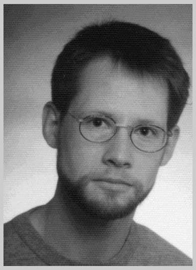
Datenschutzorientierte Abrechnung medizinischer Leistungen

Gerrit Bleumer, Matthias Schunter

Wir beschreiben ein Verfahren zur Abrechnung medizinischer Leistungen, das die Sicherheitsinteressen aller Akteure und insbesondere auch die Datenschutzinteressen der Betroffenen berücksichtigt. In einer entwickelten informationstechnischen Infrastruktur ermöglicht das solidarische Finanzierungsprinzip der gesetzlichen Krankenkassen den Patienten und Ärzten, ihre Vertrauensverhältnisse wirksamer als bisher zu schützen, wobei die Krankenkassen gleichzeitig die anfallenden Gesamtkosten unter Kontrolle behalten können.



Dipl.-Inform.
Gerrit Bleumer

wiss. Mitarbeiter, Universität Dortmund, Fachbereich Informatik; forscht und lehrt über moderne Kryptographie. Mitarbeit und Beratung in mehreren EU-Projekten über Sicherheit in medizinischen Infrastrukturen und Anwendungen.

Dipl.-Inform.
Matthias Schunter

wiss. Mitarbeiter, Universität Dortmund, Lehrstuhl Prof. Biskup. Er entwickelt derzeit im Rahmen des EU-Projekts SEMPER eine integrierte Sicherheitsarchitektur für elektronischen Handel und entwickelt nebenbei Protokolle zum fairen Werte- und Güteraustausch.

1 Einleitung

Der Trend zur elektronischen Abrechnung von Leistungen erfaßt nun auch das Gesundheitswesen. Hierbei ist zu befürchten, daß bei der Umsetzung bisheriger Abläufe in elektronische Transaktionen dem Datenschutz der Patienten keine oder zu geringe Beachtung geschenkt wird. In diesem Positionspapier zeigen wir, daß die wünschenswerte [1, 2] datenschutzorientierte Abrechnung möglich ist und nicht im Widerspruch zur effektiven Kontrolle der Gesamtausgaben steht.[1] Bei bestehenden papierbasierten Lösungen werden meist zur Sicherung der Integrität unverhältnismäßig viele personenbezogene Daten gespeichert; die Konsequenzen dieser Praxis werden nur durch datenschutzgesetzliche Vorkehrungen aufgefangen. In der Praxis funktionieren diese solange, wie die mißbräuchliche Weitergabe, Erfassung oder Speicherung durch Unbefugte zeitraubend und unpraktikabel ist. Diese Voraussetzungen sind immer weniger gegeben, da elektronische Verarbeitung die manuelle zunehmend ersetzt. Daher muß der Schutz persönlicher Daten mehr und mehr Teil der technischen Infrastrukturen selbst werden.

Neue Technologien eröffnen einerseits bisher nicht gekannte Überwachungsmöglichkeiten (rechnergestützte Versichertendatenauswertung), ermöglichen andererseits aber auch ein sehr hohes Sicherheitsniveau, ohne daß große Mengen personenbezogener Daten identifizierbarer Individuen gespeichert werden müssen (neben Prozessorchipkarten auch durch elektronische Brieftaschen und kleine Personal Digital Assistants jeweils mit eigener Tastatur und Anzeige [19]). Investitionen in zunehmend lei-

---

[1] Eine frühere Version dieses Beitrags wurde auf dem Workshop „Personal Information — Security, Engineering and Ethics" vorgestellt [4].

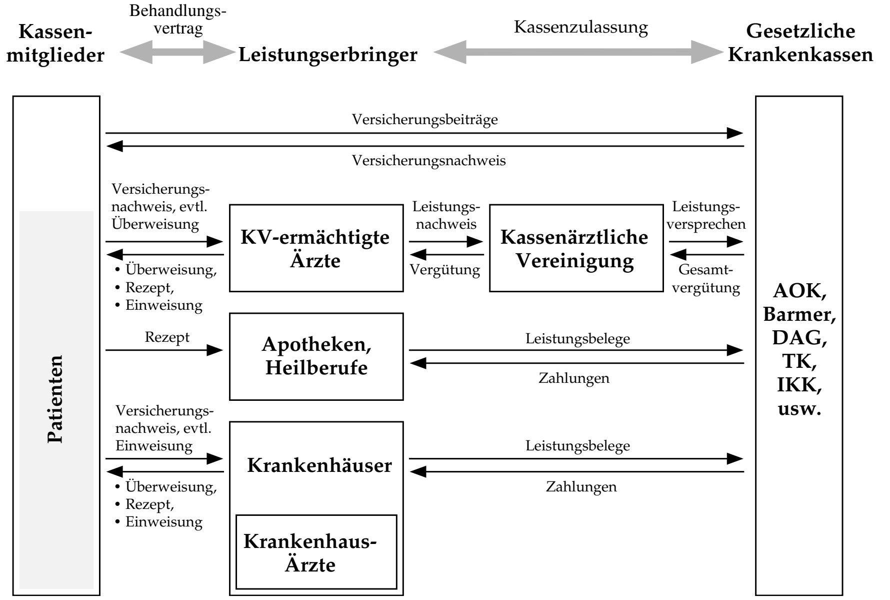

Kassen-
mitglieder
Behandlungs-
vertrag
Leistungserbringer
Kassenzulassung
Gesetzliche
Krankenkassen
Versicherungsbeiträge
Versicherungsnachweis
Versicherungs-
nachweis, evtl.
Überweisung
• Überweisung,
• Rezept,
• Einweisung
KV-ermächtigte
Ärzte
Leistungs-
nachweis
Vergütung
Kassenärztliche
Vereinigung
Leistungs-
versprechen
Gesamt-
vergütung
Rezept
Apotheken,
Heilberufe
Leistungsbelege
Zahlungen
Patienten
Versicherungs-
nachweis, evtl.
Einweisung
• Überweisung,
• Rezept,
• Einweisung
Krankenhäuser
Krankenhaus-
Ärzte
Leistungsbelege
Zahlungen
AOK,
Barmer,
DAG,
TK,
IKK,
usw.

Abbildung 3-1 Vertragsverhältnisse und Informationsflüsse einiger Akteure des deutschen Gesundheitswesens

stungsfähigere Informations- und Kommunikationstechnik im Gesundheitswesen können nur dann gesichert werden, wenn neue Techniken sowohl die rechtlichen Bestimmungen (Datenschutzgesetze) erfüllen, als auch die zu erwartenden Folgen von den betroffenen gesellschaftlichen Gruppen (Krankenkassen, Patienten, Leistungserbringer) bejaht oder wenigstens in Kauf genommen werden. Eine simple Nachbildung der Abrechnungsvorgänge im Gesundheitswesen wird diese Kriterien nicht erfüllen, da mangels ausreichendem Schutz der medizinischen Abrechnungsdaten die entstehende Lösung für Patienten und Ärzte nicht akzeptabel ist. Vom Rat des Bundesministeriums für Forschung, Technologie und Information wird sogar gefordert [8], daß solche „Verfahren den Vorrang verdienen, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern". Erforderlich sei also eine Datenschutztechnologie, die die normativen Vorgaben unterstütze und gegebenenfalls ergänze. Gleichzeitig entwickelt die Industrie Lösungen, um Individuen Anonymität ihrer Transaktionen zu garantieren [17, 18].

Um bei der Abrechnung medizinischer Leistungen zu einer für alle Akteure akzeptablen Lösung zu gelangen, sollen die Aufgaben und Ziele jeder beteiligten Gruppe definiert und anschließend jeweils die zentrale Frage beantwortet werden: *Welche Daten braucht ein Akteur zur Erfüllung seiner Aufgaben?*

Anschließend werden geeignete Verfahren des technischen Datenschutzes vorgeschlagen. Wir beschreiben im folgenden exemplarisch eine Lösung für elektronische Rezepte und die Abrechnung ärztlicher Leistungen.

