(19) Deutsches Patent- und Markenamt

(10) **DE 10 2008 000 897 B4** 2018.05.03

(12) # Patentschrift

(21) Aktenzeichen: **10 2008 000 897.4**
(22) Anmeldetag: **31.03.2008**
(43) Offenlegungstag: **01.10.2009**
(45) Veröffentlichungstag der Patenterteilung: **03.05.2018**

(51) Int Cl.: ***H04B 5/00*** (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
CompuGroup Medical SE, 56070 Koblenz, DE

(74) Vertreter:
Richardt Patentanwälte PartG mbB, 65185 Wiesbaden, DE

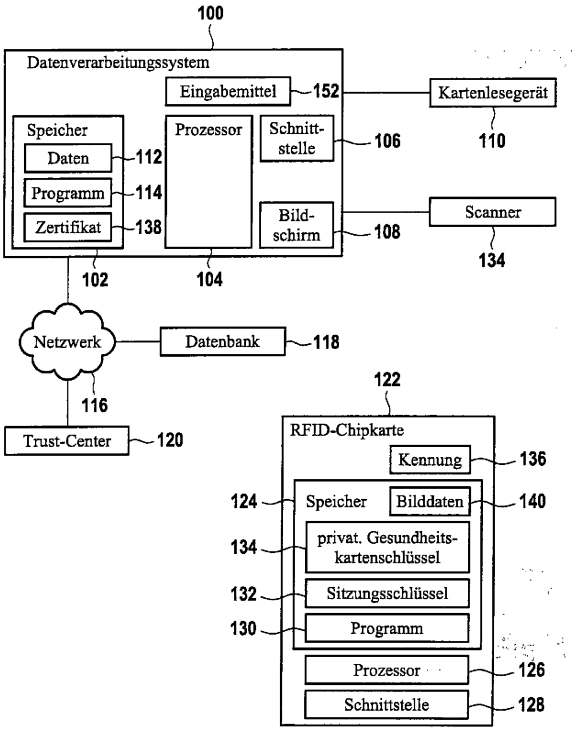
(72) Erfinder:
Gotthardt, Frank, 56337 Eitelborn, DE

(56) Ermittelter Stand der Technik:

DE	**10 2004 051 296**	**B3**
DE	**102 58 769**	**A1**
DE	**10 2004 026 933**	**A1**
DE	**10 2005 009 051**	**A1**
DE	**10 2005 025 806**	**A1**
US	**5 721 781**	**A**

(54) Bezeichnung: **Kommunikationsverfahren einer elektronischen Gesundheitskarte mit einem Lesegerät**

(57) Hauptanspruch: Kommunikationsverfahren einer elektronischen Gesundheitskarte (122) mit einem Lesegerät, wobei zwischen der elektronischen Gesundheitskarte (122) und dem Lesegerät (110) eine Kommunikationsverbindung aufgebaut wird, wobei es sich bei der Kommunikationsverbindung um eine Nahfeldverbindung handelt, wobei das Kommunikationsverfahren ferner den Schritt umfasst des Anmeldens der elektronischen Gesundheitskarte (122) an dem Lesegerät, wobei beim Anmelden die folgenden Schritte ausgeführt werden:
- optisches Lesen einer auf der elektronischen Gesundheitskarte (122) aufgedruckten Kennung (136) durch das Lesegerät,
- Durchführung eines Challenge-Response Verfahrens zwischen der elektronischen Gesundheitskarte (122) und dem Lesegerät, wobei für eine Verschlüsselung beim Challenge-Response Verfahren eine Verschlüsselung unter Verwendung der Kennung erfolgt, wobei es sich bei der Kennung um einen öffentlichen Gesundheitskartenschlüssel handelt, wobei ferner in der elektronischen Gesundheitskarte (122) ein privater Gesundheitskartenschlüssel elektronisch gespeichert ist, wobei der öffentliche und der private Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden.



Beschreibung

[0001] Die Erfindung betrifft ein Kommunikationsverfahren einer elektronischen Gesundheitskarte mit einem Lesegerät, eine elektronische Gesundheitskarte, ein Lesegerät, sowie ein Computerprogrammprodukt.

[0002] Die elektronische Gesundheitskarte, abgekürzt eGK, soll seit Beginn des Jahres 2006 die Krankenversicherungskarte in Deutschland ersetzen. Ziel ist es dabei, eine Datenübermittlung zwischen medizinischen Leistungserbringern, Krankenkassen, Apotheken und Patienten in Zukunft kostengünstiger zu gestalten, zu vereinfachen und zu beschleunigen. Dazu gehört unter anderem auch die Ermöglichung eines Zugriffs auf einen elektronischen Arztbrief, einer elektronischen Krankenakte, sowie des elektronischen Rezeptes mit Hilfe der elektronischen Gesundheitskarte. Auf der elektronischen Gesundheitskarte ist aufgrund des dort verfügbaren geringen Speicherplatzes nur ein gewisser Teil von Pflichtangaben gespeichert. So sind z. B. Angaben zur Identität des Patienten, zur Notfallversorgung und optional auch Vermerke, z. B. zum Organspenderstatus des Patienten auf der Karte gespeichert. Der Zugriff auf Dokumentationen zu eingenommenen Medikamenten, dem elektronischen Arztbrief, der elektronischen Krankenakte und dem elektronischen Rezept erfolgt über gesicherte Zugangsknoten zu Fachdiensten der Telematik-Infrastruktur.

[0003] Die DE 10 2004 051 296 B3 beschreibt ein Verfahren zur Speicherung von Daten und zur Abfrage von Daten, sowie entsprechende Computerprogrammprodukte. Eine personalisierte Chipkarte ermöglicht die Speicherung einer virtuellen Patientenakte auf einem Datenserver. Unter Verwendung der Chipkarte können Daten, wie z. B. eine Patientenakte, von einem Praxis-EDV-System einer Arztpraxis verschlüsselt an den Datenserver übertragen werden.

[0004] Aus der DE 102 58 769 A1 ist eine weitere Anwendung von Chipkarten für Patientendaten bekannt.

[0005] DE 10 2005 009 051 A1 offenbart eine Chipkarte für eine Kommunikationseinrichtung, wobei es sich bei der Chipkarte beispielsweise um eine Gesundheitskarte handelt. Über eine Nahfeldkommunikation kann die Gesundheitskarte mit einem entsprechenden Empfänger kommunizieren.

[0006] DE 10 2004 026 933 A1 offenbart ein Systemverfahren zur Authentifizierung eines Benutzers. Auch hier erfolgt eine Datenübertragung zwischen einer elektronischen Gesundheitskarte und einem entsprechenden Empfänger drahtlos.

[0007] US 5 721 781 A offenbart ein Authentifizierungssystem unter Verwendung einer Chipkarte.

[0008] DE 10 2005 025 806 A1 offenbart ein Verfahren zum Zugriff von einer Datenstation auf ein elektronisches Gerät sowie ein Computerprogrammprodukt, ein elektronisches Gerät und eine Datenstation. Das elektronische Gerät weist eine Zuordnungstabelle auf, in der unterschiedlichen Datenobjekten ein kryptografisches Protokoll unterschiedlicher Sicherheitsstufe zugeordnet ist. Die Datenstation übermittelt dem elektronischen Gerät hierbei zunächst eine Anforderung für das eine der Datenobjekte. Das elektronische Gerät bestimmt mit Hilfe der Zuordnungstabelle ein kryptografisches Protokoll für das eine der Datenobjekte. Das elektronische Gerät und die Datenstation führen das kryptografische Protokoll durch. Unter der Voraussetzung einer erfolgreichen Durchführung übermittelt das elektronische Gerät das eine der Datenobjekte an die Datenstation.

[0009] Aus dem Stand der Technik bekannte Gesundheitskarten sind kontaktbehaftet. Dies bedeutet, dass zur Verwendung einer Chipkarte in Form einer elektronischen Gesundheitskarte diese in ein Lesegerät eines z. B. Apotheken-Informationssystems eingeführt werden muss, so dass daraufhin ein entsprechender Zugriff auf beispielsweise elektronische Rezeptdaten ermöglicht wird.

[0010] Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein verbessertes Kommunikationsverfahren einer elektronischen Gesundheitskarte mit einem Lesegerät, eine verbesserte elektronische Gesundheitskarte, ein verbessertes Lesegerät sowie ein verbessertes Computerprogrammprodukt zu schaffen.

[0011] Die der Erfindung zugrundeliegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

[0012] Erfindungsgemäß wird ein Kommunikationsverfahren zur Kommunikation zwischen einer elektronischen Gesundheitskarte und einem Lesegerät geschaffen, wobei zwischen der elektronischen Gesundheitskarte und dem Lesegerät eine Kommunikationsverbindung aufgebaut wird, wobei es sich bei der Kommunikationsverbindung um eine Nahfeldverbindung handelt. Bei der Kommunikationsverbindung handelt es sich nach einer Ausführungsform der Erfindung um eine sicherte Kommunikationsverbindung, dh. eine Kommunikationsverbindung, bei welcher z.B. ein secure messaging Verfahren Verwendung findet.

[0013] Das erfindungsgemäße Kommunikationsverfahren hat den Vorteil, dass Patienten beispielsweise

in einer Apotheke nicht mehr die elektronische Gesundheitskarte in ein entsprechendes Lesegerät einführen müssen. Dieses Extra-Einführen der Chipkarte in das Lesegerät hat in der Vergangenheit zu verschiedenen Problematiken geführt. Eine Hauptproblematik liegt in dem Verschleiß des Lesegerätes, da für jede Bedienung eines Patienten in einer Apotheke ein Lesevorgang durchgeführt werden muss. Durch das erfindungsgemäße kontaktlose Kommunikationsverfahren ist ein Verschleiß sowohl von Gesundheitskarten als auch entsprechenden Lesegeräten ausgeschlossen.

