilnehmer, die Festlegung „technischer" Namen und die Ausgabe von „Health Professional Cards" (HPCs) sowie die Dienste einer „Public Key"- Infrastruktur (PKI), wie Schlüsselerzeugung, Zuordnung von Schlüsseln zu Personen, Ausstellung von Zertifikaten, Verzeichnisdienste und Zeitstempel. Grundlage dieser organisatorischen Funktionen ist eine Sicherheitspolitik und die Einbettung in eine Zertifizierungshierarchie.

Wesentliche organisatorische Elemente der Sicherheitsinfrastruktur sind registerführende Stellen und vertrauenswürdige Stellen für die Ausstellung und Aushändigung der Zertifikate und Chipkarten sowie der Betrieb sicherer Verzeichnisdienste.

Diese organisatorischen Funktionen sind wie andere Dienstleistungen mit Haftung und Gewährleistung verbunden.

Für die sensiblen Daten im Gesundheitsbereich ist allein ein paßwortgeschützter Zugang nicht geeignet.

Die einwandfreie Authentifizierung einer handelnden Person in einer elektronischen Welt setzt nach Stand der Technik voraus, dass diese Person in geeigneter Form einen kryptografischen Schlüssel benutzt, der dem Namen und sonstigen Eigenschaften der Person über eine elektronische Bescheinigung (Zertifikat) zugeordnet wird. Die Benutzung eines solchen Schlüssels geschieht idealerweise mittels einer Chipkarte - oder einem äquivalenten Hardware-Token -, welche durch (ggfs. mehrere) Paßphrasen (Paßwörter/PINs) oder (ggfs. auch zusätzlich) über ein biometrisches Verfahren geschützt ist.

Derartige Chipkarten, die eine Digitale Signatur, eine Authentisierung und eine Entschlüsselung verschlüsselter Objekte gestatten, sind grundsätzlich im Wettbewerb unterschiedlicher Anbieter am Markt erhältlich, wenn auch die Interope-

rabilität von Angeboten verschiedener Lieferanten derzeit nicht gegeben ist und die Standardisierung der Inhalte auf solchen Karten nicht abgeschlossen ist.

Organisatorische Funktionen, Register und vertrauenswürdige Stellen

Kernelemente einer Sicherheitsinfrastruktur sind kryptografische Schlüssel und ihnen zugeordnete elektronische Bescheinigungen (Zertifikate) vertrauenswürdiger Stellen, in denen Name (im Schlüsselzertifikat) und bestimmte weitere Eigenschaften (ggfs. in separaten Attribut-Zertifikaten) des Schlüsseleigentümers bescheinigt werden.

Die Angaben in den Zertifikaten werden in der Regel auch in einem elektronischen Adressbuch verfügbar gemacht.

Für die elektronische Kommunikation im Gesundheitswesen ist ein gemeinsames, hierarchisch organisiertes elektronisches Adressbuch sinnvoll, welches Teil eines Verzeichnisdienstes einer „Public Key“ Infrastruktur ist.

Private (geheime) kryptografische Schlüssel werden den Teilnehmern an der Sicherheitsinfrastruktur zusammen mit den zugehörigen elektronischen Zertifikaten auf Chipkarten ausgehändigt.

Zugehörige öffentliche Schlüssel, d. h. Schlüssel die über sichere kryptografische Verfahren mit dem privaten (geheimen) Schlüssel verbunden sind, stehen in sicheren Verzeichnisdiensten, in denen auch überprüft werden kann, ob Zertifikate aktuell noch gültig sind.

Für die Ausstellung von Zertifikaten und die Aushändigung von Chipkarten müssen die Teilnehmer an der Sicherheitsinfrastruktur einwandfrei identifiziert werden.

Die Identifizierung und Registrierung von Teilnehmern der Sicherheitsinfrastruktur und die Aushändigung von Chipkarten sind typische organisatorische Aufgaben, die in der Regel von den Stellen wahrgenommen werden, die für den Teilnehmerkreis organisatorisch zuständig sind. Bei verkammerten Berufen kann diese Aufgabe in Zusammenarbeit mit anderen Beteiligten von den Kammern übernommen werden, bei angestellten Personen von deren Arbeitgebern (z. B. Krankenkassen).

Die zu bescheinigenden Eigenschaften müssen registriert werden oder werden aus vorhandenen (Berufs-) Registern entnommen.

Die ausgegebenen Chipkarten müssen bei Bedarf ersetzt, gesperrt oder eingezogen werden, ebenso zugehörige kryptografische Schlüssel und Zertifikate.