2 Vertraglicher Rahmen

Zunächst betrachten wir einige Geschäftsprozesse im deutschen Gesundheitswesen [5, 9, 16], die der Abrechnung von Behandlungen von Patienten über gesetzliche Krankenkassen dienen (vgl. Abb. 3–1). Daraus werden anschließend Sicherheitsforderungen für die einzelnen Akteure abgeleitet. Wir unterscheiden die folgenden Gruppen von Leistungserbringern:

1) KV-ermächtige Ärzte, d.h. niedergelassene Ärzte und Zahnärzte, rechnen nicht direkt mit den Krankenkassen, sondern mit den kassen(zahn)ärztlichen Vereinigungen ab. Diese nehmen als Vertragspartner von den Krankenkassen eine Gesamtvergütung entgegen und verteilen sie auf die Kassenärzte.
2) Apotheken und Heilberufe bilden die Gruppe der nichtärztlichen Akteure, die auf eine Verschreibung hin aktiv werden.
3) Krankenhäuser rechnen ebenso wie KV-ermächtige Ärzte nicht direkt, sondern über Krankenhausgesellschaften mit den Krankenkassen ab.

Leistungserbringer werden als solche legitimiert, indem sie vom gemeinsamen Zulassungsausschuß der Kassenärztlichen Vereinigung und der Krankenkassen eine Kassenzulassung erhalten. Zum Beispiel sind Ärzte daraufhin berechtigt, Heilbehandlungen und Medikamente zu verschreiben. Alle Leistungserbringer sind berechtigt, die Heilbehandlungen bzw. Dienste, für die sie zugelassen sind, an Patienten vorzunehmen und die entstandenen Kosten mit der Krankenkasse des betreffenden Patienten abzurechnen. Als Abrechnungsstelle bezeichnen wir im folgenden jeweils den Akteur, mit dem ein Leistungserbringer seine Leistung abrechnet. Zum Beispiel ist die Kassenärztliche Vereinigung die Abrechnungsstelle der KV-ermächtigten Ärzte.

3 Herkömmliche Abrechnung

Wir betrachten nun die derzeitige Leistungsabrechnung im deutschen Gesundheitswesen. Dabei blenden wir die eigentlichen Leistungen (Heilbehandlungen) aus und konzentrieren uns auf die Informationsflüsse (Abb. 3–1).

Der Patient beauftragt durch seinen unterschriebenen Krankenschein den Arzt mit einer Behandlung und teilt ihm seine Abrechnungsdaten mit. Außer dem Fall einer selbst vorgenommenen Heilbehandlung kann der Arzt

- eine Überweisung an einen Facharzt, bzw. eine Rücküberweisung[2] an den Hausarzt, vornehmen,
- ein Rezept ausstellen, welches die Abrechnungsdaten des Patienten und die Verschreibung enthält,

oder

- eine Einweisung in ein Krankenhaus veranlassen, die Abrechnungsdaten und Diagnose enthält.

---

[2] Diese erfolgt derzeit mit einem Arztbrief des Facharztes, der dessen Diagnose und Therapie beschreibt.

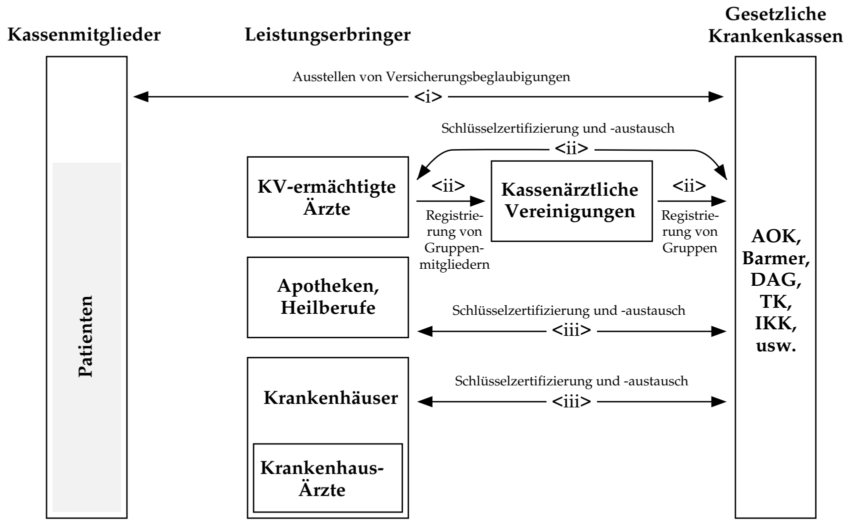

Kassenmitglieder
Leistungserbringer
Gesetzliche Krankenkassen
Ausstellen von Versicherungsbeglaubigungen
<i>
Schlüsselzertifizierung und -austausch
<ii>
KV-ermächtigte Ärzte
<ii>
Registrierung von Gruppenmitgliedern
Kassenärztliche Vereinigungen
<ii>
Registrierung von Gruppen
Apotheken, Heilberufe
Schlüsselzertifizierung und -austausch
<iii>
Krankenhäuser
Schlüsselzertifizierung und -austausch
<iii>
Krankenhaus-Ärzte
Patienten
AOK, Barmer, DAG, TK, IKK, usw.

Abbildung 4-1 Initialisierung der Abrechnungsvorgänge

Während eines komplexen Behandlungsvorgang können diese Schritte wiederholt werden. In jedem der drei Fälle sammelt der Arzt Abrechnungs-, Diagnose- und Therapiedaten und stellt dem Patienten ein Dokument mit den Abrechnungsdaten und Teilen der medizinischen Daten aus. Dieses Dokument reicht der Patient in der Regel selbst und unverändert an den jeweiligen Leistungserbringer weiter, und erhält daraufhin die gewünschte Leistung.[3] Die Bezahlung dieser Leistungen erfolgt, indem die Leistungserbringer erhaltene Dokumente bei der zuständigen Abrechnungsstelle einreichen.

3.1 Kritik

Im Kern ist das herkömmliche Abrechnungssystem ein post-paid Zahlungssystem. Krankenscheinformulare sind gleichsam spezielle Schecks, die Patienten für bestimmte Leistungen (z.B. ärztliche Behandlung, Medikamente, etc.) legitimieren. Der Leistungserbringer rechnet dann mit der Krankenkasse des Patienten ab. Dies erfordert, daß der Krankenkasse die Abrechnungsdaten oft inklusive ärztlicher Diagnose samt Patientenidentität mitgeteilt werden. In einer entwickelten informationstechnischen Infrastruktur kann diese brisante Ansammlung persönlicher medizinischer Daten vermieden werden, indem stattdessen ein prepay Zahlungssystem eingesetzt wird.

3.2 Sicherheitsanforderungen der Akteure

Wir wenden uns nun der Frage zu, welcher Akteur welche Informationen tatsächlich benötigt. Welche Integritätsanforderungen stellt jeder Akteur, d.h., welche Daten muß er erhalten ?

(1) Arzt: Der behandelte Patient soll genau die verschriebenen Leistungen erhalten. Insbesondere soll jedes Rezept[4] nur einmal verwendet werden können. Zusätzlich könnte eine einfache Gültigkeitsdauer oder eine Gültigkeitsregelung gemäß einem Therapieplan wünschenswert sein.

(2) Patient: Ein frei wählbarer Leistungserbringer soll die verschriebene Leistung bei Vorlage eines gültigen Rezepts erbringen.

(3) Apotheken und Heilberufe: Den zugelassenen Leistungserbringern sollen gültige Rezepte nach Vorlage von Behandlungsnachweisen von der Krankenkasse erstattet werden.

(4) Krankenkasse: Nur zugelassene Ärzte sollen Rezepte ausstellen können. Jedes Rezept soll nur einmal (bzw. nach Therapieplan) verwendet werden können. Nur zugelassene Leistungserbringer sollen Rezepte einreichen dürfen. Nur Rezepte und ärztliche Behandlung für eigene Patienten sollen vergütet werden. Die Gesamtkosten sollen begrenzbar sein (Deckelungsprinzip).

Offensichtlich benötigen die Akteure oft nur wenige administrative Daten zur korrekten Durchführung ihrer Aufgaben und müssen noch weniger Daten weitergeben. Die Identität eines Patienten wird nur beim Vertragsabschluß mit der Krankenkasse benötigt. Der Arzt benötigt nur einen eindeutigen Bezeichner für jeden Patienten, den er behandelt, und für die zu verschreibenden Medikamente. Der Patient benötigt anschließend einen Nachweis, daß er das Recht auf die verschriebene Leistung hat.

Der Leistungserbringer benötigt einen Nachweis, daß der Patient berechtigt ist, die Leistung zu erhalten, sowie eine Quittung, daß die Leistung erfolgt ist. Praktisch dient das ärztliche Rezept für beide Nachweise.

Wir fragen nun nach den zusätzlichen Vertraulichkeitsanforderungen jedes Akteurs.

(5) Arzt und Patient: Unbedingter Schutz des für eine medizinische Behandlung notwendigen Vertrauensverhältnisses zwischen Arzt und Patient und insbesondere Vertraulichkeit von Diagnose und Therapie.