[0014] Eine weitere Problematik ergab sich in der Vergangenheit dadurch, dass entweder die Patienten selbst die Gesundheitskarte in das Lesegerät eingeführt haben oder aber dass Patienten die Gesundheitskarte z. B. dem Apothekenpersonal überreicht haben, woraufhin diese die Gesundheitskarte in ein entsprechendes Lesegerät eingeführt haben. Beide Praktiken haben sich in der Vergangenheit als zeitaufwendig erwiesen, da bei einem selbstständigen Einführen der Gesundheitskarte in das Lesegerät die Gesundheitskarte oft falsch herum, das heißt mit der falschen Ausrichtung des Chips relativ zum Lesekopf des Lesegeräts, eingeführt wurde, oder weil durch das Heraussuchen der Gesundheitskarte beispielsweise aus einem Geldbeutel des Patienten, das Überreichen an das Apothekenpersonal, das Auslesen der Gesundheitskarte durch ein entsprechendes Lesegerät, das Zurücküberreichen der Gesundheitskarte an den Patienten, usw., wertvolle Zeit verschwendet wurde, welche den eigentlichen Bedienvorgang eines Patienten wesentlich verlangsamt hat.

[0015] Durch die Verwendung eines kontaktlosen Kommunikationsverfahrens werden all diese Nachteile vermieden.

[0016] Nach einer Ausführungsform der Erfindung wird die Kommunikationsverbindung durch ein RFID-Verfahren aufgebaut. RFID-Systeme beinhalten im Allgemeinen sowohl eine Sende-/Empfangseinheit seitens des Lesegeräts und einen Transponder seitens des RFID-Chips. Der Transponder wird auch als RFID-Etikett, RFID-Chip, RFID-Tag, RFID-Label oder Funketikett bezeichnet Bei RFID-Systemen handelt es sich um Radio Frequency-Identification-Systems, so genannte Funkerkennungssysteme. Die Kommunikation zwischen RFID-Transponder und Lesegerät erfolgt typischerweise über hochfrequente elektromagnetische Wechselfelder.

[0017] Die Verwendung eines RFID-Verfahrens hat den Vorteil, dass die elektronische Gesundheitskarte ohne eigene Stromversorgung verwendet werden kann. Durch ein elektromagnetisches Hochfrequenzfeld des Lesegeräts wird der Transponder der elektronischen Gesundheitskarte mit Energie versorgt, wodurch eine aktive Stromversorgung der Gesundheitskarte entfällt. Dies hat mehrere Vorteile. Zum einen muss sich ein Patient nach einmaligem Ausstellen und Erhalt seiner personalisierten Gesundheitskarte nicht mehr um die „Pflege“ der Gesundheitskarte kümmern. Einmal ausgestellt und aktiviert, wird die Karte ihren Dienst für den gesamten Ausstellungszeitraum der Karte verrichten. Des weiteren hat die Verwendung der RFID-Technik den Vorteil, dass diese miniaturisiert in weitere bereits existierende Geräte und Karten implementiert werden kann: beispielsweise ist es möglich, aufgrund der miniaturisierten RFID-Technik die elektronische Gesundheitskarte in ein bestehendes Ausweisdokument zu integrieren. Beispielsweise bietet sich hier die Möglichkeit, auf ein bestehendes Ausweisdokument, wie z. B. einen Führerschein, eine dünne Folie aufzukleben, welche den RFID-Chip der elektronischen Gesundheitskarte enthält. In diesem fall bleibt es jedem Patienten selbst überlassen, mit welcher personalisierten Karte er die elektronische Gesundheitskarte kombinieren will. Hier bieten sich z. B. Kreditkarten, Geldkarten, Führerscheine, Personalausweise und vieles mehr an. Alternativ ist es auch möglich, aufgrund der geringen Größe des RFID-Chips den RFID-Chip in Armbanduhren, mobile Telekommunikationsgeräte, usw. zu implementieren. Eine weitere Möglichkeit besteht darin, den RFID-Chip direkt unter die menschliche Haut zu implantieren. Aufgrund der geringen Größe des RFID-Chips besteht hier keinerlei Gesundheitsrisiko.

[0018] Nach einer Ausführungsform der Erfindung umfasst das Kommunikationsverfahren ferner den Schritt des Authentifizierens des Nutzers der elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst. Dies kann auf verschiedene Art und Weise erfolgen.

[0019] Nach einer Ausführungsform der Erfindung erfolgt eine Eingabe einer Benutzeridentifikation am Lesegerät, gefolgt von einer Übertragung einer Anforderung zur Fernüberprüfung der Benutzeridentifikation von dem Lesegerät an die elektronische Gesundheitskarte und der Durchführung der Fernüberprüfung der Benutzeridentifikation durch die elektronische Gesundheitskarte. Unter einer „Fernüberprüfung“ wird hier jedes Verfahren verstanden, bei dem die zu überprüfende Kennung nicht an die Gesundheitskarte zur Authentifizierung direkt z.B. verschlüsselt übertragen werden muss, sondern bei dem die Überprüfung mittels eines das Lesegerät und die Gesundheitskarte involvierenden Protokolls erfolgt Entsprechende Protokolle sind an sich aus dem Stand der Technik bekannt, wie zum Beispiel Strong Password Only Authentication Key Exchange (SPEKE), Diffie-Hellman Encripted Key Exchange (DH-EKE), Bellovin-Merritt Protokoll oder Password Authenticated Connection Establishment (PACE).

[0020] Nach einer weiteren dazu alternativen Ausführungsform der Erfindung erfolgt eine Eingabe einer Benutzer-Identifikation am Lesegerät, eine Verschlüsselung der Benutzer-Identifikation durch das Lesegerät mit einem öffentlichen Gesundheitskartenschlüssel der Gesundheitskarte und ein Senden der verschlüsselten Benutzer-Identifikation an die elektronische Gesundheitskarte. Daraufhin entschlüsselt die elektronische Gesundheitskarte die empfangene verschlüsselte Benutzer-Identifikation, wobei die Entschlüsselung mittels eines privaten Gesundheitskartenschlüssels erfolgt, wobei in der elektronischen Gesundheitskarte der private Gesundheitskartenschlüssel elektronisch gespeichert ist, wobei der öffentliche und der private Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden, wobei das Anmelden erfolgreiche ist, wenn die entschlüsselte Benutzer-Identifikation durch die Gesundheitskarte verifiziert wurde.

[0021] Das Authentifizieren des Nutzers der elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte hat den Vorteil, dass gewährleistet ist, dass ein Missbrauch von gestohlenen oder verlorengegangenen elektronischen Gesundheitskarten weitgehend verhindert wird. Ausschließlich der Besitzer der elektronischen Gesundheitskarte, der auch gleichzeitig über die Benutzer-Identifikation verfügt, ist in der Lage, sich gegenüber der elektronischen Gesundheitskarte als rechtmäßiger Besitzer zu identifizieren. Als Benutzer-Identifikation kommt hierbei beispielsweise die Verwendung einer PIN in Betracht, welche am Lesegerät bzw. an einem am Lesegerät angeschlossenen Tastenblock eingegeben wird. Ebenso ist es möglich, als Benutzer-Identifikation ein biometrisches Merkmal des Eigentümers der elektronischen Gesundheitskarte einzugeben. Beispielsweise kann dies in Form eines Fingerabdruck-Scans erfolgen.

[0022] Dadurch, dass zur gesicherten Kommunikation eine Verschlüsselung der Benutzer-Identifikation mit dem öffentlichen Gesundheitskartenschlüssel der Gesundheitskarte erfolgt, wird der Datenaustausch zwischen Gesundheitskarte und Lesegerät minimiert: Eine Aushandlung von Schlüsseln ist nicht erforderlich, was insbesondere im Hinblick auf die Leistungsfähigkeit von RFID-Prozessoren von Vorteil ist: Aufgrund der ohnehin vorgesehenen Chipkarten-Fähigkeiten einer elektronischen Gesundheitskarte ist in jeder Gesundheitskarte bereits die Funktionalität implementiert, dass empfangene Daten unter Verwendung des privaten Gesundheitskartenschlüssels durch die Gesundheitskarte entschlüsselt werden können. Die Implementierung einer zusätzlichen Funktionalität in Form der Verifizierung einer entschlüsselten PIN stellt daher für eine Implementierung in Form eines RFID-Chips keinerlei Problematik dar, da dies weder hohe zusätzliche Rechenkapazitäten noch großen zusätzlichen Speicherplatz benötigt. Um bei der Verwendung von Benutzer-Identifikationen in Form von biometrischen Merkmalen die Rechen- und Speicherkapazität der elektronischen Gesundheitskarte zu minimieren, bietet es sich hier an, beispielsweise bei der Fingerprint-Erkennung lediglich einige wenige Merkmale zu verifizieren, wie z. B. die Lage der Fingerbild-Wirbel, der Knotenpunkte, Linienenden usw.

[0023] Nach einer weiteren Ausführungsform der Erfindung wird der öffentliche Gesundheitskartenschlüssel von der Gesundheitskarte selbst oder von einer externen Datenbank abgerufen. Letzteres ist aus den obig genannten Gründen bevorzugt, da damit der Datenaustausch zwischen Gesundheitskarte und Lesegerät minimiert werden kann. Im Falle des Abrufens des öffentlichen Gesundheitskartenschlüssels von einer externen Datenbank müsste von der Gesundheitskarte lediglich eine entsprechende kryptische Patientenkennung an das Lesegerät übertragen werden, auf Basis derer das Lesegerät den öffentlichen Gesundheitskartenschlüssel aus der externen Datenbank abrufen kann. Es sei hier angemerkt, dass das Konzept der elektronischen Gesundheitskarte ohnehin die Verwendung von öffentlichen Gesundhertskartenschlüsseln vorsieht, so dass hier eine Integration des erfindungsgemäßen Kommunikationsverfahrens in bestehende Telematik-Infrastrukturen ohne weiteres und ohne Änderung der Infrastruktur möglich ist.