Hinsichtlich des Inhalts und der gegenseitigen Anerkennung von Zertifikaten und kryptografischen Verfahren sind prinzipiell Vereinbarungen notwendig mit allen potentiellen Kommunikationspartnern einer elektronischen Kommunikation.

Die Anforderungen des (deutschen) Signaturgesetzes und der zugehörigen Verordnung müssen von den in der Organisation der Sicherheitsinfrastruktur beteiligten Stellen erfüllt werden, damit rechtssichere elektronische Verfahren etabliert werden können.

Aus Gründen einer rechtssicheren elektronischen Kommunikation ist die Erfüllung der Voraussetzungen des Signaturgesetzes durch die beteiligten organisatorischen Stellen sinnvoll.

Für den technischen Betrieb von Verzeichnisdiensten und die technische Herstellung ausgabefertiger personalisierter Chipkarten werden in der Regel Dienstleister (Rechenzentren, Zertifizierungsdiensteanbieter) beauftragt.

Teilaufgaben können dabei auf geeignete technische Dienstleister verlagert werden.

Die Inhalte der Verzeichnisse, Zertifikate und Chipkarten sind jedoch von der jeweils ausgebenden Stelle zu verantworten. Ebenso ist im Sinne einer Auftrags- und Organisationskontrolle der korrekte Betrieb beauftragter technischer Dienstleister zu verantworten.

Die Digitale Signatur unter Signaturschlüssel-Zertifikaten muss bei zum Signaturgesetz (SigG) konformen Sicherheitsinfrastrukturen von einer (ggfs. akkreditierten) Zertifizierungsstelle geleistet werden, welche die Bedingungen des SigG (Sicherheitspolitik - Policy - Signaturgesetz) erfüllt. Diese Voraussetzung gilt auch für die Ausstellung von Attributzertifikaten, die außer den zu bestätigenden Eigenschaften der Person lediglich einen Bezug zum Signaturschlüssel-Zertifikat enthalten, so dass z. B. berufsregisterführende Stellen, die derartige elektronische Bescheinigungen ausstellen wollen, entweder selbst den Bedingungen des SigG genügen müssen, oder sich für Teilfunktionen wiederum eines geeigneten Dienstleisters bedienen müssen.

Diese Voraussetzungen gelten nicht für die ebenfalls erforderlichen Verschlüsselungs-Zertifikate und Authentisierungs-Zertifikate; es empfiehlt sich jedoch, auch für die Ausstellung derartiger Zertifikate die selben organisatorischen und technischen „Mechanismen“ zu benutzen.

Eine Zertifikate ausstellende Instanz die sich hierzu ggfs. eines technischen Dienstleisters bedient, verantwortet die Inhalte der Zertifikate und – falls notwendig - deren unverzügliche Sperrung. Sie haftet gegenüber den Nutzern der Zertifikate.

An berufsregisterführende Stellen, die mit Zertifizierungsstellen zusammenarbeiten, werden hohe Anforderungen bezüglich der sicheren Verfahrensabwicklung gestellt, sie müssen sich dem Sicherheitskonzept der Zertifizierungsstelle unterwerfen.

Berufsregister führende Stellen, die Aufgaben innerhalb einer „Public Key“ Infrastruktur (PKI) übernehmen, müssen hohe Anforderungen bezüglich der sicheren Verfahrens-abwicklung erfüllen

Die Anforderungen sind in einem Sicherheitskonzept eines Zertifizierungsdienste-anbieters festgelegt.

Für die Zusammenarbeit der organisatorischen Stellen, die bei der Ausgabe von Chipkarten und Zertifikaten und der Führung von Verzeichnisdiensten beteiligt sind, sind auf der Grundlage eines Organisationsmodells, einer Beschreibung der funktionalen Aufgabenverteilung und einer Beschreibung prozeduraler Abläufe organisatorische und technische Schnittstellen festzulegen und zu definieren.

Dabei kann unterschieden werden zwischen Aufgaben einer Registrierungsstelle (Identifizierung, Zuordnung), einer Chipkarten ausgebenden Stelle, einer Attributinstanz, welche die Inhalte von Attribut-Zertifikaten und deren korrekte Zuordnung verantwortet, der Zertifizierungsstelle, welche die Zertifikate signiert, dem Verzeichnisdienst und technischen Dienstleisters, welche Teilaufgaben aus diesem Spektrum übernehmen können.

Aufgaben und Obliegenheiten

Die Sicherheitsinfrastruktur besteht nicht nur aus technischen Komponenten, sondern bedarf daneben organisatorischer Dienstleistungen und vertraglicher Regelungen zwischen den beteiligten organisatorischen Instanzen und zwischen diesen und den Benutzern der Infrastruktur.