Krankenkassen dürfen daher keinen systematischen Überblick bekommen, welcher Arzt welchen Patienten behandelt. Dies schließt später Verfahren aus, die bestimmten Dritten ermöglichen, die Anonymität aufzuheben (zum Beispiel Key-Escrow und aufdeckbar anonyme Beglaubigungssysteme [21]).

(6) Arzt: Die Krankenkassen sollen keine Profile über die Verschreibungsgewohnheiten von Ärzten erstellen können. Eventuell zur Kostenkontrolle verwendete stichprobenartige Kontrollen dürfen nur mit Mitwirkung einer den Ärzten vertrauten Instanz (z.B. KV) möglich sein.

(7) Patient: Rezeptdaten eines Patienten, die bei verschiedenen Leistungserbringern anfallen, sollen unverkettbar sein, so daß die Leistungserbringer daraus keine Patientenprofile erstellen können. Ärzte und Leistungserbringer sollen unter normalen Umständen nicht in der Lage sein, Patientendaten ohne Mitwirkung des Patienten auszutauschen.

---

[3] Natürlich gibt es Ausnahmen von diesem Verlauf, insbesondere dann, wenn die gesundheitliche Verfassung des Patienten ein eigenverantwortliches Handeln zeitweilig nicht erlaubt; zum Beispiel im Falle der Rettungsdienste.

[4] Rezepte stehen im folgenden auch für Ein- und Überweisungen.

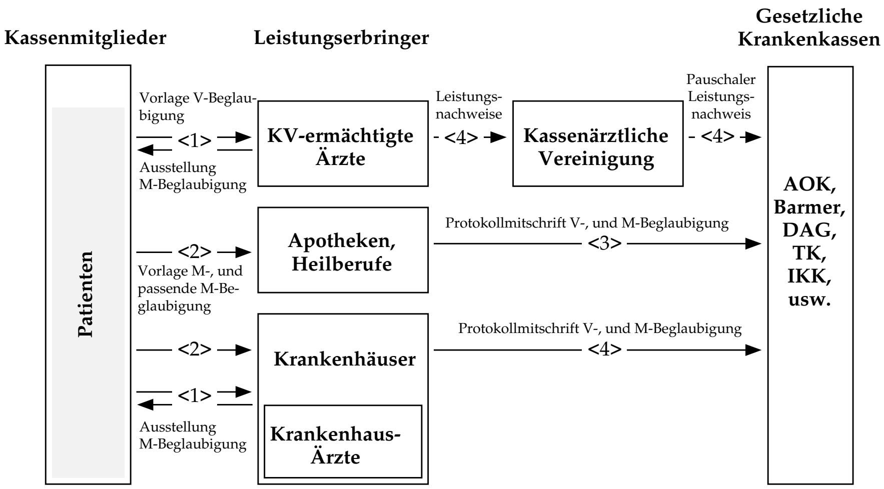

Kassenmitglieder
Leistungserbringer
Gesetzliche Krankenkassen
Patienten
Vorlage V-Beglaubigung
<1>
Ausstellung M-Beglaubigung
KV-ermächtigte Ärzte
Leistungsnachweise
<4>
Kassenärztliche Vereinigung
Pauschaler Leistungsnachweis
<4>
<2>
Vorlage M-, und passende M-Beglaubigung
Apotheken, Heilberufe
Protokollmitschrift V-, und M-Beglaubigung
<3>
<2>
Krankenhäuser
Protokollmitschrift V-, und M-Beglaubigung
<4>
<1>
Ausstellung M-Beglaubigung
Krankenhaus-Ärzte
AOK, Barmer, DAG, TK, IKK, usw.

Abbildung 4-2 Digitale Abrechnung von ärztlicher Behandlung und Rezepten

In Deutschland sind gesetzlich versicherte Patienten spätestens seit 1992 (Einführung der Versichertenkarte) auf Nachfrage verpflichtet, ihre bürgerliche Identität jedem medizinischen Leistungserbringer und ihrer Krankenkasse zu offenbaren. Diese verläßliche „Totalidentifizierung“ berücksichtigt offenbar vorrangig die (Sicherheits-) interessen der Krankenkassen; aber kaum die berechtigten Datenschutzinteressen der Patienten.

Die immer leistungsfähigeren Möglichkeiten gerade zur Informationsgewinnung aus Abrechnungsdaten macht neben gesetzlichen Vorschriften technische Datenschutzmaßnahmen erforderlich, die alle Akteure in die Lage versetzen, ihre Sicherheitsforderungen effektiv und nicht nur nachträglich vor Gericht durchzusetzen. Zudem setzen dezentrale präventive Datenschutzmaßnahmen weniger Vertrauen in Dritte voraus.

4 Digitale Abrechnung

Wir werden nun ein digitales Verfahren für die wichtigen Abrechnungarten im Gesundheitswesen vorstellen. Unsere Lösung erfüllt im Gegensatz zu bestehenden Ansätzen [22, 23] die Datenschutzanforderungen (5)-(7). Das Verfahren setzt voraus, daß alle Beteiligten mit eigener Hardware ausgestattet sind:

- Patienten sind mit einem portablen benutzereigenen Gerät ausgestattet, das es ihnen ermöglicht, eigene digitale Signaturen zu erzeugen und Protokolle auszuführen [19].
- Dienstleistungserbringer und Krankenkasse stellen Geräte bereit, mit denen die Patientengeräte kommunizieren können.

Daß diese Annahmen nicht unrealistisch sind, zeigt der derzeitige Verbreitungsgrad der Patientenkarten: Bereits der Austausch der Speicher- gegen Prozessorchipkarten könnte die Sicherheit wesentlich erhöhen.

Die unserer Lösung zugrundeliegende Idee ist, daß Krankenscheine und Rezepte durch elektronische Beglaubigungen ersetzt werden. Als Versicherungsnachweis stellt jede Kranken kenkasse ihren Mitgliedern sogenannte Versicherungs-Beglaubigungen (V-Beglaubigungen) aus. Diese ersetzen Krankenscheine und berechtigen zum einmaligen Bezug von Versicherungsleistungen. Jeder verschreibungsberechtigte Arzt kann Medizin-Beglaubigungen (M-Beglaubigungen) ausstellen. Diese ersetzen Rezepte, Überweisungen und Einweisungen und können nur zusammen mit einer Versicherungs-Beglaubigung einmal vorgelegt werden.

4.1 Initialisierung

In Abbildung 4–1 werden die drei Initialisierungsschritte erläutert. Sie sind unabhängig voneinander und können daher gleichzeitig durchgeführt werden.

<i> Die Krankenkasse stellt eine Anzahl von V-Beglaubigungen, z.B. für ein Quartal, aus. Diese V-Beglaubigungen haben folgende Eigenschaften:

a) Aus einer V-Beglaubigung ist die ausstellende Krankenkasse ersichtlich.

b) Die Krankenkasse kann einer ihr später wiedervorgelegten V-Beglaubigung nur ansehen, daß sie einem ihrer Mitglieder ausgestellt wurde, aber nicht welchem. Genauer ist das Vorlegen einer V-Beglaubigung mit dem Ausstellen nicht verkettbar, d.h. obwohl die Krankenkasse die bürgerliche Identität des Patienten kennt, erkennt sie eine vorgelegte V-Beglaubigung nicht wieder und kann somit auch nicht feststellen, welchem Patienten sie ausgestellt wurde.

c) Jede V-Beglaubigung kann höchstens einmal vorgelegt werden. Wird sie mehrfach vorgelegt, führt dies zur Identifizierung des Patienten, dem sie ausgestellt wurde.

Außerdem erhält jeder Patient zu Beginn den öffentlichen Signaturschlüssel seiner Krankenkasse zur Prüfung von deren Zertifikaten[5].

<ii> Ärzte werden vom Zulassungsausschuß als Ärzte legitimiert und erhalten die notwendigen Schlüssel zum Erzeugen ärztlicher Beglaubigungen, wie z.B. Rezepten, Überweisungen an andere Ärzte, Krankenhauseinweisungen (analog zur Kassenzulassung).

Nachdem die Ärzte ihre Schlüssel erhalten haben, bilden sie von der Kassenärztlichen Vereinigung verwaltete Gruppen, innerhalb der sie anonym gegenüber Patient und Krankenkasse abrechnen können. Zum Beispiel könnten die Ärzte einer Krankenhausabteilung, oder eines ganzen Krankenhauses eine Gruppe bilden; ebenso wären Gruppen nach Facharztrichtung oder geographischer Niederlassung möglich. Hier sind die legitimen Kontrollinteressen der Krankenkassen mit den berechtigten Unbeobachtbarkeitsinteressen der Ärzte auszuhandeln.