[0024] Nach einer weiteren Ausführungsform der Erfindung umfasst das Kommunikationsverfahren ferner den Schritt des Authentifizierens des Lesegeräts gegenüber der elektronischen Gesundheitskarte, wobei nach erfolgreicher Authentifizierung eine Freigabe von Daten zur Datenübertragung von der Gesundheitskarte an das Lesegerät erfolgt, wobei die Daten auf der Gesundheitskarte gespeichert sind. Ein solches Authentifizieren des Lesegeräts gegenüber der elektronischen Gesundheitskarte hat den Vorteil, dass ein Datenaustausch zwischen elektronischer Gesundheitskarte und Lesegerät überhaupt dann erst stattfindet, wenn sich die Gesundheitskarte sicher sein kann, dass das Lesegerät zum Zugriff auf die Gesundheitskarte überhaupt befugt ist. Damit wird wirkungsvoll ein unbemerktes Kontaktaufnehmen beliebiger unbefugter Lesegeräte mit der elektronischen Gesundheitskarte verhindert. Beispielsweise genügt es damit nicht, für den Fall einer PIN-Authentifizierung eines Benutzers gegenüber der Gesundheitskarte die richtige PIN durch kontinuierliches Durchprobieren aller möglichen Kombinationen mittels eines „Brute-Force-Angriffs“ zu erlangen. Die elektronische Gesundheitskarte wird ausschließlich mit solchen Geräten kommunizieren, welches sich als berechtigt gegenüber der elektronischen Gesundheitskarte authentifizieren können.

[0025] Nach einer weiteren Ausführungsform der Erfindung umfasst das Authentifizieren die Schritte des Empfangs eines digitalen Zertifikats durch die elektronische Gesundheitskarte von dem Lesegerät, der Überprüfung der Zertifikats durch die elektronische Gesundheitskarte, wobei das Lesegerät authentifiziert ist, wenn die Zertifikatsprüfung erfolgreich ist. Nach erfolgreicher Zertifikatsüberprüfung, erfolgt der Schritt der Freigabe der Übertragung der Daten von der elektronischen Gesundheitskarte an das Lesegerät, wobei die zur Übertragung vorgesehenen Daten durch die im Zertifikat spezifizierten Zugriffsberechtigungen bestimmt sind.

[0026] Durch die Überprüfung des Zertifikats durch die elektronische Gesundheitskarte beispielsweise unter Verwendung einer Public-Key-Infrastruktur (PKI) wird sichergestellt, dass das Lesegerät vertrauenswürdig ist. Somit kann sich ein Benutzer der elektronischen Gesundheitskarte sicher sein, dass lediglich zertifizierte Stellen mit der elektronischen Gesundheitskarte kommunizieren werden.

[0027] Alternativ zur Verwendung einer Public-Key-Infrastruktur ist es auch möglich, auf der Karte selbst entsprechende öffentliche Schlüssel und die die Schlüssel verifizierenden Zertifikate abzulegen, so dass zur Zertifikat-Verifizierung die elektronische Gesundheitskarte lediglich auf interne Speicherbereiche zugreifen muss. Eine solche Zertifikatsüberprüfung ist beispielsweise als „Card-Verifiable-Certificate (CVC)“ bekannt.

[0028] Die Verwendung von Zertifikaten zur Authentifizierung des Lesegeräts gegenüber der Gesundheitskarte hat ferner den Vorteil, dass Zertifikate in der Regel auch Informationen über den zulässigen Anwendungs- und Geltungsbereich des Zertifikats enthalten. In anderen Worten sind in dem Zertifikat entsprechende Zugriffsberechtigungen spezifiziert, so dass die Gesundheitskarte anhand des Zertifikats feststellen kann, auf welche Bereiche ein entsprechendes Lesegerät zugreifen darf. So ist es z. B. wünschenswert, dass ein behandelnder Arzt Zugriff auf alle Datenbereich der Karte hat, wohingegen ein Apotheken-Informationssystem lediglich auf solche Bereiche zugreifen darf, welche zur Aushändigung von Medikamenten aufgrund eines elektronischen Rezepts notwendig sind. So könnte z. B. ein Arzt auf umfangreiche elektronische Krankenakten unter Verwendung der elektronischen Gesundheitskarte zugreifen dürfen, wohingegen einem Apotheken-Informationssystem lediglich der Zugriff auf hinterlegte Rezeptdaten gestattet ist. Es sei hier darauf hingewiesen, dass die Rezeptdaten und Krankenäkten nicht auf der elektronischen Gesundheitskarte selbst abgelegt sind oder sein müssen, sondern dass vorzugsweise die elektronische Gesundheitskarte lediglich Speicherbereiche mit entsprechenden Verweisen auf extern gespeicherte Daten enthält. Das heißt, die mit dem Zertifikat spezifizierten Zugriffsberechtigungen erlauben es vorzugsweise lediglich, entsprechende Speicherverweise der elektronischen Gesundheitskarte auszulesen, so dass daraufhin die Daten in Form von Rezeptdaten oder Patientenakten von entsprechenden Servern anhand der Speicherverweise abgerufen werden können.

[0029] Nach einer Ausführungsform der Erfindung werden nach erfolgreicher Zertifikatsüberprüfung in der Gesundheitskarte gespeicherte Bilddaten von der Gesundheitskarte an das Lesegerät gesendet, wobei die Bilddaten zumindest ein Gesichtsbild des Inhabers der Gesundheitskarte aufweisen. Daraufhin wird das in den Bilddaten enthaltene Bild visuell am Lesegerät oder an einem an dem Lesegerät angeschlossenen Datenverarbeitungssystem angezeigt, um eine Sichtprüfung zu ermöglichen.

[0030] In anderen Worten wird nach erfolgreicher Zertifikatsüberprüfung auf einem Bildschirm beispielsweise einem Arzt oder einem Apotheker das auf der Patientenkarte gespeicherte Lichtbild des Patienten angezeigt Dadurch kann der Arzt oder Apotheker durch eine einfache Sichtprüfung entscheiden, ob der momentane Besitzer der Gesundhertskarte auch deren rechtmäßiger Eigentümer ist. Der Arzt wird einen weiteren Zugriff auf die Gesundheitskarte nur dann gegenüber dem Lesegerät bzw. Datenverarbeitungssystem bestätigen und genehmigen, wenn offensichtlich kein Missbrauch der elektronischen Gesundheitskarte vorliegt Dieses Verfahren ist insbesondere deshalb vorteilhaft, da hier der Patient keinerlei Handlungen vornehmen muss, um seine elektronische Gesundheitskarte zu benutzen. Dennoch ist ein Missbrauch der elektronischen Gesundheitskarte nahezu ausgeschlossen.

[0031] Die Verwendung der elektronischen Gesundheitskarte ohne jedwede Interaktion ihres Besitzers hat noch weitere Vorteile. Beispielsweise können wie oben erwähnt auf der Gesundheitskarte Notfalldaten, wie z. B. Adressdaten, nächster Angehöriger, Blutgruppe, eingenommene Medikamente usw. gespeichert sein. In einem Notfall ist es damit möglich, dass in einem Krankenwagen bei Eintreffen am Unfallort automatisch auf einem Display Informationen zum Patienten angezeigt werden, ohne dass es eines zeitaufwendigen Durchsuchens des Patienten nach einer entsprechenden Patientenkarte bedarf. Hier können wertvolle Sekunden gewonnen werden, wobei sich zusätzlich durch die Anzeige des Gesichtsbildes des Patienten der behandelnde Arzt sicher sein kann, am Unfallort über z. B. die richtige Blutgruppe genau dieses Patienten informiert worden zu sein.

[0032] Ein weiterer Anwendungsbereich ist beispielsweise auch die erweiterte Verwendung der elektronischen Gesundheitskarte innerhalb von Krankenhäusern: Beispielsweise können innerhalb ei-

nes Krankenhauses geplante Untersuchungsverfahren für einen Patienten direkt mit dessen elektronischer Gesundheitskarte verknüpft werden. Wenn also beispielsweise ein Patient zunächst in einer Abteilung geröntgt werden soll, genügt es, wenn der Patient lediglich die Gesundheitskarte ständig bei sich trägt Sobald der Patient im Röntgenbereich erscheint, wird das entsprechende Lichtbild des Patienten auf einem Bildschirm des Bedienpersonals eingeblendet, so dass dieses nach entsprechender Bestätigung direkten Zugriff auf die Krankenakte des Patienten hat. Fehlerhafte, doppelte oder unnötige Untersuchungen werden damit weitestgehend vermieden, da das Bedienpersonal z. B. der Röntgenabteilung aufgrund der vollständig vorliegenden Akte und damit auch der entsprechenden ärztlichen Untersuchungsverordnungen nach Sichtprüfung des Patienten lediglich die Untersuchungen vornehmen wird, welche auch mit der Gesundheitskarte verknüpft in der Krankenakte des Patienten vermerkt sind. Dieses Verfahren lässt sich sogar dahingehend ausdehnen, dass entsprechende ärztliche Eingriffe bis hin zu aufwendigen Operationen mit der elektronischen Gesundheitskarte verknüpft sind: Wird ein Patient für eine Operation vorbereitet und trägt er dabei die elektronische Gesundheitskarte bei sich, ist es behandelnden Ärzten ohne großen Aufwand möglich, festzustellen, ob das vorbereitete Operationsverfahren auch für den gegenwärtig behandelten Patienten vorgesehen ist Damit entfällt das Risiko einer Patientenverwechslung aufgrund der Möglichkeit der Sichtprüfung nahezu vollständig.

[0033] Nach einer weiteren Ausführungsform der Erfindung umfasst das Kommunikationsverfahren ferner den Schritt des Authentifizierens des Benutzers der elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst, wobei nach erfolgter Zertifikatsüberprüfung die Schritte des Sendens einer Benutzer-Identifikation von der Gesundheitskarte an das Lesegerät und dem Empfang einer Benutzereingabe am Lesegerät ausgeführt werden, wobei der Benutzer der elektronischen Gesundheitskarte erfolgreich authentifiziert ist, wenn die Benutzer-Identifikation mit der Benutzereingabe übereinstimmt. In anderen Worten bedarf es hier eine Interaktion eines Benutzers, das heißt eines Patienten, um einen Zugriff auf die elektronische Gesundheitskarte zu ermöglichen bzw. zu erlauben. Bei der Benutzer-Identifikation kann es sich wiederum um eine PIN, eine Buchstabenkombination oder auch um ein beliebiges biometrisches Merkmal handeln. Dadurch, dass die Benutzer-Identifikation mit der Benutzereingabe direkt am Lesegerät verglichen wird, ist gewährleistet, dass eine elektronische Gesundheitskarte nicht so manipuliert werden kann, dass ein entsprechendes Lesegerät getäuscht wird und der Meinung ist, ihm liege eine zur Kommunikation autorisierte elektronische Gesundheitskarte vor, die auch dem aktuellen Besitzer der Gesundheitskarte gehört.