Die Anerkennung von in einer Sicherheitsinfrastruktur erzeugter Zertifikate und der von ihr benutzen Verfahren und der zugrunde liegenden Sicherheitspolitik (Policy) in anderen Sicherheits-infrastrukturen bedarf vertraglicher Vereinbarungen und organisatorisch-technischer Maßnahmen.

Die Aufgaben und Obliegenheiten aller beteiligten Stellen und die Beschreibung der Beziehung untereinander sowie ihr Verhältnis zu Teilnehmern der Sicherheitsinfrastruktur und zu den Nutzern von Verzeichnisdiensten und Zertifikaten müssen in einem Rahmenwerk für die Sicherheits-infrastruktur beschrieben werden.

Hierzu muss ein gemeinsames organisatorisch-technisches Rahmenwerk entworfen

Die Bestandteile dieses Rahmenwerks, die im Sinne allgemeiner Geschäftsbedingungen nach außen (Teilnehmer, Nutzer, fremde Sicherheits-infrastrukturen, welche Verfahren und Zertifikate anerkennen sollen) wirken, werden als Sicherheitspolitik (Policy) bezeichnet. Die Policy ist die Grundlage für den Umgang mit Chipkarten und Zertifikaten in informationstechnischen Anwendungen.

Innerhalb des deutschen Gesundheitssystems sollen eine einheitliche, gemeinsam abgestimmte und vereinbarte Sicherheitspolitik und gleiche Standards verwendet werden.

Bildung einer Zertifizierungshierarchie

Zertifikate einer Sicherheitsinfrastruktur können zur erleichterten Prüfung der Akzeptanz von Verfahren Bestandteil einer Zertifizierungshierarchie sein.

Alle Zertifizierungsstellen sollen in eine Hierarchie eingebettet werden.

Für den Gesundheitsbereich wird eine deutsche Zertifizierungshierarchie mit einer vereinbarten sog. Wurzelinstanz und einer gemeinsamen Sicherheitspolitik (Policy) angestrebt, international ist eine weltweite Zertifizierungshierarchie für den Gesundheitsbereich denkbar, dessen Wurzel die WHO verantworten könnte.

Für die Prüfung und Anerkennung von Policies und für den Betrieb einer (deutschen) Wurzelinstanz sind organisatorische (und technische) Maßnahmen erforderlich.

Interoperabilität der Sicherheitsinfrastrukturen

Es versteht sich von selbst, dass eine Kommunikation unter Verwendung von Sicherheitsmechanismen nur funktionieren kann, wenn zu Art und Ausprägung verbindliche Absprachen getroffen wurden.

Eine elektronische Kommunikation kann nur auf der Grundlage verbindlicher Absprachen funktionieren. Dies trifft auch auf die Sicherheitsinfrastruktur zu.

Beispielsweise ist eine Entschlüsselung einer Nachricht grundsätzlich nicht denkbar, wenn der zu Grunde liegende Verschlüsselungsalgorithmus unbekannt ist.

Deshalb sind zu allen Details, nämlich von der Sicherheitspolitik über die verwendeten Verfahren bis hin zum Inhalt und der Form von Zertifikaten Absprachen erforderlich. Hierzu sind gemeinsame Definitionen notwendig oder die gegenseitige Anerkennung gewählter Lösungen.