<iii> Apotheken und Heilberufe werden von den Krankenkassen als solche legitimiert und hinterlegen die notwendigen Signaturschlüssel, um später Rezepte verbindlich abrechnen zu können.

---

[5] Ein Zertifikat ist eine Unterschrift unter einem öffentlichen Schlüssel und evtl. einer Identität. Meist wird hiermit ein Recht oder die Zugehörigkeit zur mitunterschriebenen Identität versichert.

4.2 Ausstellen eines Rezepts

Die in den folgenden Abschnitten beschriebenen Abrechnungsschritte sind in Abbildung 4–2 zusammengestellt.

<1> Der Patient zeigt eine seiner V-Beglaubigungen als Versicherungsnachweis und wählt eine weitere V-Beglaubigung zum Versicherungsnachweis gegenüber dem Leistungserbringer aus. Hierzu passend erhält der Patient von seinem Arzt eine M-Beglaubigung (Rezept bzw. Facharzt-Überweisung, Krankenhauseinweisung). M-Beglaubigungen sind gruppenorientert und haben folgende Eigenschaften:
  a) Aus einer M-Beglaubigung ist nur die Gruppe des Ausstellers (Arzt) ersichtlich. Im Gegensatz zu V-Beglaubigungen nicht seine Identität.
  b) Eine M-Beglaubigung kann nur zusammen mit einer passenden V-Beglaubigung vorgelegt werden; also ebenso wie jene höchstens einmal.

4.3 Vorlegen eines Rezepts

<2> Der Patient legt seine M-Beglaubigung (Verschreibung) zusammen mit der vorher dafür ausgewählten V-Beglaubigung einem Leistungserbringer vor. Der Leistungserbringer prüft beide Beglaubigungen auf Gültigkeit und ob sie zueinander passen. Ist die Prüfung erfolgreich, erbringt er die gewünschte Leistung. In Abschnitt 5 wird gezeigt, wie dies mit Hilfe kryptographischer Gruppenbeglaubigungen (Credentials) realisiert werden kann [3, 10].

4.4 Digitale Abrechnung von Rezepten

<3> Der Leistungserbringer reicht je eine Protokollmitschrift der ihm vorgelegten V- und M-Beglaubigungen bei der entsprechenden Krankenkasse ein. Diese prüft die Gültigkeit der Beglaubigungen, und die Budgetierung der betroffenen Ärztegruppe(n). Wird gegen Budgetierungen verstossen, so können die aus dieser Gruppe eingereichten Rezepte teilweise oder ganz ihren Urhebern (ausstellenden Ärzten) zugeordnet werden. Diese Identifizierung (Deanonymisierung) von Gruppenmitgliedern auf Betreiben der Kassen kann nur durch die Gruppenzentrale (z.B. KV) erfolgen.

Die Leistungserbringer müssen der Abrechnungsstelle nicht vertrauen, da sie alle Forderungen zur Not gerichtlich durchsetzen können. Das beschriebene Verfahren läßt sich direkt auf mehrere Krankenkassen erweitern.

4.5 Digitale Abrechnung ärztlicher Behandlung

Im Gegensatz zu anderen Leistungserbringern entscheiden Ärzte autonom über die Therapie und legen daher auch indirekt selbst ihre Vergütung fest. Falls dieses Prinzip des derzeitigen Abrechnungssystems aufrechterhalten werden soll, ist also einzig sicherzustellen, daß die Behandelten versichert sind und daß ein Arzt nur Leistungen abrechnet, die er tatsächlich erbracht hat. Bei digitaler Abrechnung wird dies sichergestellt, indem der Arzt bei der Abrechnung eine Protokollmitschrift von ausgestellten M-Beglaubigungen (die die zuvor vorgelegten V-Beglaubigungen enthalten) einreicht. Wünscht die Krankenkasse (im Gegensatz zum heutigen System) Kontrolle durch den Patienten, so sollte der Patient die Art der Behandlung in seine V-Beglaubigung eintragen, die er seinem Arzt ausstellt.

Entsprechend den Sicherheitsanforderungen von Arzt und Patient (Abschnitt 3.2) müssen dabei zwei Randbedingungen berücksichtigt werden:

- Die Behandlungsbeziehung zwischen Arzt und Patient und die daraus entstehenden Daten wie Diagnosen, Therapiepläne und Verschreibungen dürften der Krankenkasse – wenn überhaupt – nur unter unverkettbaren Pseudonymen bekannt werden.
- Der Arzt muß seine Behandlung in Ausnahmefällen vergütet bekommen, auch ohne daß der Patient seine Behandlung quittiert hat, weil letztlich der Arzt verantwortet (und dafür haftet), ob, wann und gegebenenfalls wie er seinen Patienten aufklärt. Im Normalfall soll der Arzt aber nicht beliebige Kosten unquittiert in Rechnung stellen können.

Eine Möglichkeit, die Abrechnung ärztlicher Behandlung zu gestalten, wäre daher:

<4> Der Arzt läßt seinen Leistungsnachweis vom Patienten anonym unterschreiben und nimmt diese Quittung zur Patientenakte. Anschließend trennt er die identifizierenden Daten des Patienten ab und unterschreibt die abrechnungsrelevanten Behandlungsdaten mit dem Signaturschlüssel seiner Arztgruppe. So aufbereitet reicht er sie – gegebenenfalls unter Einbeziehung der Kassenärztlichen Vereinigung – bei der Krankenkasse des Patienten zur Vergütung ein.

Die Ärzte archivieren die Patientenquittungen ähnlich zur ohnehin vorgeschriebenen medizinischen Dokumentationspflicht und machen diese nur bei stichprobenweise Kontrollen der Krankenkassen zugänglich. Durch die verwendeten anonymen (Gruppen-) signaturen, ist somit der Datenschutz der Patienten auch bei Kontrollen durch die Krankenkassen gewährleistet.

4.6 Sicherheit und Datenschutz

Wir skizzieren nun, warum das vorgeschlagene Abrechnungsverfahren die Sicherheitsanforderungen in Abschnitt 3.2 erfüllt:

Zu (1): Jede Manipulation einer M-Beglaubigung ist vom Leistungserbringer erkennbar und macht sie dadurch ungültig. Mehrfaches Vorlegen ist nur mit derselben V-Beglaubigung möglich und führt daher zur Deanonymisierung des Patienten.

Zu (2): Diese Forderung kann nicht durch technische Maßnahmen, sondern nur durch rechtliche Rahmenbedingungen sichergestellt werden. Das Abrechnungssystem stellt nur sicher, daß ein Leistungserbringer korrekt erbrachte Leistungen abrechnen kann.

Zu (3): Da die Krankenkasse die Zulassung über Vergabe zertifizierter Schlüssel kontrolliert, kann sie sicherstellen, daß nur zugelassene Ärzte M-Beglaubigungen ausstellen. Die Erstattung muß vertraglich gesichert werden. Da der Leistungserbringer die Prüfung des Rezepts beweisen kann, kann er seine Forderungen ggfs. gerichtlich durchsetzen.

Zu (4): Zur Zulassung der Ärzte vergleiche dieselbe Forderung der Leistungserbringer. Dasselbe Verfahren zertifizierter Schlüssel wird für die Leistungserbringer verwandt.

Jede Behandlung wird nur einmal vergütet, da V- und hierdurch auch indirekt M-Beglaubigungen nur einmal vorlegbar sind. Weiterhin sind Mehrfacheinreichungen derselben Protokollmitschrift beweisbar und werden daher nicht erstattet[6]

Die V-Beglaubigungen sind zwar nur für medizinische Dienstleistungen verwendbar, dort aber so universell, daß sie als Blankoschecks angesehen werden müssen. Da sie im Gegensatz zu richtigen Blankoschecks bei der Krankenkasse, die sie deckt, anonym eingereicht werden, bergen sie die größte Gefahr zum Mißbrauch. Die Gefahr, daß ein Patient seine V-Beglaubigungen oder sein ganzes Gerät anderen Personen absichtlich zur Verfügung stellt, ist relativ gering, weil er selbst nur einen begrenzten Vorrat an V-Beglaubigungen hat. Gefährlicher ist der Verlust seines persönlichen Gerätes. In diesem Fall könnte jemand das fremde Gerät als eigenes verwenden oder die darin gespeicherten V-Beglaubigungen ausforschen. Dies kann erschwert werden, indem die V-Beglaubigungen einerseits in geschützten Hardwarebausteinen gespeichert werden und jede Transaktion, durch deren Ausgaben eine V-Beglaubigung erschlossen werden könnte, durch PIN- oder Passwortabfrage, eventuell auch durch biometrische Identifikation oder Aufdruck eines nicht-maschinenlesbaren Paßfotos des Eigentümers geschützt wird.