[0034] Nach einer weiteren Ausführungsform der Erfindung umfasst das Kommunikationsverfahren ferner den Schritt des Anmeldens der elektronischen Gesundheitskarte an dem Lesegerät, wobei beim Anmelden eine Kennung optisch von der elektronischen Gesundheitskarte durch das Lesegerät gelesen und ein Challenge-Response-Verfahren zwischen der elektronischen Gesundheitskarte und dem Lesegerät durchgeführt wird, wobei für eine Verschlüsselung beim Challenge-Response-Verfahren eine Verschlüsselung unter Verwendung der Kennung erfolgt.

[0035] Dies hat den Vorteil, dass ein Besitzer der elektronischen Gesundheitskarte in der Lage ist zu bestimmen, wann eine Kommunikation zum Auslesen von Daten aus der elektronischen Gesundheitskarte stattfindet: Eine solche Kommunikation findet nämlich nur dann statt, wenn der Besitzer der Gesundheitskarte aktiv die Gesundheitskarte beispielsweise vor einen entsprechenden Scanner hält. Die Kennung, welche zur Verschlüsselung beim Challenge-Response-Verfahren verwendet wird, kann ein beliebiger personalisierter maschinenlesbarer Code sein. Dabei kann die Kennung beispielsweise selbst direkt als Schlüssel dienen. Möglich ist jedoch auch, unter Verwendung von entsprechenden Algorithmen aus der Kennung einen entsprechenden symmetrischen oder auch asymmetrischen Schlüssel zu erzeugen, unter dessen Verwendung das Challenge-Response-Verfahren abläuft.

[0036] Nach einer Ausführungsform der Erfindung handelt es sich bei der Kennung um einen öffentlichen Gesundheitskartenschlüssel, wobei ferner in der elektronischen Gesundheitskarte selbst ein privater Gesundheitskartenschlüssel elektronisch gespeichert ist, wobei der öffentliche und der private Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden. Beispielsweise kann der öffentliche Gesundheitskartenschlüssel in Form eines zweidimensionalen Strichcodes auf der Gesundheitskarte selbst aufgedruckt sein. Dies stellt keinerlei Sicherheitsrisiko dar, da der öffentliche Gesundheitskartenschlüssel ohnehin öffentlich zugänglich ist und keinerlei Rückschlüsse auf die Identität des Patienten erlaubt.

[0037] Um die Sicherheit bei der Verwendung des Challenge-Response-Verfahrens weiter zu erhöhen, umfasst das Challenge-Response-Verfahren nach einer weiteren Ausführungsform der Erfindung ferner den Schritt des Empfangs eines Autorisierungsschlüssels am Lesegerät, der Erzeugung eines Sitzungsschlüssels anhand der Kennung und des Autorisierungsschlüssels am Lesegerät und der Durchführung des Challenge-Response-Verfahrens unter Verwendung des Sitzungsschlüssels, wobei der Sitzungsschlüssel ferner auf der elektronischen Gesundheitskarte gespeichert ist Beispielsweise kann

es sich bei dem Autorisierungsschlüssel um einen Masterkey handeln, weicher auf einem Heilberufsausweis eines Gesundheitsdienstleisters abgespeichert ist. Somit genügt es nicht, lediglich im Besitz eines entsprechenden Lesegeräts zu sein, sondern zur Bedienung des Lesegeräts zum Zugriff auf die elektronische Patientenkarte wird zusätzlich noch der Autorisierungsschlüssel des Heilberufsausweises benötigt. Der Autorisierungsschlüssel des Heilberufsausweises ist dabei ein geheimer Schlüssel, welcher im Rahmen der Personalisierung der elektronischen Gesundheitskarte zusammen mit der Kennung der elektronischen Gesundheitskarte dazu verwendet wurde, um einen Sitzungsschlüssel zu erzeugen, welcher in einem gesicherten Speicherbereich der elektronischen Gesundheitskarte abgelegt wurde. Je nach verwendetem Algorithmus ist es hier möglich, symmetrische oder asymmetrische Schlüsselpaare zu verwenden.

[0038] In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung der Verfahrensschritte des erfindungsgemäßen Kommunikationsverfahrens.

[0039] In einem weiteren Aspekt betrifft die Erfindung eine elektronische Gesundheitskarte, wobei die Gesundheitskarte eine Nahfeld-Funkschnittstelle aufweist und zur Nahfeld-Kommunikation über eine Kommunikationsverbindung mit einem Lesegerät ausgebildet ist. Dabei handelt es sich vorzugsweise bei der Funkschnittstelle um einen RFID-Transponder.

[0040] Nach einer Ausführungsform der Erfindung handelt es sich bei der erfindungsgemäßen elektronischen Gesundheitskarte um eine Chipkarte. Alternativ ist es auch wie oben erwähnt möglich, die als RFID-Chip ausgebildete elektronische Gesundheitskarte in Form von Klebefolien bzw. Dünnschichtfolien auszubilden, so dass es einem Patienten überlassen ist, auf welches Trägermedium er die elektronische Gesundheitskarte aufzubringen gedenkt.

[0041] In einem weiteren Aspekt betrifft die Erfindung ein Lesegerät, wobei das Lesegerät eine Nahfeld-Funkschnittstelle aufweist und zur Nahfeldkommunikation über eine Kommunikationsverbindung mit einer elektronischen Gesundheitskarte ausgebildet ist. Auch hier handelt es sich vorzugsweise bei der Funkschnittstelle um eine RFID-Sende-/Empfangseinheit.

[0042] Nach einer Ausführungsform der Erfindung handelt es sich bei dem Lesegerät um einen Konnektor. Ein Konnektor ist dazu ausgebildet, um die Kommunikation zwischen elektronischer Gesundheitskarte, Arzt- oder Apotheken-Informationssystem und Telematik-Infrastruktur, wie z. B. einem Rezept-Server herzustellen.

[0043] Im Folgenden werden Ausführungsformen der Erfindung anhand der Zeichnungen näher erläutert. Es zeigen:

Fig. 1: ein Blockdiagramm eines Datenverarbeitungssystems zur kontaktlosen Kommunikation zwischen einer elektronischen Gesundheitskarte und einem Lesegerät.;

Fig. 2: ein Flussdiagramm verschiedener Ausführungsformen von Kommunikationsverfahren zwischen einer elektronischen Gesundheitskarte und einem Lesegerät;

Fig. 3: ein weiteres Flussdiagramm zur Authentifizierung eines Benutzers einer elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst;

Fig. 4: ein Flussdiagramm eines Anmeldeverfahrens einer elektronischen Gesundheitskarte an einem Lesegerät;

Fig. 5: ein weiteres Flussdiagramm zur Authentifizierung eines Benutzers einer elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst.

[0044] Die **Fig. 1** zeigt ein Blockdiagramm eines Datenverarbeitungssystems **100** zur kontaktlosen Kommunikation zwischen einer elektronischen Gesundheitskarte **122** und einem Lesegerät **110**. Dabei ist das Lesegerät **110** an das Datenverarbeitungssystem **100** angekoppelt Beispielsweise kommuniziert das Datenverarbeitungssystem **100** über seine Schnittstelle **106** mit dem Kartenlesegerät **110**. Das Kartenlesegerät **110** kann alternativ über einenso genannten Konnektor an das Datenverarbeitungssystem **100** angeschlossen werden. In diesem Fall ist der sog. Konnektor üblicherweise über das Netzwerk **116** mit dem Datenverarbeitungssystem **100** verbunden.

[0045] Teile des Datenverarbeitungssystems **100** können auch in dem Lesegerät **110** integriert sein, oder das Lesegerät kann Bestandteil des Datenverarbeitungssystems selbst sein.

[0046] Das Datenverarbeitungssystem **100** weist Eingabemittel **152**, wie z. B. eine Tastatur, eine Maus usw. auf. Des weiteren umfasst das Datenverarbeitungssystem **100** einen Speicher **102** und einen Prozessor **104**. Im Speicher **102** befinden sich beliebige Daten **112**, sowie Programmodule **114**.

[0047] Der Prozessor **104** dient zur Ausführung der Programm-Module **114**. Des weiteren umfasst das Datenverarbeitungssystem **100** Ausgabemittel in Form beispielsweise, eines Bildschirms **108**.

[0048] Das Datenverarbeitungssystem **100** ist des weiteren über ein Netzwerk **116**, wie z. B. das Internet, mit einer externen Datenbank **118** sowie einem Trust-Sender **120** verbunden. Die Datenbank **118** ist z. B. ein zentraler Rezeptdaten-Server. Alternativ kann die Datenbank **118** auch eine Patientenakten-Datenbank umfassen, wenn das Datenverarbeitungssystem **100** Teil eines Arzt-Informationssystems, beispielsweise in einem Krankenhaus ist.

[0049] Das Kartenlesegerät **110** kommuniziert drahtlos mit der RFID-Chipkarte **122**, welche als elektronische Gesundheitskarte ausgebildet ist. Zu diesem Zweck verfügt die Chipkarte **122** über eine Schnittstelle **128**, z. B. in Form eines RFID-Transponders. Ferner verfügt die RFID-Chipkarte **122** über einen Prozessor **126** und einen speicher 124. In dem Speicher **124** sind unter anderem Programm-Module **130** enthalten, welche durch den Prozessor **126** ausgeführt werden können. Des weiteren weist der Speicher einen geschützten Speicherbereich auf; in welchem sich ein privater Gesundheitskartenschlüssel **134** und ein Sitzungsschlüssel **132** gespeichert befinden.

[0050] An das Datenverarbeitungssystem **100** ist außerdem noch einen optischer Scanner **134** angeschlossen, mittels welchem eine auf der RFID-Chipkarte **122** aufgedruckte Kennung **136**, z.B. in Form eines Barcodes gescannt werden kann.