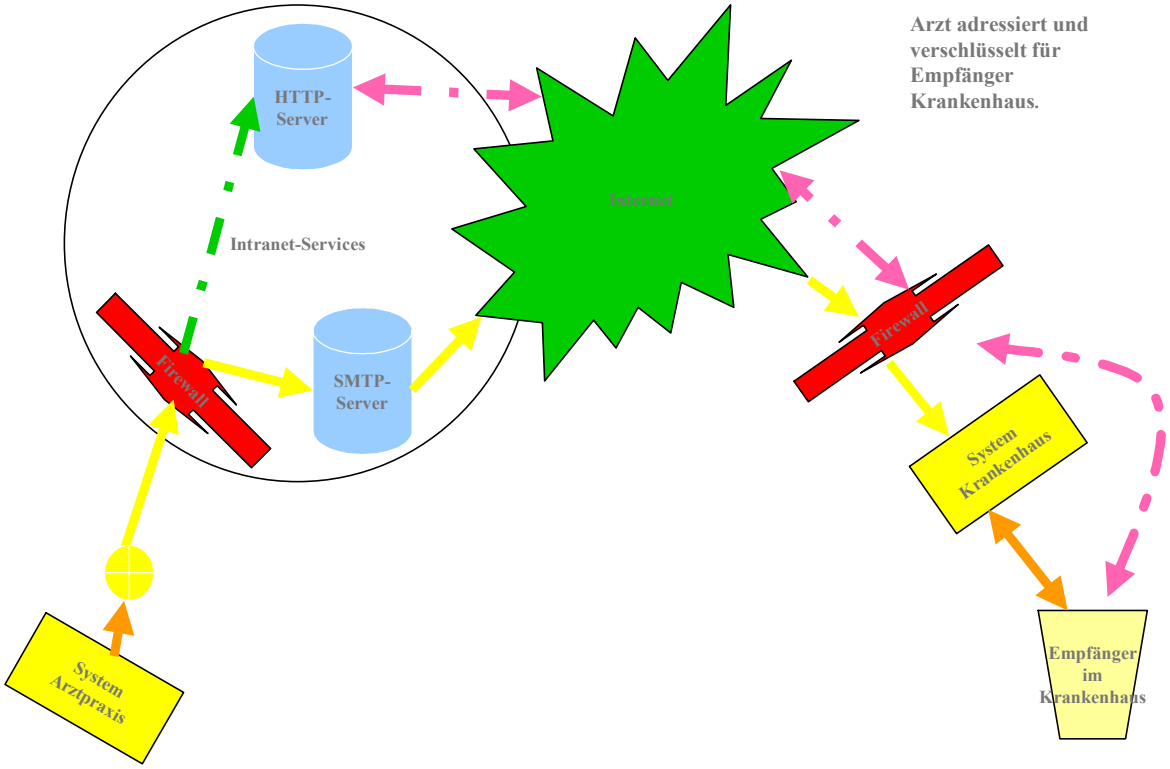
Verschiedene Anwendungen, die auf der Basis unterschiedlicher Sicherheitsinfrastrukturen funktionieren, können nur interoperabel miteinander zusammenwirken, wenn konkrete Absprachen zur Benutzung bestimmter Standards existieren.

Anhang: Kommunikationsanalyse

Die Sicherheitsinfrastruktur ist notwendige Ergänzung einer Kommunikationsinfrastruktur. Zur Ermittlung der Anforderungen an eine Sicherheitsinfrastruktur wurde die Methode der Untersuchung konkreter Szenarien gewählt. Dabei war es naheliegend, innerhalb der Arbeiten des ATG den „Elekrtronischen Arztbrief“ und das „Elektronische Rezept“ zu untersuchen. Selbstverständlich musste dabei der Versuch unternommen werden, die Ergebnisse der Untersuchung so zu abstrahieren, dass die Erkenntnisse möglichst allgemein für viele elektronische Kommunikationsvorgänge gelten. Die Chance, dass dies gelingt, ist schon dadurch gegeben, dass als Grundlage für die elektronische Kommunikation Standardverfahren des Internet einschließlich sogenannter „Public Key“- Infrastrukturen verwendet werden.

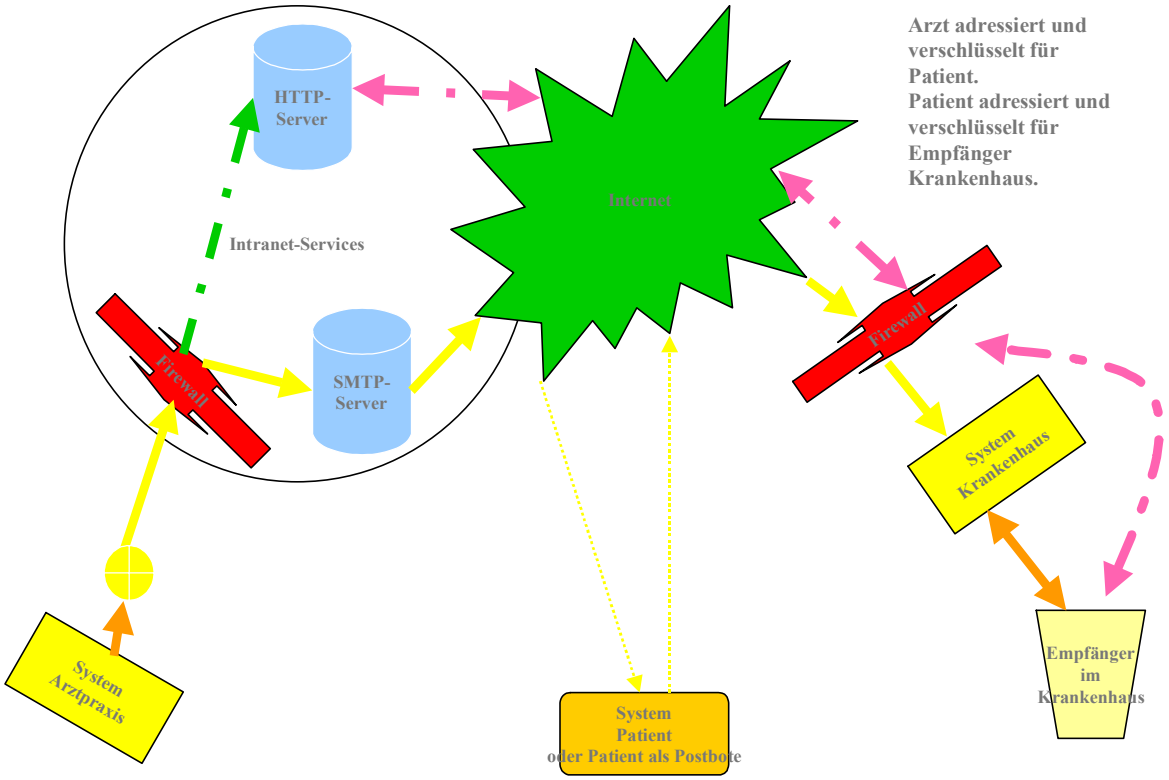
Bei der Kommunikationsanalyse wurden folgende Fälle wurden unterschieden, wobei der Transport eines elektronischen Rezepts als Sonderfall eines elektronischen Arztbriefes nicht näher betrachtet werden musste:

1. Der Arzt adressiert und verschlüsselt eine E-Mail für den Empfänger Krankenhaus.



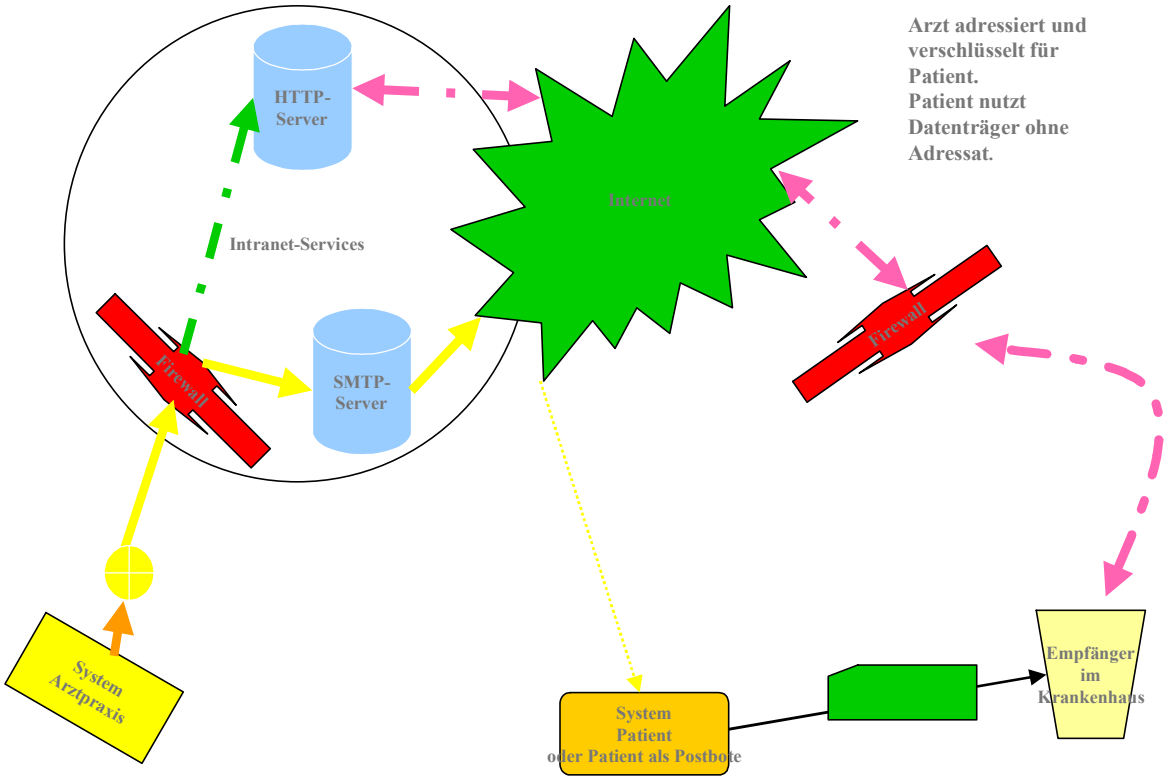
Die E-Mail geht bei der Organisation Krankenhaus ein, wird dort in einer elektronischen Poststelle automatisiert entschlüsselt und dann anhand standardisierter Adreßangaben intern (vertrauenswürdig) automatisiert dem berechtigten Empfänger – auf der Grundlage der Organisationshoheit und Verantwortung des Empfängers - zugestellt.