Durch Ausgabe einer begrenzten Anzahl von V-Beglaubigungen an Patienten kann die Krankenkasse die Kosten vorab grob begrenzen. Durch gruppenweise Deckelungs- bzw. Regressmechanismen der Abrechnungsstelle kann eine absolute Begrenzung sichergestellt werden. Hierbei kann die Krankenkasse zusammen mit der Kassenärztlichen Vereinigung auch einzelne Praxen genauer überprüfen.

Zu (5): Da der Arzt Medikamente nur mit einer Gruppen-Beglaubigung ausstellt, und der Patient beim Vorlegen unverkettbare Einmal-Pseudonyme verwendet, gibt die zur Vergütung bei der Krankenkasse eingereichte Protokollmitschrift keine Information über die Arzt-Patient Beziehung preis. Dasselbe gilt für die Abrechnungen der anderen Leistungserbringer.

Zu (6): In der beschriebenen Lösung können nur Profile von Ärztegruppen, nicht aber Profile einzelner Ärzte erstellt werden.

Zu (7): Da der Patient für jede Leistungserbringung eine neue V-Beglaubigung verwendet, sind alle Leistungen untereinander unverkettbar. Hierbei ist zu beachten, daß das persönliche Benutzergerät keinerlei maschinenlesbare Individualmerkmale (z.B. Gerätenummer) aufweisen darf.

5 Skizze einer kryptographischen Realisierung

---

[6] Zwei Kopien einer Mitschrift eines Leistungsnachweises sind identisch. Wird ein von der Abrechnungsstelle gewählter Zufallswert vom Leistungserbringer mitsigniert, sind die Unterschrift unter beiden Einreichungen unterschiedlich. Die zweite Einreichung wird dann unter Vorlage der ersten Unterschrift abgewiesen [7].

Wir führen in Abschnitt 5.1 vier kryptographischen Primitive ein: Signaturen und Einmal-Beglaubigungen jeweils für Individuen und Gruppen. In Abschnitt 5.2 skizzieren wir die Realisierung der Transaktionen des vorgeschlagenen Abrechnungskonzept mithilfe der Primitive.

5.1 Primitive

Abbildung 5–1 gibt einen Überblick über die verwendeten Primitive, ihre Operationen und deren Argumente. Wir führen die Primitive gleich anhand der Akteure ein, die sie später hauptsächlich benutzen: Krankenkasse (*K*), Arzt (*A*), Patient (*P*), Apotheke/nichtärztliche Leistungserbringer (*L*).

5.1.1 Digitale Signaturen

Mit digitalen Signaturen können digitale Dokumente verbindlich, d.h. durch Gerichte nachprüfbar, authentisiert werden [14, 20]. Digitale Signaturen stellen drei Operationen bereit.

- **Erzeuge Schlüsselpaar** (*genKey*)*:* Ein

Operation	Aufruf	Argumente	
	Digitale Signaturen		
Generiere Schlüsselpaar	$(rk, pk) = genKey(\bullet)$	rk, pk: $\bullet$:	geheimer/öffentlicher Schlüssel Sicherheitsparameter
Signiere	$\sigma = sign(rk, m)$	m: σ:	Nachricht Signatur
Prüfe eine Signatur	$ok = verify(pk, \sigma, m)$	ok:	Ergebnis der Prüfung
	Gruppensignaturen		
Generiere Individualschlüsselpaar	$(ri_A, pi_A) = genIKey(\bullet)$	ri_A: pi_A:	Geheimer Individualschlüssel öffentlicher Individualschlüssel
Generiere Gruppenschlüsselpaar	$(rg_G, pg_G) = genGKey(pi_A, \bullet)$	$\bullet$: rg_G:	Sicherheitsparameter geheimer Gruppenschlüssel
Signiere	$\sigma = gSign(ri_A, pi_A, pk_G, m)$	pg_G:	öffentlicher Gruppenschlüssel
Prüfe Gruppensignatur	$ok = gVerify(pg_G, \sigma, m)$		
Deanonymisiere Signierer	$pi_A = idSigner(rg_G, pg_G, \sigma, m)$		
	Einmal-Beglaubigungen		
Generiere Schlüsselpaar	$(rk_A, pk_A) = genKeyC(\bullet)$	rk_A: pk_A:	geheimer Schlüssel (Aussteller) öffentlicher Schlüssel (Aussteller)
Stelle Beglaubigung aus	$(VB, ps) = issue(rk_K, m, P)$	P: VB:	Empfänger (Patient) V-Beglaubigung
Lege Beglaubigung vor	$(VT, ps) = show(pk_K, VB, A)$	ps: A:	Zielpseudonym Prüfer (Arzt)
Rechne Beglaubigung ab	$ok = deposit(pk_K, VT, A, K)$	VT: id:	Protokollmitschrift für VB Errechnete Identität nach Mehrfachvorlage
Identifiziere Mehrfachabrechner	$id = idShower(VT)$		
	Gruppen-Beglaubigung		
Generiere Individualschlüsselpaar	$(ri_A, pi_A) = genIKeyC(\bullet)$	l: MB:	Typ der Beglaubigung Gruppen-Beglaubigung
Generiere Gruppenschlüsselpaar	$(rg_G, pg_G) = genGKeyC(pi_A, \bullet)$	L: MT:	Prüfer (Leistungserbringer) Protokollmitschrift für MB
Stelle Beglaubigung aus	$MB = gIssue(ri_A, pi_A, pk_G, m, l, ps)$		
Lege Beglaubigung vor	$(MT, ps) = gShow(pk_G, MB, L)$		
Deanonymisiere Aussteller	$pi_A = idIssuer(rg_G, pg_G, MT)$		

Abbildung 5-1 Kryptographische Primitive

Leistungserbringer generiert sich einen geheimen Schlüssel *rk* und einen zugehörigen öffentlichen Schlüssel *pk*. Der öffentliche Schlüssel wird später zur Prüfung von Signaturen benötigt und muß daher authentisch unter dem Namen des Leistungserbringers, z.B. mit Hilfe eines Trust Centers, veröffentlicht werden. Dies gilt auch für die öffentlichen Schlüssel aller folgenden Primitive.

- **Signiere** (*sign*): Ein Leistungserbringer signiert mit Hilfe seines geheimen Schlüssels *rk* eine Nachricht m. Das Ergebnis ist eine digitale Signatur σ.
- **Prüfe eine Signatur** (*verify*): Die Krankenkasse prüft mit Hilfe des öffentlichen Schlüssels *pk* eines Leistungserbringers, ob dessen Signatur σ unter der Nachricht *m* gültig ist.

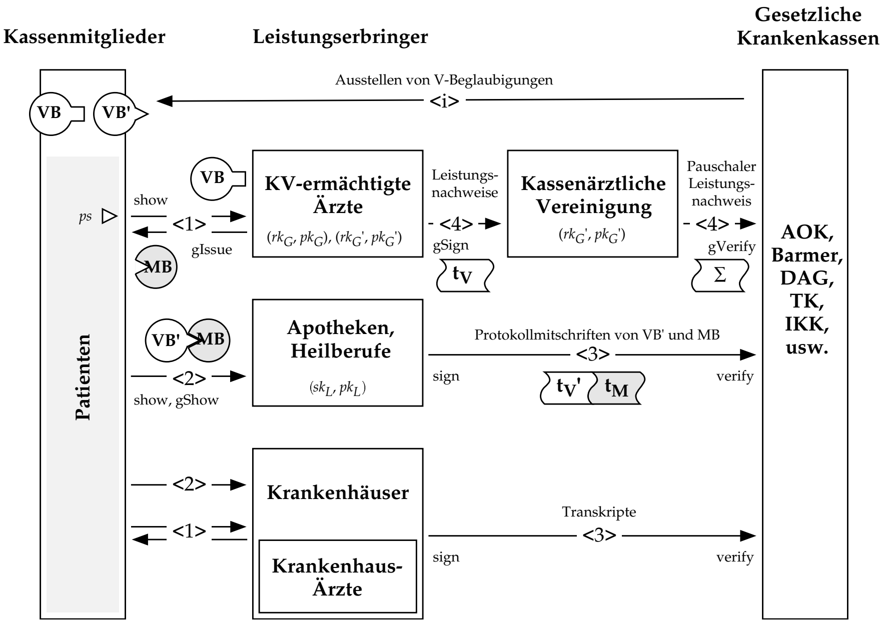


Abbildung 5-2 Digitale Abrechnung von ärztlicher Behandlung und Rezepten

5.1.2 Gruppensignaturen

Gruppensignaturen sind digitale Signaturen, die nur von Mitgliedern einer Gruppe erzeugt werden können, denen aber das unterschreibende Mitglied selbst nicht anzusehen ist. Einzig eine Gruppenzentrale kann diese Anonymität aufheben [12, 13]. Gruppensignaturen stellen fünf Operationen bereit.