[0051] Im Folgenden sei die grobe Funktionsweise eines Kommunikationsverfahrens zwischen der elektronischen Gesundheitskarte **122** und dem Datenverarbeitungssystem **100** beziehungsweise dessen Lesegerät **110** skizziert. Nach einer Ausführungsform der Erfindung erfolgt nach Aktivierung des Transponders der RFID-Chipkarte **122** mittels Sendespulen des Lesegeräts **110** eine Authentifikation des Nutzers der elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst. Dies ist wie oben bereits erwähnt, hilfreich, um ein unbefugtes Benutzen der elektronischen Gesundheitskarte z. B. im Falle eines Diebstahls oder Verlustes zu verhindern. Hierzu wird beispielsweise ein sicherer Kommunikationskanal zwischen der RFID-Chipkarte **122** und dem Lesegerät **110** aufgebaut. Ein Benutzer der RFID-Chipkarte gibt mit Hilfe der Eingabemittel **152** eine Benutzerkennung am Datenverarbeitungssystem **100** ein. Diese Benutzerkennung wird daraufhin mit den öffentlichen Gesundheitskartenschlüssel der Gesundheitskarte in Form der RFID-Chipkarte **122** verschlüsselt. Der öffentliche Gesundheitskartenschlüssel kann dabei beispielsweise aus der Datenbank **118** über das Netzwerk **116** durch das Datenverarbeitungssystem **100** abgerufen werden. Alternativ ist es möglich, den öffentlichen Gesundheitskartenschlüssel aus dem Speicher **124** der Chipkarte **122** auszulesen.

[0052] Die Verschlüsselung der Benutzerkennung erfolgt mittels eines Verschlüsselungsalgorithmus, welcher z. B. in Form eines Programm-Moduls **114** implementiert ist. Im Falle des Einsatzes eines sog. Konnektors erfolgt die Verschlüsselung und Entschlüsselung im Konnektor. Nach Verschlüsselung wird die verschlüsselte Benutzerkennung durch das Lesegerät **110** an die Chipkarte **122** übertragen. Dort wird mit einem entsprechenden Entschlüsselungsprogramm, welches beispielsweise als Programm-Modul **130** implementiert sein kann, eine Entschlüsselung vorgenommen unter Verwendung des privaten Gesundheitskartenschlüssels **134**. In diesem Fall bilden der private und öffentliche Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar. Die RFID-Chipkarte **122** beziehungsweise das entsprechende Programm-Modul **130** wird eine weitere Kommunikation mit dem Lesegerät **110** nur dann freigeben, wenn die durch die Chipkarte entschlüsselte Benutzerkennung einer entsprechenden Benutzerkennung entspricht, welche auf der RFID-Chipkarte in einem nichtauslesbaren Speicherbereich abgelegt ist. So ist gewährleistet, dass ein unbefugter Zugriff auf die RFID-Chipkarte wirkungsvoll verhindert wird.

[0053] Anstatt der Verwendung beispielsweise einer PIN zur Benutzer-Identifikation ist es auch möglich, biometrische Merkmale mittels der Eingabemittel **152** aufzunehmen. In diesem Fall handelt es sich bei den Eingabemitteln **132** um einen biometrischen Scanner, wie z. B. einem Fingerabdruck-Scanner. Im Falle der Aufnahme zum Beispiel eines Fingerabdrucks wird dieser nach dem Scan digitalisiert, wie obig beschriebenen verschlüsselt und an die RFID-Chipkarte zur Verifizierung übertragen. Allerdings findet hier vorzugsweise wie ebenfalls obig beschrieben eine Reduktion der zu übertragenden Biometriedaten statt, da typischerweise die Speicher- und Prozessorkapazität einer RFID-Chipkarte begrenzt ist.

[0054] Nach einer weiteren Ausführungsform der Erfindung kann eine Kommunikation zwischen Datenverarbeitungssystem **100** und Chipkarte **122** auch in einer alternativen Art und Weise erfolgen; Hierzu ist beispielsweise auf der RFID-Chipkarte **122** eine Kennung **136** aufgedruckt. Mittels des optischen Scanners **134** wird nun das Datenverarbeitungssystem **100** die Kennung **136** erfassen. Beispielsweise handelt es sich bei der Kennung **136** um einen zweidimensionalen Barcode, so dass hier eine hohe Informationsdichte gewährleistet ist. Zum Zwecke des Scannens führt, nun ein Besitzer der Chipkarte **122** diese mit der Kennung zum Scanner **134**. Aus der gescannten Kennung **136** generiert nun ein Programm-Modul **114** unter Verwendung entsprechender Algorithmen einen Sitzungsschlüssel. Dieser Sitzungsschlüssel kann entweder die Kennung **136** selbst sein, wobei es sich in diesem Fall anbietet, als Kennung **136** den öffentlichen Gesundheitskartenschlüs-

sel der RFID-Chipkarte, 122 zu verwenden. In diesem Fall ist eine Kommunikation zum Abruf des öffentlichen Gesundheitskartenschlüssels über das Netzwerk **116** mit der Datenbank **118** bzw. durch die Luftschnittstelle mit der Chipkarte **122** nicht notwendig.

[0055] Unter Verwendung eines Challenge-Response-Verfahrens können nun das Datenverarbeitungssystem **100** und die RFID-Chipkarte **122** mittels des Sitzungsschlüssels eine Authentifizierungsprüfung durchführen. Anschaulich bedeutet dies zum Beispiel, dass die elektronische Gesundheitskarte eine Zufallskennung, z. B. eine Zufallszahl, erzeugt. Die Zufallskennung wird im Klartext an das Datenverarbeitungssystem **100** übermittelt. Daraufhin verschlüsselt das Datenverarbeitungssystem diese Zufallskennung mit dem zuvor unter Verwendung der Kennung **136** erzeugten Sitzungsschlüssels. Vorzugsweise geht in die Erzeugung des Sitzungsschlüssels ferner noch ein Autorisierungsschlüssel ein, welcher beispielsweise mittels des Kartenlesegeräts **110** von einem Heilberufsausweis empfangen wurde. Bevorzugterweise wird jedoch die gescannte Kennung an den Heilberufsausweis gesendet, welcher nun in der Lage ist, unter Verwendung des Autorisierungsschlüssels den Sitzungsschlüssel zu erzeugen.

[0056] Nach Verschlüsselung der empfangenen Zufallszahl mit dem Sitzungsschlüssel wird die verschlüsselte Zufallszahl an die RFID-Chipkarte **122** zurückübermitteit. Da auch die RFID-Chipkarte **122** in deren Speicher **124** den Sitzungsschlüssel **132** gespeichert hat, kann nun die RFID-Chipkarte die empfangene verschlüsselte Zufallszahl wiederum entschlüsseln. Gelingt dies, ist verifiziert, dass das Datenverarbeitungssystem **100** zuvor die Kennung **136** zur Erzeugung des Sitzungsschlüssels **132** gescannt hat Damit ist klar, dass eine Kommunikation zwischen Chipkarte **122** und Datenverarbeitungssystem **100** mit Willen des Besitzers der Chipkarte **122** zustande gekommen ist, da dieser selbst die Chipkarte zum Scannen der Kennung **136** bereitgestellt hat.

[0057] Es sei hier darauf hingewiesen, dass es sich bei dem Sitzungsschlüssel **132** nicht notwendigerweise um einen symmetrischen Schlüssel handeln muss. Hier können auch asymmetrische kryptografische Schlüsselpaare zum Einsatz kommen.

[0058] Nach einer weiteren Ausführungsform der Erfindung bildet eine weitere Sicherheitsstufe für eine Kommunikation zwischen dem Datenverarbeitungssystem **100** und der RFID-Chipkarte die Verwendung von Zertifikaten. Beispielsweise enthält das Datenverarbeitungssystem **100** ein Zertifikat **138**, welches das Datenverarbeitungssystem als vertrauenswürdig auszeichnet. In der Regel liegt das Zertifikat im Kartenleser, da auch dieser eine kryptografische Identität besitzt. Bei Verwendung eines Konnektors hat dieser in jedem Fall ein Zertifikat. Beispielsweise wird für eine Kommunikation zwischen dem Datenverarbeitungssystem **100** und der Chipkarte **122** das Zertifikat **138** vom Datenverarbeitungssystem **100** an die Chipkarte **122** übertragen. Mittels des Programm-Moduls **130** erfolgt nun eine Überprüfung des Zertifikats **138**. Dies kann entweder durch Kommunikation mit dem Trust-Center **120** erfolgen, oder aber unter Verwendung entsprechender Root-Schlüssel und Zertifikate, welche selbst im Speicher **134** in einem nicht auslesbaren und gesicherten Speicherbereich abgelegt sind. Nach erfolgreichem Überprüfen und Bestätigen des Zertifikats **138** erfolgt eine weitere Kommunikation zwischen dem Datenverarbeitungssystem **100** und der Chipkarte **122**. Wie ebenfalls oben erwähnt, kann beispielsweise das Zertifikat bestimmte Zugriffsberechtigungen auf Daten, welche im Speicher **124** abgelegt sind, enthalten.

[0059] Dies umfasst beispielsweise eine weitere Sicherheitsstufe, indem nach erfolgreicher Zertifikatsüberprüfung Bilddaten **140** von der Chipkarte **122** an das Datenverarbeitungssystem **100** übertragen werden. Diese Bilddaten enthalten zum Beispiel ein Gesichtsbild des Eigentümers der Chipkarte **122**. Nach Empfang der Bilddaten **140** durch das Datenverarbeitungssystem **100** werden die Bilddaten am Bildschirm **108** visualisiert. Dies ermöglicht einem Betrachter des Bildschirms **108**, z. B. einem Apotheker oder einem Arzt eine Sichtprüfung, ob der Besitzer der RFID-Chipkarte **122** auch tatsächlich deren Eigentümer entspricht.