2. Der Arzt adressiert und verschlüsselt eine E-Mail für den Patienten. Dieser entschlüsselt diese E-Mail und adressiert und verschlüsselt sie dann für den Empfänger Krankenhaus.



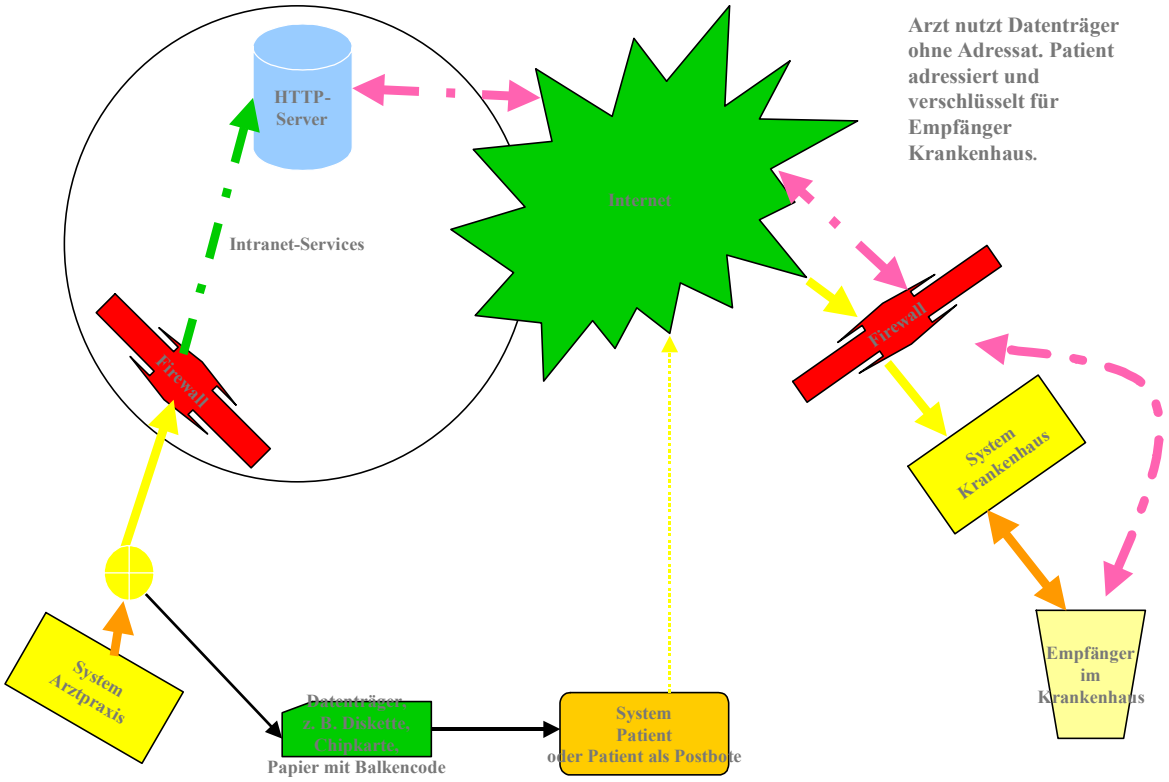
Für diesen Vorgang benötigt der Patient – ggfs. selbst beschaffte – geeignete Kommunikations- und Sicherheitswerkzeuge.

3. Der Arzt adressiert und verschlüsselt eine E-Mail für den Patienten. Dieser entschlüsselt diese E-Mail und gibt sie unverschlüsselt und ohne Adresse auf einem Datenträger an den Arzt im Krankenhaus weiter.