- **Erzeuge Individualschlüsselpaar und Gruppenschlüsselpaar** (*genIkey, GenGkey*): Ein Arzt A generiert sich einen geheimen ri_A und zugehörigen öffentlichen Individualschlüssel pi_A (private und public individual key). Jeder, der sich auf diese Art einen Individualschlüssel erzeugt hat, kann anschließend mit anderen Ärzten eine Gruppe bilden. Eine Zentrale der Gruppe G kann aus den öffentlichen Individualschlüsseln der Mitglieder einen gehei
- men rg_G und einen öffentlichen Gruppenschlüssel pg_G erzeugen (private und public group key). Es gibt weitere Operationen zum Einrichten und Löschen der Mitgliedschaft in einer Gruppe. Man wird z.B. Mitglied in einer Gruppe, indem man seinen öffentlichen Individualschlüssel mitteilt und dafür das Gruppenschlüsselpaar erhält.
- **Signiere** (*gSign*): Der Arzt A signiert mit Hilfe seines geheimen Individualschlüssels eine Nachricht *m*. Das Ergebnis ist eine digitale Gruppensignatur σ.
- **Prüfe eine Gruppensignatur** (*gVerify*): Die Krankenkasse prüft mit Hilfe des öffentlichen Gruppenschlüssels pg_G der Ärztegruppe *G* die Unterschrift σ unter der Nachricht *m*. Eine erfolgreiche Prüfung bedeutet, daß die Unterschrift σ von einem Mitglied der Gruppe *G* geleistet wurde, gibt aber keinen weiteren Hinweis von welchem.
- **Deanonymisiere Signierer** (*idSigner*): Die Zentrale der Ärztegruppe *G* ermittelt mit Hilfe ihres geheimen und öffentlichen Gruppenschlüssels, welches Grup penmitglied die Signatur σ zur Nachricht *m* erzeugt hat, und zwar anhand der öffentlichen Individualschlüssel der Gruppenmitglieder.

5.1.3 Einmal-Beglaubigungen

Einmal-Beglaubigungen sind die digitale Version von Münzgeld: Nach Ausstellen einer Beglaubigung (Münze) kann diese einmal vorgelegt (bezahlt) werden. Ausstellen und Vorlegen sind nicht verkettbar [6, 7, 11]; der Aussteller ist jedoch identifizierbar. Empfangen und Vorlegen einer Einmal-Beglaubigung geschieht unter einem Pseudonym. Zwei Beglaubigungen *passen* zueinander, wenn sie unter demselben Pseudonym vorgelegt werden können. Beglaubigungen stellen fünf Operationen bereit.

- **Erzeuge Schlüsselpaar** (*genKeyC*): Eine Krankenkasse *K*, die V-Beglaubigungen ausstellen möchte, erzeugt sich einen geheimen *rk* und einen zugehörigen öffentlichen Schlüssel *pk*. Der geheime Schlüssel dient zum Ausstellen von Beglaubigungen, der öffentliche zum Prüfen.
- **Stelle Einmal-Beglaubigung aus** (*issue*): Eine Krankenkasse *K* mit geheimem Schlüssel rk_K stellt einem Patienten *P* eine V-Beglaubigung auf ein Recht *m* aus. Dabei wird bereits festgelegt, unter welchem Pseudonym *ps* der Patient seine V-Beglaubigung später vorlegen kann. Dies Pseudonym wird zufällig erzeugt, seine Wahl hängt von den Eingaben der Krankenkasse und des Patienten ab und allein der Patient kennt es anschließend. Könnte die Krankenkasse das Pseudonym allein wählen, könnte sie Merkmale des Patienten hineinkodieren; könnte es der Patient allein wählen, könnte er sich zwei V- Beglaubigungen für dasselbe Pseudonym ausstellen lassen und anschließend dieselbe M-Beglaubigung zweimal verwenden (vgl. Abschnitte 5.2.2 und 5.2.5).
- **Lege Einmal-Beglaubigung vor** (*show*): Nachdem ein Patient *P* eine V-

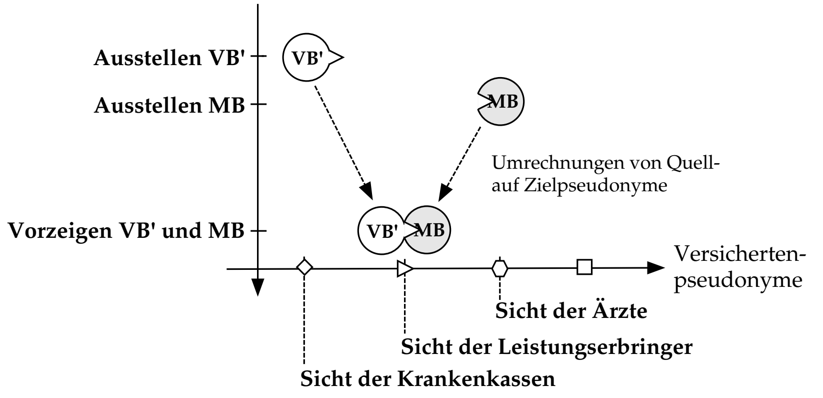


Abbildung 5-3 Verkettung einer M- und einer V-Beglaubigung durch identische Pseudonyme

Beglaubigung erhalten hat, kann er sie einem Arzt *A* unter dem vorbereiteten Pseudonym *ps* vorlegen. Da das Pseudonym schon bei der Ausstellung festgelegt wurde, ist es keine Eingabe an diese Operation. Als Ergebnis erhält der Arzt eine Protokollmitschrift *VT* des Einreichens von *VB* und das Pseudonym *ps*. Die Protokollmitschrift dient dem Arzt später als Abrechnungsbeleg.

- **Rechne Beglaubigung ab** (*deposit*): Der Arzt *A* reicht die Protokollmitschrift *VT* bei der entsprechenden Krankenkasse ein. Verwendet wird der öffentliche Schlüssel *pk* der Krankenkasse, die *VB* ausgegeben hat. Ist die Prüfung erfolgreich, wird der Betrag erstattet.
- **Identifiziere Mehrfachvorleger** (*idShower*): Anhand einer Datenbank aller bisher eingereichten Protokollmitschriften prüft die Krankenkasse, ob die neue Protokollmitschrift *VT* schon einmal vorgelegt worden ist. Aus beiden Protokollmitschriften wird dann der betreffende Patient identifiziert. Anstelle einer nachträglichen Identifizierung beim Einreichen kann der Arzt Betrug auch vorbeugen, indem er die Protokollmitschriften schon beim Prüfen on-line auf Mehrfachvorlage prüfen läßt [6, 7].

5.1.4 Gruppen-Beglaubigungen

Gruppen-Beglaubigungen sind eine Erweiterung von Einmal-Beglaubigungen, bei der der Aussteller innerhalb einer Gruppe anonym ist. Gruppen-Beglaubigungen verhalten sich zu Beglaubigungen wie Gruppensignaturen zu Signaturen, wobei Aussteller (-gruppen) Signierer (-gruppen) entsprechen. Analog gibt es auch hier eine Gruppenzentrale, die den Aussteller einer Beglaubigung deanonymisieren kann.