[0060] In einer noch weiteren Sicherheitsstufe gibt es alternativ auch die Möglichkeit, nach erfolgreicher Zertifikatsüberprüfung eine entsprechende Kennung an das Datenverarbeitungssystem **100** zu übertragen. Dies erfordert innerhalb des Datenverarbeitungssystems **100** eine hohe Absicherung, so dass ein unbefugtes Ausspähen oder Auslesen der übertragenen Kennung durch Unbefugte verhindert wird. Nachdem diese Kennung an das Datenverarbeitungssystem **100** übertragen wurde, kann nun mittels der Eingabemittel **152** am Datenverarbeitungssystem eine Benutzerkennung eingegeben werden. Dies kann beispielsweise wiederum in Form einer PIN oder auch eines Fingerabdruck-Scans oder allgemein eigenes Scans eines biometrischen Merkmals erfolgen. Stimmt die an das Datenverarbeitungssystem übertragene Kennung mit der eingegebenen Benutzerkennung überein, so weiß das Dätenverarbeitungssystem **100**, dass der Benutzer der RFID-Chipkarte auch deren Eigentümer ist. Diese Funktionalität kann auch in dem sog. Konnektor, an dem der PC z.B. des Apothekers angeschlossen ist, realisiert sein.

[0061] Die **Fig. 2** zeigtein Flussdiagramm verschiedener Ausführungsformen von Kommunikätionsverfahren zwischen einer elektronischen Gesundheits-

karte und einem Lesegerät. Nach dem Aufbau eines Kommunikationskanals in Schritt 200 zwischen der Gesundheitskarte und dem Lesegerät gibt es verschiedene Prüfschritte, mit welchen verifiziert wird, dass zum einen das Lesegerät für einen Zugriff auf die Gesundheitskarte autorisiert ist und zum anderen der Träger der Gesundheitskarte auch zu deren Benutzung berechtigt ist.

[0062] In einer ersten Alternative erfolgt nach Schritt 200 der Schritt 202 mit dem Authentifizieren des Nutzers der elektronischen Gesundheitskarte gegenüber der elektronisehen Gesundheitskarte selbst Dieses Authentifizieren des Schritts 202 umfasst die Eingabe einer Benutzer-Identifikation am Lesegerät, das Verschlüsseln dieser Benutzer-Identifikation und das Senden der verschlüsselten Benutzer-Identifikation an die Gesundheitskarte, wo eine Verifikation der Benutzer-Identifikation stattfindet. Nach erfolgreicher Authentifizierung erfolgt schließlich im Schritt 204 der Datenaustausch zwischen den Lesegerät und der Gesundheitskarte. Weitere Details bezüglich des Schrittes 202 sind in der **Fig. 3** erläutert.

[0063] Eine Alternative zur Durchführung des Schrittes 202 in der **Fig. 2** bietet sich in der Durchführung des Schritts 206, des Schritts 206, dem Anmelden der elektronischen Gesundheitskarte am Lesegerät. Dieses Anmelden kann beispielsweise unter Verwendung einer optisch lesbaren Kennung erfolgen, welche auf der elektronischen Gesundheitskarte aufgedruckt ist. Diese aufgedruckte optische Kennung kann vom Lesegerät gelesen werden und als Basis für einen Schlüssel für ein Challenge-Response-Verfahren zwischen der Gesundheitskarte und dem Lesegerät verwendet werden. Da dies das aktive Beteiligen des Nutzers der elektronischen Gesundheitskarte fordert, ist sichergestellt, dass ein unbemerkter drahtloser Funkzugriff auf die Gesundheitskarte ausgeschlossen ist, da in diesem Fall aufgrund der dem Lesegerät unbekannten optisch lesbaren Kennung das Challenge-Response-Verfahren fehlschlagen würde. Weitere Details zur Durchführung des Schrittes 206 finden sich in der **Fig. 4**.

[0064] Nach erfolgreicher Durchführung des Schrittes 206 bietet sich die Möglichkeit, direkt mit Schritt 204, dem Datenaustausch zwischen Gesundheitskarte und Lesegerät fortzufahren. Dies könnte beispielsweise dann sinnvoll sein, wenn ein Träger der Gesundheitskarte aufgrund der gegebenen Umstände davon ausgehen kann, dass mit höchster Wahrscheinlichkeit das Lesegerät ein vertrauenswürdiges Lesegerät ist. Dies wird zum Beispiel innerhalb einer Apotheke oder einer Arztpraxis der Fall sein. Ein Patient wird hier unter normalen Umständen nicht die Vertrauenswürdigkeit eines entsprechenden Lesegeräts in Frage stellen, so dass hierfür weitere Authentifizierungsüberprüfungen bezüglich der Zugriffsberechtigung des Lesegeräts auf die Gesundheitskarte unnötig sind.

[0065] In einer weiteren Alternative gibt es entweder nach Durchführung des Schrittes 206 mit den Anmelden der Gesundheitskarte am Lesegerät oder direkt nach Schritt 200 ohne Verwendung des Schrittes 206 die Möglichkeit einer Zertifikatsüberprüfung in Schritt 208. Bei dieser Zertifikatsüberprüfung handelt es sich um eine Überprüfung des Zertifikates des Lesegeräts, so dass in einem automatischen Prüfverfahren ohne jedwede Interaktion des Trägers der Gesundheitskarte durch die Gesundheitskarte selbst festgestellt werden kann, ob das zugreifende Lesegerät vertrauenswürdig ist und ob demzufolge ein weiterer Zugriff des Lesegeräts auf die Gesundheitskarte erlaubt werden soll. Die Zertifikatsüberprüfung in Schritt 208 umfasst dabei die Schritte des Empfangs eines digitalen Zertifikats des Lesegeräts durch die elektronische Gesundheitskarte und der Überprüfung des Zertifikats durch elektronische Gesundheitskarte. Vorzugsweise kommt hier als Zertifikat ein so genanntes „Card-Verifiable-Certificate (CVC)“ zur Anwendung. Zur Prüfung der Signatur eines CVCs muss ein in der Gesundheitskarte eingetragener öffentlicher Schlüssel einer Zertifizierungsinstanz benutzt werden. Alternativ bietet sich jedoch auch die Möglichkeit, dass die Gesundheitskarte über das Lesegerät auf einen Trust-Center zugreift, um unter Verwendung dessen eine Zertifikatsüberprüfung durchzuführen.

[0066] Ist die Zertifikatsüberprüfung in Schritt 210 erfolgreich, erfolgt eine Freigabe der Übertragung von Daten von der elektronischen Gesundheitskarte an das Lesegerät. Dabei sind die zur Übertragung vorgesehenen Daten durch die im Zertifikat spezifizierten Zugriffsberechtigungen bestimmt. Beispielsweise kann nach erfolgreicher Zertifikatüberprüfung in Schritt 210 eine Sichtprüfung in Schritt 214 erfolgen. Die Sichtprüfung im Schritt 214 erfordert, dass ein Gesichtsbild des Inhabers der Gesundheitskarte in der Gesundheitskarte selbst in Form von Bilddaten gespeichert ist. Im Falle dessen, dass das Zertifikat eine Zugriffsberechtigung auf Bilddaten des Inhabers der Gesundheitskarte aufweist, werden in Schnitt 214 die in der Gesundheitskarte gespeicherten Bilddaten von der Gesundheitskarte an das Lesegerät gesendet. Daraufhin wird das in den Bilddaten enthaltene Bild visuell am Lesegerät oder an einem an dem Lesegerät angeschlossenen Datenverarbeitungssystem angezeigt. Dies ermöglicht einem Gesundheitsdienstleister visuell zu erkennen und zu entscheiden, ob der gegenwärtige Besitzer der Gesundheitskarte auch deren rechtmäßiger Eigentümer ist. Ist dies der Fall, kann nach Schritt 214 ein Datenaustausch mit Schritt 204 stattfinden.

[0067] Alternativ zur Durchführung der Sicht der Sichtprüfung in Schritt 214 kann nach erfolgreicher Zertifikatsüberprüfung in Schritt 210 auch eine Be-

nutzer-Authentifikation mit Schritt 216 durchgeführt werden. In diesem Fall enthält das Zertifikat eine Zugriffsberechtigung zum Lesen einer Benutzer-Identifikation von der Gesundheitskarte. Diese Benutzer-Identifikation der Gesundheitskarte kann daraufhin mit einer Benutzereingabe am Lesegerät verglichen werden, womit das Lesegerät dazu in der Lage ist zu entscheiden, ob der gegenwärtige Benutzer der Gesundheitskarte auch zu deren Benutzung autorisiert ist Nach erfolgreicher Benutzer-Authentisierung in Schritt 216 erfolgt wiederum in Schritt 204 der Datenaustausch zwischen Gesundheitskarte und Lesegerät.

[0068] Ist die Zertifikatsüberprüfung Schritts 210 nicht erfolgreich, erfolgt seitens der Gesundheitskarte ein Abbruch der Kommunikation zwischen Lesegerät und Gesundheitskarte. Da dieser Abbruch in Schritt 212 aufgrund der automatischen Zertifikatsüberprüfung ebenfalls vollautomatisch erfolgt, ist gewährleistet, dass im Falle des Durchführens der Schritte 200 und daraufhin folgend 208 ein „zufälliges Ausprobieren“ von verschiedenen Kennungen zur Authentifizierung eines unbefugten Benutzers gegenüber der Gesundheitskarte effektiv verhindert werden kann.

[0069] Eine weitere Sicherheitsstufe kann ferner dadurch erhalten werden, indem zum Beispiel die nach Überprüfung eines Zertifikat ein interner Countdown in Gang gesetzt werden kann, nach dessen Ablauf erst eine weitere Zertifikatüberprüfung stattfinden kann. So kann zum Beispiel die Gesundheitskarte dafür konfiguriert werden, nur alle 5 Sekunden eine Zertifikatsprüfung durchzuführen. Damit wird verhindert, dass unter Verwendung zum Beispiel von Brute-Force-Methoden Zertifikate „ausprobiert“ und „erraten“ werden. Diese Sperre von zum Beispiel 5 Sekunden wird im normalen Betrieb den Einsatz der Gesundheitskarte nicht beeinflussen, da hier davon ausgegangen werden muss, dass korrekt zertifizierte Lesegeräte vorliegen. In diesem Fall ist also eine wiederholte Zertifikatsüberprüfung überhaupt nicht notwendig.