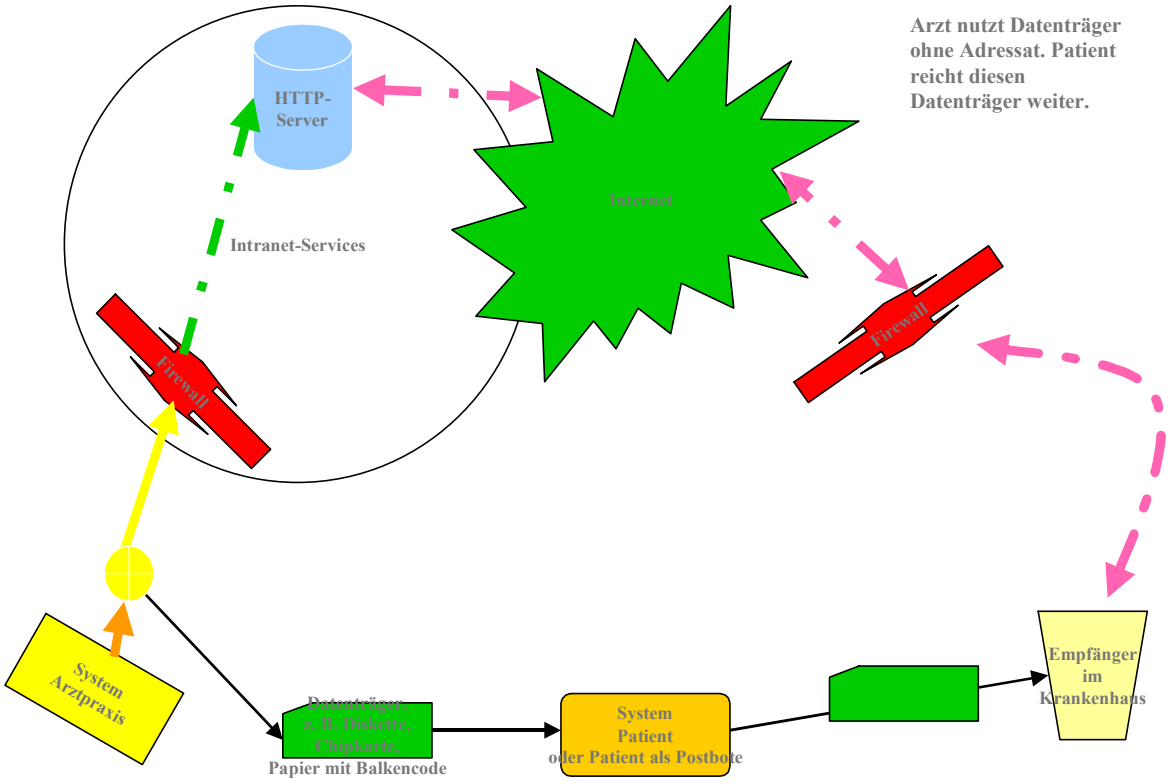
Für diesen Vorgang benötigt der Patient – ggfs. selbst beschaffte – geeignete Kommunikations- und Sicherheitswerkzeuge.

4. Der Arzt übergibt dem Patienten einen unverschlüsselten Datenträger ohne Adresse, der Patient sendet den Inhalt als E-Mail verschlüsselt an den Empfänger Krankenhaus.