Aufgrund dieser Ähnlichkeiten ist es naheliegend, Gruppen-Beglaubigungen durch blinde Gruppensignaturen [4] zu realisieren. Gruppen-Beglaubigungen stellen fünf Operationen bereit

- **Erzeuge Individualschlüsselpaar und Gruppenschlüsselpaar** (*genIKeyC, genGKeyC*): Ein Arzt *A* erzeugt sich einen geheimen Individualschlüssel ri_A und einen öffentlichen Individualschlüssel pi_A zum Erzeugen bzw. späteren Prüfen von Gruppen-Beglaubigungen. Eine Zentrale einer Gruppe *G* kann aus den öffentlichen Individualschlüsseln der Mitglieder einen geheimen rg_G und einen öffentlichen Gruppenschlüssel pg_G erzeugen (private und public group key). Die Verwaltung von Gruppenmitgliedern geschieht analog wie bei Gruppensignaturen.
- **Stelle Gruppen-Beglaubigung aus** (*gIssue*): Ein Arzt *A* der Gruppe *G* stellt einem Patienten *P* eine Gruppen-Beglaubigung auf die Verschreibung *m* vom Typ *l* aus. Der Patient liefert als geheime Eingabe sein Pseudonym *ps* unter dem er seine M-Beglaubigung später vorlegen möchte.
- **Lege Gruppen-Beglaubigung vor** (*gShow*): Nachdem ein Patient *P* eine M-Beglaubigung erhalten hat, kann er sie einem Leistungserbringer unter dem vorbereiteten Pseudonym *ps* vorlegen. Da das Pseudonym schon bei der Ausstellung festgelegt wurde, ist es keine Eingabe an diese Operation. Als Ergebnis erhält der Leistungserbringer eine Protokollmitschrift *MT* dieser Operation und das Pseudonym *ps*. Die Protokollmitschrift dient dem Leistungserbringer später als Abrechnungsbeleg.
- **Deanonymisiere Aussteller** (*idIssuer*): Die Gruppenzentrale identifiziert mit Hilfe des geheimen und öffentlichen Gruppenschlüssels den Arzt *A* aus Gruppe *G*, der die M-Beglaubigung *MB* für die Verschreibung *m* erzeugt hat.

5.2 Protokollskizze

Im folgenden wird ein vollständiger Abrechnungsvorgang gemäß Abschnitt 4 exemplarisch mit Hilfe der eingeführten Primitive (Abschnitt 5.1) ausgedrückt. Die Grundidee ist, V-Beglaubigungen als Einmalbeglaubigungen (weiße Münzen in der Abbildung) und M-Beglaubigungen als Gruppen-Beglaubigungen (graue Münzen) zu realisieren. Zum Einreichen von Abrechnungsdaten verwenden Ärzte Gruppensignaturen (Abschnitt 5.1.2) und Apotheken/Heilberufe verwenden digitale Signaturen (Abschnitt 5.1.1). Die Abschnitte 5.2.1 bis 5.2.4 beschreiben die einmalige Initialisierung aus Abb. 4-1. Die Abschnitte 5.2.5 bis 5.2.8 zeigen die anschließende Abrechnung.

5.2.1 Initialisierung

Ärzte erzeugen sich je einen Individualschlüssel um Gruppen-Signaturen (Abrechnung ärztlicher Honorare) und Gruppen-Beglaubigungen (Verschreibungen) leisten zu können. Leistungserbringer erzeugen sich jeweils Individualschlüssel um digitale Signaturen leisten zu können.

5.2.2 Ausstellen von V-Beglaubigungen an Patienten

Die Krankenkasse stellt ihren Mitgliedern V-Beglaubigungen in Form von Einmal-Beglaubigungen aus. Für jede

Behandlung und jede Leistungserbringung legen Patienten später eine frische V-Beglaubigung vor (Abschnitt 5.1.4):

<i> Die Krankenkasse K mit geheimem Schlüssel rk_K erzeugt für einen Patienten P je eine Menge von V-Beglaubigungen für Arztbesuche, Zahnarztbesuche, etc. Zwei Aufrufbeispiele für diese Operation sind unten gezeigt. Der Patient kann diese V-Beglaubigungen anschließend unter den Pseudonymen bzw. ▷ vorlegen (vgl. Abb. 5–2):

$(VB,\ \ ) = issue(rk_K, \text{'Arztbesuch'}, P),$
$(VB', \triangleright) = issue(rk_K, \text{'Arztbesuch'}, P)$

5.2.3 Eintragung von Kassenzulassungen

Als Kassenzulassung für den Arzt dient die Mitgliedschaft in einer Gruppe zugelassener Ärzte. Solche Gruppen können z.B. von einer Kassenärztlichen Vereinigung verwaltet werden. Um später ein Rezept anonym ausstellen zu können, erzeugt sich der Arzt ein eigenes Schlüsselpaar (ri_A, pi_A) und läßt sich in eine Gruppe G aufnehmen (Abschnitt 5.1.2).

<ii> Ein Arzt A erzeugt sich je ein persönliches Schlüsselpaar für Gruppenbeglaubigungen und Gruppensignaturen:

$(ri_A, pi_A) = genIKeyC(\bullet)$, und
$(ri_A', pi_A') = genIKey(\bullet)$.

Die Gruppenzentrale erzeugt den geheimen und öffentlichen Gruppenschlüssel aus den Schlüsseln der Mitglieder. Der geheime Gruppenschlüssel verbleibt bei der Zentrale, der andere wird veröffentlicht:

$(rg_G, pg_G) = genGKeyC(pi_A, \bullet)$, und
$(rg_G', pg_G') = genGKey(pi_A', \bullet)$.

5.2.4 Erzeugen von Zulassungen für Leistungserbringer

Leistungserbringer generieren sich ein Schlüsselpaar, um digitale Signaturen (Abschnitt 5.1.1) leisten zu können. Die öffentlichen Schlüssel werden von den Krankenkassen registriert.

<iii> Aufruf für einen Leistungserbringer (L):

$(rk_L, pk_L) = genKey(\bullet)$.

Nachdem die Initialisierungsphase abgeschlossen ist, können beliebig viele Abrechnungen erfolgen. Wir beschreiben die einzelnen Schritte (Abb. 5-2).

5.2.5 Ausstellen eines Rezepts

Auf Vorlage einer V-Beglaubigung seines Patienten

$(VT, ps) = show(pk_K, VB, A)$

stellt der Arzt eine M-Beglaubigung als Verschreibung m vom Typ l aus. Der Typ gibt an, ob es sich z.B. um ein Medikament, eine Facharztüberweisung oder eine Krankenhauseinweisung handelt. Der Patient gibt ein Pseudonym ein, unter dem er die erwartete M-Beglaubigung später vorlegen möchte. Er wählt dafür eines seiner Pseudonyme (hier ▷) aus, für das er bereits eine V-Beglaubigung hat (Abb. 5-3):

<1> Der Arzt A aus Gruppe G stellt seinem Patienten eine M-Beglaubigung MB auf den Inhalt m vom Typ l aus, so daß sein Patient die M-Beglaubigung später unter dem gewünschten Pseudonym ▷ vorlegen kann. Das Pseudonym ▷ ist ein geheimer Eingabeparameter des Patienten, den der Arzt nicht erfährt:

$MB = gIssue(ri_A, pi_A, pk_G, m, l, \triangleright)$

Diese Operation ist dem Ausstellen von V-Beglaubigungen sehr ähnlich, erlaubt dem Patienten aber, ein Pseudonym vorzugeben, statt es zufällig wählen lassen.

5.2.6 Vorlegen eines Rezepts

Der Patient reicht nun sein Rezept bei einem Leistungserbringer ein. (Zur Vorbeugung vor mehrfachem Vorlegen siehe Abschnitt 5.1.3.)

<2> Der Patient P legt seine M-Beglaubigung MB zusammen mit der dazu passenden V-Beglaubigung VB' einem Leistungserbringer L zur Prüfung vor:

$(MT, ps) = gShow(pk_G, MB, L)$,
$(VT', ps') = show(pk_K, VB', L)$.

Der Leistungserbringer erstattet die Kosten später nur, wenn beide Beglaubigungen unter demselben Pseudonym vorgelegt werden ($ps \overset{?}{=} ps'$). Im Beispiel ergibt sich

$ps = ps' = \triangleright$.

5.2.7 Abrechnen eines Rezepts

<3> Ein Leistungserbringer L rechnet die vorgelegte M-Beglaubigung mit der entsprechenden Krankenkasse ab, indem er die Protokollmitschriften der eingereichten M- und V-Beglaubigungen einreicht und durch seine digitale Signatur bestätigt, daß er die Leistung erbracht hat.

$\sigma = sign(rk_L, (\text{'invoice'}, MT, VT))$

Die Krankenkasse prüft die Unterschrift des Leistungserbringers und ob die M-Beglaubigung von einem Arzt ausgestellt worden ist, indem er die Überprüfungen des Leistungserbringers wiederholt:

$ok = verify(pk_L, \sigma, (\text{'invoice'}, MT, VT'))$,

$(MT, ps) = gShow(pk_G, MB, K)$,

$ok = deposit(pk_K, VT', L, K)$.