[0070] Die **Fig. 3** zeigt ein weiteres Flussdiagramm zur Authentifizierung eines Benutzers einer elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst Die Schritte 300 bis 308 der **Fig. 3** entsprechen dabei wie bereits erwähnt, dem Schritt 202 in der **Fig. 2**, nämlich dem Authentifizieren des Nutzers der elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst. In Schritt 300 erfolgt das Lesen des öffentlichen Gesundheitskartenschlüssels der Gesundheitskarte durch das Lesegerät. Der öffentliche Gesundheitskartenschlüssel kann dabei entweder durch ein optisches Verfahren von der Oberfläche der Gesundheitskarte abgescannt und gelesen werden, er kann über Nahfeld-Funkübermittlung von der Gesundheitskarte ans Lesegerät übermittelt werden oder das Lesegerät kann den öffentlichen Gesundheitskartenschlüssel von einer externen Datenbank abfragen. Nach Durchführung des Schritts 300 wird der Benutzer am Lesegerät, beziehungsweise an dem Datenverarbeitungssystem, welches an ein Lesegerät angeschlossen ist, dazu aufgefordert, einige Benutzer-Identifikation für die elektronische Gesundheitskarte einzugeben. Diese Benutzer-Identifikation kann ein biometrisches Merkmal sein, sie kann eine PIN sein oder eine beliebige alphanumerische Zeichen-Buchstaben-Kombination.

[0071] Nach Eingabe der Benutzer-Identifikation in Schritt 302 wird die Benutzer-Identifikation in Schritt 34 mit dem öffentlichen Gesundheitskartenschlüssel durch das Lesegerät verschlüsselt. In Schritt 306 wird die verschlüsselte Benutzer-Identifikation an die elektronische Gesundheitskarte gesendet, welche diese in Schritt 308 entschlüsselt. Die Entschlüsselung erfolgt dabei mit dem privaten Gesundheitskartenschlüssel der Gesundheitskarte. Dies erfordert, dass der öffentliche und private Gesundheitskartenschlüssel der Gesundheitskarte ein asymmetrisches kryptografisches Schlüsselpaar bilden.

[0072] Es sei hier noch angemerkt, dass anstatt der Verwendung des öffentlichen und privaten Gesundheitskartenschlüssels zur verschlüsselten Kommunikation zwischen dem Lesegerät und der Gesundheitskarte auch beliebige andere sichere kryptografische Verfahren zur gesicherten Datenübertragung Verwendung finden können. Entscheidend ist, dass ein vertrauenswürdiger Kanal „Trusted Channel“ zwischen der Gesundheitskarte und dem Lesegerät hergestellt wird.

[0073] Die **Fig. 4** zeigt ein Flussdiagramm des Anmeldeverfahrens einer elektronischen Gesundheitskarte an einem Lesegerät. Dieses Anmeldeverfahren wird wie bereits oben erwähnt, unter Verwendung einer optisch lesbaren Kennung durchgeführt, welche auf der elektronischen Gesundheitskarte aufgedruckt ist. Die Verfahrensschritte 400 bis 424, welche in der **Fig. 4** veranschaulicht sind, entsprechen dabei im Verfahrensschritt 206 der **Fig. 2**.

[0074] In Schritt 400 erfolgt das Lesen der optischen Kennung durch das Lesegerät beziehungsweise durch einen entsprechenden Scanner, welcher mit dem Lesegerät verbunden ist. Wie bereits erwähnt, kann die Kennung in Form eines zweidimensionalen Strichcodes auf der Oberfläche der Gesundheitskarte aufgedruckt sein. Um hier die Fälschungssicherheit der elektronischen Gesundheitskarte weiter zu erhöhen, besteht auch die Möglichkeit, anstatt der Verwendung eines einfachen Schwarz-Weiß-Aufdruckes auf die Gesundheitskarte die Kennung unter Verwendung von speziellen pigmentierten Farbstoffen auf die Gesundheitskarte aufzubringen. Beispielswei-

se können fluoreszierende oder phosphoreszierende Farbstoffe zum Einsatz kommen. In diesem Fall kann die Kennung mit einer Lichtwellenlänge zum phosphoreszierenden Leuchten angeregt werden, wohingegen das Auslesen auf einer Lichtwellenlänge stattfindet, in deren Wellenlängenbereich die Kennung fluor- oder phosphoreszierendes Licht emittiert.

[0075] Nach dem Lesen der optischen Kennung in Schritt 400 erfolgt das Erzeugen einer Zufallskennung in Schritt 402. Diese Zufallskennung wird durch die elektronische Gesundheitskarte erzeugt. Nun bieten sich zwei unterschiedliche Möglichkeiten, wie das Verfahren fortgeführt werden kann. Die eine Möglichkeit bietet sich in der Durchführung der Schritte 404 bis 412 und darauffolgenden dem Schritt 414, die andere Möglichkeit bietet sich in der Durchführung der Schritte 416 bis 424 und darauffolgend der Durchführung des Schrittes 414.

[0076] Bei der Durchführung der Schritte 404 bis 412 wird die von der Gesundheitskarte in Schritt 402 erzeugte Zufallskennung an das Lesegerät gesendet. In Schritt 406 liest das Lesegerät einen speziellen Autorisierungsschlüssel, zum Beispiel einen Masterkey. Bei diesem Masterkey kann es sich z.B. um einen besonderen geheimen Schlüssel eines Heilberufsausweises handeln, womit sichergestellt ist, dass eine Anmeldung einer elektronischen Gesundheitskarte an einem Lesegerät nur dann erfolgreich sein kann, wenn das Lesegerät auch von einem autorisierten Benutzer, z.B. eines Arztes oder eines Apothekers, welcher im Besitz des Heilberufsausweises ist betrieben wird. Unter Verwendung des gelesenen Autorisierungsschlüssels, sowie der gelesenen Kennung, wird in Schritt 408 durch das Lesegerät ein Sitzungsschlüssel erzeugt. Daraufhin wird in Schritt 410 die Zufallskennung mit dem in Schritt 408 erzeugten Sitzungsschlüssel verschlüsselt und in Schritt 412 an die elektronische Gesundheitskarte übermittelt.

[0077] Da die elektronische Gesundheitskarte selbst über den Sitzungsschlüssel verfügt, welcher in einem gesicherten nichtauslesbaren Speicherbereich der Gesundheitskarte gespeichert ist, ist die Gesundheitskarte in Schritt 414 in der Lage, die Zufallskennung zu verifizieren, indem sie die verschlüsselte Zufallskennung wiederum entschlüsselt und den so erhaltenen Wert mit der zuvor erzeugten Zufallskennung vergleicht, welche an das Lesegerät übermittelt wurde. Die Verifikation ist erfolgreich, wenn die entschlüsselte Zufallskennung mit der erzeugten Zufallskennung übereinstimmt. Der Sitzungsschlüssel, welcher zur Verschlüsselung der Zufallskennung verwendet wird und ihr Sitzungsschlüssel, welcher in der Gesundheitskarte gespeichert ist müssen nicht notwendigerweise identisch sein. Dies ist nur dann notwendig, wenn ein symmetrischer Schlüssel zur Kryptographie verwendet wird. Im Falle eines asymmetrischen Schlüsselpaares sind der in Schritt 408 erzeugte Sitzungsschlüssel, sowie der in Schritt 414 zur Verifikation der Zufallskennung verwendete Schlüssel aufgrund deren Asymmetrie nicht identisch.

[0078] Alternativ zur Durchführung der Schritte 404 bis 412, sowie des Schritts 414 bietet sich wie obig erwähnt, auch die Durchführung der Schritte 416 bis 424, gefolgt von Schritt 414 an. Dies sei nun näher erläutert: Nachdem in Schritt 402 die Zufallskennung durch die Gesundheitskarte erzeugt wurde, wird in Schritt 416 diese Zufallskennung durch die Gesundheitskarte mit der in der Gesundheitskarte gespeicherten Sitzungsschlüssel verschlüsselt. Die verschlüsselte Zufallskennung wird daraufhin von der Gesundheitskarte in Schritt 418 an das Lesegerät übermittelt. In Schritt 420 erzeugt das Lesegerät selbst den Sitzungsschlüssel, wobei hier die optisch gelesene Kennung (Schritt 400) verwendet wird. Alternativ oder zusätzlich kann auch hier wiederum ein Autorisierungsschlüssel gelesen werden, welcher zusammen mit der gelesenen optischen Kennung zur Erzeugung des Sitzungsschlüssels in Schritt 420 dient. In Schritt 422 wird die verschlüsselte Zufallskennung mit dem Sitzungsschlüssel entschlüsselt und die entschlüsselte Zufallskennung wird daraufhin in Schritt 424 an die elektronische Gesundheitskarte zurückübermittelt. Nun kann in dem nachfolgenden Schritt 414 die Gesundheitskarte wiederum verifizieren, ob die empfangene Zufallskennung der in Schritt 402 erzeugten Zufallskennung entspricht, womit eine Verifikation gegeben ist.

[0079] Die **Fig. 5** zeigt ein weiteres Flussdiagramm zur Authentifizierung eines Benutzers einer elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte selbst. Die Durchführung der Schritte 500 bis 504 entspricht dabei dem Schritt 216 der **Fig. 2**. Wie in der **Fig. 2** erläutert, setzt die Durchführung der Schritte 500 bis 504 zunächst eine erfolgreiche Zertifikatsüberprüfung des Lesegeräts voraus. Der Grund liegt darin, dass die elektronische Gesundheitskarte in Schritt 500 an das Lesegerät eine Benutzer-Identifikation übermittelt. In anderen Worten bedeutet dies, dass hier ein eine eigentlich nur der Gesundheitskarte bekannte Information diese zum Zwecke einer Benutzer-Authentifikation verlässt. Dies erfordert zwingenderweise, dass eine Übermittlung einer solchen Benutzer-Identifikation nur an solche Lesegeräte erfolgt, von welchen sich der Benutzer der Gesundheitskarte bzw. die Gesundheitskarte selbst sicher sein kann, dass diese vertrauenswürdig sind. Im Gegenzug erfordert dies natürlich, dass eine Manipulation des Lesegeräts zuverlässig verhindert werden muss, so dass ein Auslesen der an das Lesegerät übertragenen Benutzer-Identifikation verhindert wird.