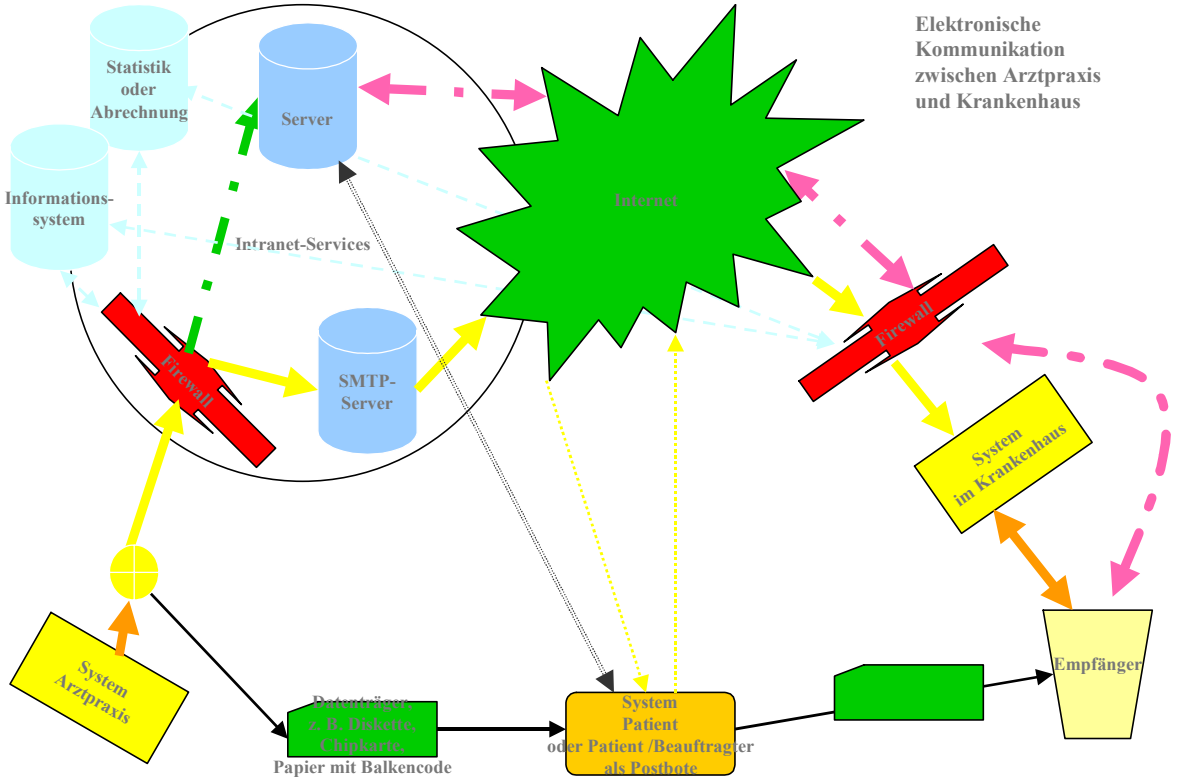


Für diesen Vorgang benötigt der Patient geeignete, d. h. vorgegebenen Standards genügende, Kommunikations- und Sicherheitswerkzeuge. Da es zur Zeit noch keine abgesicherten und etablierten Standards gibt, setzt dies derzeit eine einheitliche – ggf. kostenfreie – Ausstattung der Patienten voraus.

5. Der Arzt übergibt dem Patienten einen unverschlüsselten Datenträger ohne Adresse, der Patient übergibt diesen Datenträger den den Arzt im Krankenhaus.



Diese fünf Fälle stellen alle nach Stand der Technik denkbaren elektronischen Kommunikationsabläufe dar, ohne dass bewertet wird, ob sie in einer bestimmten Situation sinnvoll sind. In allen Fällen kann dem Empfänger im Krankenhaus optional noch eine Server-Adresse mit übermittelt werden, von der er weitere Daten nachfordern kann. Diese Server-Adresse kann bei Bedarf durch ein elektronisches Ticket ergänzt werden, welches den Empfänger zur (ggfs. einmaligen) Abholung des Informationsobjekts und zur lokalen Entschlüsselung berechtigt.



Das vorstehende Schaubild integriert alle untersuchten Kommunikationsvorgänge und ergänzt ohne nähere Betrachtung weitere symbolisch angeführte Intranet-Services.

Die Fälle 2 – 4 setzen die Ausstattung des Patienten mit – ggfs. selbst beschafften – geeigneten Kommunikations- und Sicherheitswerkzeugen (z. B. SmartCard) voraus. Deshalb stellen Fall 1 (E-Mail mit Daten und/oder Abrufticket) für die gerichtete Kommunikation und Fall 5 (Datenträger mit Daten und/oder Abrufticket) für die ungerichtete Kommunikation die beiden wesentlichen Verfahren für die elektronische Kommunikation im Gesundheitswesen dar.

Während E-Mail (Fall 1) im Gesundheitswesen auf Basis von Internet-Standard-verfahren realisiert werden kann, muss ein ticketgestütztes Abrufverfahren (Fall 1 und Fall 5) ebenso realisiert werden wie ein Datentransport auf standardisierten Chipkarten. Es ist naheliegend, die Industrie zu bitten, handelsübliche SmartCards (z. B. Bankenkarten) mit einem Bereich zu versehen, der für einen Daten (oder Ticket-) transport benutzt werden kann. Auf diese Weise könnte vermieden werden, dass das Gesundheitssystem Bürger/Patienten auf seine Kosten ausstatten müßte. Ebenso sollte die Industrie aufgefordert werden, ein ticketgestütztes Abrufverfahren als Standard-Internet-Lösung zu entwickeln und anzubieten. Auf diese Weise wäre es schließlich möglich, die elektronische Kommunikation im Gesundheitswesen auf der Basis von angepaßten Standardverfahren zu realisieren.

Die das ATG tragenden Organisationen in alphabetischer Reihenfolge:

- **Bundesärztekammer**
- **Bundesknappschaft**
- **Bundesverband der Allgemeinen Ortskrankenkassen**
- **Bundesverband der Betriebskrankenkassen**
- **Bundesverband der Innungskrankenkassen**
- **Bundesverband der landwirtschaftlichen Berufsgenossenschaften**
- **Bundesverband der landwirtschaftlichen Krankenkassen**
- **Bundesvereinigung Deutscher Apothekerverbände**
- **Bundesversicherungsanstalt für Angestellte**
- **Bundeszahnärztekammer**
- **Deutsche Krankenhausgesellschaft**
- **Hauptverband der gewerblichen Berufsgenossenschaften e.V.**
- **Kassenärztliche Bundesvereinigung**
- **Kassenzahnärztliche Bundesvereinigung**
- **Verband der Angestelltenkrankenkassen**
- **Verband der privaten Krankenversicherung e.V.**
- **Zentralverband der Krankengymnasten und Physiotherapeuten e.V.**