Ist die Prüfung erfolgreich, erstattet die Krankenkasse die Kosten. Bei Mehrfachvorlage der Protokollmitschrift *VT'* kann der betrügerische Patient identifiziert werden und Regress erfolgen:

$idShower(VT')$

Die Prüfung auf Mehrfachvorlage ist nur eine zusätzliche Sicherungsmaßnahme zum Erkennen von Hardwaremanipulationen. Sie ist bereits nach Schritt <2> erforderlich, wenn nicht nur Bezahlung unberechtigt erhaltener Leistungen verhindert, sondern auch die Leistungserbringung selbst unterbunden werden soll, zum Beispiel im Fall riskanter bzw. teurer Medikamente (Betäubungsmittel, etc.).

5.2.8 Abrechnen ärztlicher Leistungen bei der KV

Der Arzt *A* aus Gruppe *G* rechnet seine Behandlungsleistungen mit der Krankenkasse ab. Einziger Unterschied zur Abrechnung anderer Leistungserbringer ist, daß Ärzte anonym abrechnen können, was durch Verwendung von Gruppensignaturen anstelle digitaler Signaturen erreicht wird:

<4> Arzt:

$\sigma = gSign(ri_A, pi_A, pk_G, (\text{'invoice'}, VT))$,

$ok = deposit(pk_K, VT, A, K)$

Die Krankenkasse erstattet die Kosten, falls die Gruppensignatur gültig ist und die Protokollmitschrift *VT* nicht von einer mehrfach vorgelegten V-Beglaubigung stammt:

$ok = gVerify(pk_G, \sigma, (\text{'invoice'}, VT))$,

$idShower(VT)$

5.3 Kostenkontrolle

Das hier vorgestellte Konzept ermöglicht effektive Kostenkontrolle durch die Krankenkasse und die Kassenärztliche Vereinigung. Da Ärzte nur innerhalb ihrer Gruppe anonym sind, kann die Krankenkasse Verschreibungsprofile von einzelnen Arztgruppen erstellen. Überschreitet eine Gruppe ihr Verschreibungsbudget, können die Mitglieder dieser Gruppe mithilfe der Kassenärztlichen Vereinigung vollständig oder stichprobenhaft deanonymisiert und überprüft werden:

<5> Kassenärztliche Vereinigung:

$pi_A = idIssuer(rg_G, pg_G, MB)$

Die Zentrale der Gruppe *G* identifiziert den Arzt *A*, der die M-Beglaubigung *MB* ausgestellt hat, anhand seines öffentlichen Individualschlüssels pi_A.

Die Krankenkasse ist auch in der Lage, die Kosten der anderen medizinischen Leistungen zu begrenzen. Die Ausgaben der nichtärztlichen Leistungserbringer können direkt anhand der nichtanonymen Abrechnungen überprüft werden.

Eine weitere Kontrollmöglichkeit ist die Begrenzung der ausgegebenen V-Beglaubigungen oder die Abrechnung mit einem Punktesystem, bei dem die erbrachten Leistungen erst am Quartalsende bewertet und vergütet werden.

6 Zusammenfassung und Ausblick

Wir haben in diesem Papier gezeigt, daß Abrechnung medizinischer Daten auch bei Berücksichtigung *aller* Sicherheitsinteressen aller Beteiligten möglich ist. Dies schließt erstmals auch den Schutz der Daten der beteiligten Patienten und Ärzte ein. Eine kryptographische Realisierung mit „Group Credentials“ [3] wurde skizziert. Auf eine Darstellung technischer Details wurde in dieser Arbeit zugunsten der Erläuterung von Zusammenhängen verzichtet. Zur Vertiefung werden [3, 6, 7] empfohlen.

7 Dank

Wir danken Bernd Blobel, der uns als erster auf die besondere Verletzlichkeit des Arzt-Patientenverhältnisses aufmerksam gemacht hat, sowie Klaus Pommerening und Michael Hortmann für ihre Anregungen zu dieser Arbeit. Birgit Pfitzmann, Joachim Biskup und Simon Jenkins haben frühere Versionen dieser Arbeit sorgfältig kommentiert. Dirk Fox gab wertvolle Hinweise, diese Arbeit lesbarer und kürzer zu machen. Unterstützt wurden die Autoren von der Deutschen Forschungsgemeinschaft und den EU-Projekten ISHTAR (Implementing Secure Health Telematics Applications for euRope) und SEMPER (Secure Electronic Market Place for EuRope).

8 Literatur

[1] Biskup J: Medical Database Security; Data Protection and Confidentiality in Health Informatics – Handling Health Data in Europe in the Future, Edited by the Commission of the European Communities DG XIII/F AIM, Proc. of the AIM Working Conference, Brussels, 19-21 March 1990, IOS Press, Amsterdam 1991, 214-230.

[2] Biskup J: Protection of privacy and confidentiality in medical information systems; Database Security III: Status and Prospects (eds.: Spooner DL, Landwehr CE), North-Holland, 1990, 13 – 23.

[3] Bleumer G: Group Credentials; Hildesheimer Informatik Bericht (erscheint 12/96)

[4] Bleumer G, Schunter M: Privacy-Oriented Clearing for the German Health-Care System, Workshop on Personal Information, Cambridge, GB, 22nd June 1996.

[5] Buchholz EH: Unser Gesundheitswesen: Ein einführender Überblick zum Gesundheitswesen der Bundesrepublik Deutschland, Springer-Verlag, Berlin, 1988.

[6] Brands S: An Efficient Off-line Electronic Cash System Based On The Representation Problem; Centrum voor Wiskunde en Informatica, Computer Science/Departement of Algorithmics and Architecture, Report CS-R9323, March 1993.

[7] Brands S: Untraceable Off-line Cash in Wallet with Observers; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994 302-318.

[8] Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie: INFORMATIONSGESELLSCHAFT: Chancen, Innovationen und Herausforderungen; Rat für Forschung, Technologie und Innovation, Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, 1995.

[9] Bundesamt für Sicherheit in der Informationstechnik: Chipkarten im Gesundheitswesen; Schriftenreihe zur IT-Sicherheit Band 5, Bundesanzeiger Verlag, Köln 1995.

[10] Chaum D: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; AUSCRYPT'90, LNCS 453, Springer-Verlag, Berlin 1990, 246-264.

[11] Chaum D, Fiat A, Naor M: Untraceable Electronic Cash, Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327.

[12] Chaum D, van Heijst E: Group Signatures; Eurocrypt '91, LNCS 547, Springer-Verlag, Berlin 1991, 257-265.

[13] Chen L, Pedersen TP: New Group Signature Schemes; EUROCRYPT '94, Proceedings, LNCS 950, Springer-Verlag, Berlin 1995, 171-181.

[14] Diffie W, Hellman ME: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

[15] Focus: Handel mit geheimen Daten; Focus 43 (1996).

[16] Häußler S, Liebold R, Narr H: Die Kassenärztliche Tätigkeit; Springer-Verlag, Berlin, 1984.

[17] Low SH, Maxemchuk NF: Anonymous Credit Cards; 2nd ACM Conference on Computer and Communications Security, Fairfax, November 1994, ACM Press, New York 1994, 108-117.

[18] Maxemchuk NF, Low SH: The Use of Communication Networks to Increase Personel Privacy in a Health Insurance Architecture; Manuscript, 1995.

[19] Pfitzmann A, Pfitzmann B, Schunter M, Waidner M: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule; Brüggemann HH, Gerhardt-Häckl W (ed.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS'95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 329-350.

[20] Rivest RL, Shamir A, Adleman L: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120-126, reprinted: 26/1 (1983) 96-99.

[21] Markus Stadler, Jean-Marc Piveteau, Jan Camenisch: Fair Blind Signatures; Eurocrypt '95, LNCS 921, Springer-Verlag, Berlin 1995, 209-219.

[22] Struif B: Das elektronische Rezept mit digitaler Unterschrift; Reimer H, Struif B (eds.): Kommunikation & Sicherheit, TeleTrust Deutschland e.V., Darmstadt 1992, 71-75.

[23] Struif B: Sicherheit und Datenschutz bei elektronischen Rezepten; Multicard´94, Elektronische Kartensysteme – Anspruch und Wirklichkeit, Kongreßdokument I, 23.-25. Februar 1994, Berlin, 71-80.