[0080] Nach Empfang Benutzer-Identifikation am Lesegerät in Schritt 500 erfolgt in Schritt 502 ein Empfang einer Benutzereingabe am Lesegerät. Diese Be-

nutzereingabe kann beispielsweise eine PIN, eine alphanumerische Zeichenkombination oder auch ein biometrisches Merkmal sein. Beispielsweise erfolgt in Schritt 502 ein Fingerabdruck-Scan des Benutzers der elektronischen Gesundheitskarte. Daraufhin wird in Schritt 504 die Benutzereingabe, das heißt zum Beispiel der gescannte Fingerabdruck mit der Benutzer-Identifikation verglichen, welche in Schritt 500 von der Gesundheitskarte selbst empfangen wurde. Stimmen beim Beispiel eines Fingerabdrucks der Fingerabdruck, welcher von der Gesundheitskarte an das Lesegerät übermittelt wurde, sowie der Fingerabdruck welcher vom Lesegerät in Form der Benutzereingabe empfangen wurde, überein, kann sich das Lesegerät sicher sein, dass der gegenwärtige Benutzer der Gesundheitskarte auch deren rechtmäßiger Eigentümer ist.

[0081] Die Verwendung von biometrischen Merkmalen in Zusammenhang mit einer Benutzer-Authentifikation im Rahmen der elektronischen Gesundheitskarte ist in besonderer Weise vorteilhaft: Hier entfällt vollständig die Notwendigkeit, dass sich ein Benutzer, der Eigentümer der elektronischen Gesundheitskarte, beispielsweise eine PIN, wie bei vielen anderen elektronischen Karten der Fall, merken muss. Trotz des Nichterfordernisses einer PIN ist eine höchste Sicherheit bezüglich eines unbefugten Auslesens von Daten aus der Gesundheitskarte gewährleistet. Die Nichterfordemis einer PIN ist insbesondere vor dem Hintergrund der typischen Verwendung von elektronischen Gesundheitskarten relevant: Ältere Menschen, welche aufgrund deren Krankheitsanfälligkeit häufig eine Gesundheitskarte benutzen, werden von der Problematik ausgenommen, dass diese sich eine PIN merken müssen, was insbesondere im fortgeschrittenen Alter oft aufgrund erhöhter Vergesslichkeit zu erheblichen Schwierigkeiten führt. Auch in Familien mit Kindern, wo üblicherweise jeder einzelne Krankenversicherte eine eigene Versichertenkarte, das heißt eine eigene elektronische Gesundheitskarte besitzt, entfällt die Notwendigkeit, dass beispielsweise eine erziehende Mutter für sich und deren Kinder mehrere verschiedene PINs merken muss. Hier ist durch die Verwendung von persönlichen, individuellen biometrischen Merkmalen eine flexible und hochsichere Verwendung der erfindungsgemäßen elektronischen Gesundheitskarte möglich.

[0082] Es sei hier noch angemerkt, dass verschiedene erwähnte Sicherheitsmechanismen zum Zwecke eines flexiblen Einsatzes der elektronischen Gesundheitskarte miteinander kombiniert werden können. Beispielsweise ist es denkbar, die Eingabe einer PIN wie beispielsweise in der **Fig. 2**, Schritt 202 beschrieben, in Verbindung mit einer Sichtprüfung, Schritt 214 zu kombinieren. Das heißt zur Kommunikation zwischen der elektronischen Gesundheitskarte und dem Lesegerät kommt entweder der Schritt 202 zum Einsatz, oder die Schritte 208, 210 und 214. Kommt der Schritt 202 zum Einsatz, das heißt die einfache PIN-Eingabe zum Authentifizieren eines Benutzers der Gesundheitskarte gegenüber der Gesundheitskarte selbst, so kann die Gesundheitskarte auch beispielsweise an Betreuungspersonen gegeben werden, welche mit Kenntnis der PIN, sowie mit Besitz der Gesundheitskarte in eine Apotheke gehen können, um für den Betreuten ein elektronisches Rezept einzulösen. Wird die Sichtprüfung mit der Authentifikation des Nutzers über eine Kennung, z. B. einer PIN kombiniert, würde in einer Apotheke zunächst ein Bild des Eigentümers der Gesundheitskarte auf einem Bildschirm des Apotheken-Informationssystems erscheinen. Der Apotheker erkennt daraufhin, dass das von der Gesundheitskarte übermittelte Gesichtsbild nicht mit dem Aussehen des aktuellen Verwenders der Gesundheitskarte übereinstimmt. Daraufhin kann ein Apothekenbediensteter den Benutzer der Gesundheitskarte zur alternativen Eingabe einer PIN auffordern, um sich gegenüber der Gesundheitskarte und gegebenenfalls auch dem Lesegerät zu authentifizieren.

Bezugszeichenliste

100	Datenverarbeitungssystem
102	Speicher
104	Prozessor
106	Schnittstelle
108	Bildschirm
110	Lesegerät
112	Daten
114	Programm
116	Netzwerk
118	Datenbank
120	Trust-Center
122	Chipkarte
124	Speicher
126	Prozessor
128	Schnittstelle
130	Programm
132	Sitzungsschlüssel
134	privater Gesundheitskartenschlüssel
136	Kennung
138	Zertifikat
140	Bilddaten
152	Eingabemittel

Patentansprüche

1. Kommunikationsverfahren einer elektronischen Gesundheitskarte (122) mit einem Lesegerät, wobei zwischen der elektronischen Gesundheitskarte (122) und dem Lesegerät (110) eine Kommunikationsverbindung aufgebaut wird, wobei es sich bei der Kommunikationsverbindung um eine Nahfeldverbindung handelt, wobei das Kommunikationsverfahren ferner den Schritt umfasst des Anmeldens der elektronischen Gesundheitskarte (122) an dem Lesegerät, wobei beim Anmelden die folgenden Schritte ausgeführt werden:
- optisches Lesen einer auf der elektronischen Gesundheitskarte (122) aufgedruckten Kennung (136) durch das Lesegerät,
- Durchführung eines Challenge-Response Verfahrens zwischen der elektronischen Gesundheitskarte (122) und dem Lesegerät, wobei für eine Verschlüsselung beim Challenge-Response Verfahren eine Verschlüsselung unter Verwendung der Kennung erfolgt, wobei es sich bei der Kennung um einen öffentlichen Gesundheitskartenschlüssel handelt, wobei ferner in der elektronischen Gesundheitskarte (122) ein privater Gesundheitskartenschlüssel elektronisch gespeichert ist, wobei der öffentliche und der private Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden.

2. Kommunikationsverfahren nach Anspruch 1, wobei die Kommunikationsverbindung durch ein RFID-Verfahren aufgebaut wird.

3. Kommunikationsverfahren nach einem der vorigen Ansprüche 1 oder 2, wobei es sich bei der Kommunikationsverbindung um eine sichere Kommunikationsverbindung handelt.

4. Kommunikationsverfahren nach einem der vorigen Ansprüche, ferner mit dem Schritt des Authentifizierens des Nutzers der elektronischen Gesundheitskarte (122) gegenüber der elektronischen Gesundheitskarte (122), mit den folgenden Schritten:
- Eingabe einer Benutzeridentifikation am Lesegerät,
- Übertragung einer Anforderung zur Fernüberprüfung der Benutzeridentifikation von dem Lesegerät an die elektronische Gesundheitskarte (122),
- Durchführung der Fernüberprüfung der Benutzeridentifikation durch die elektronische Gesundheitskarte (122).

5. Kommunikationsverfahren nach einem der vorigen Ansprüche 1 bis 3, ferner mit dem Schritt des Authentifizierens des Nutzers der elektronischen Gesundheitskarte (122) gegenüber der elektronischen Gesundheitskarte (122), wobei die folgenden Schritte ausgeführt werden:
- Eingabe einer Benutzeridentifikation am Lesegerät,
- Verschlüsseln der Benutzeridentifikation durch das Lesegerät (110) mit einem öffentlichen Gesundheitskartenschlüssel der Gesundheitskarte (122),
- Senden der verschlüsselten Benutzeridentifikation an die elektronische Gesundheitskarte (122),
- Entschlüsselung der empfangenen verschlüsselten Benutzeridentifikation durch die Gesundheitskarte (122), wobei die Entschlüsselung mittels eines privaten Gesundheitskartenschlüssels (134) erfolgt, wobei in der elektronischen Gesundheitskarte (122) der private Gesundheitskartenschlüssel elektronisch gespeichert ist, wobei der öffentliche und der private Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden, wobei das Anmelden erfolgreich ist, wenn die entschlüsselte Benutzeridentifikation durch die Gesundheitskarte (122) verifiziert wurde.

6. Kommunikationsverfahren nach Anspruch 5, wobei der öffentliche Gesundheitskartenschlüssel von der Gesundheitskarte (122) oder von einer externen Datenbank (118) abgerufen wird.

7. Kommunikationsverfahren nach einem der vorigen Ansprüche 1 bis 3, ferner mit dem Schritt des Authentifizierens des Lesegeräts gegenüber der elektronischen Gesundheitskarte (122), wobei nach erfolgreicher Authentifizierung eine Freigabe von Daten zur Datenübertragung von der Gesundheitskarte (122) an das Lesegerät (110) erfolgt, wobei die Daten auf der Gesundheitskarte (122) gespeichert sind.

8. Kommunikationsverfahren nach Anspruch 7, wobei das Authentifizieren die Schritte umfasst:
- Empfang eines digitalen Zertifikats (138) durch die elektronische Gesundheitskarte (122) von dem Lesegerät,
- Überprüfung des Zertifikats durch die elektronische Gesundheitskarte (122), wobei das Lesegerät (110) Authentifiziert ist, wenn die Zertifikatsüberprüfung erfolgreich ist,
- nach erfolgreicher Zertifikatsüberprüfung, Freigabe der Übertragung der Daten von der elektronischen Gesundheitskarte (122) an das Lesegerät, wobei die zur Übertragung vorgesehenen Daten durch die im Zertifikat spezifizierten Zugriffsberechtigungen bestimmt sind.

9. Kommunikationsverfahren nach Anspruch 8, wobei nach erfolgreicher Zertifikatsüberprüfung
- in der Gesundheitskarte (122) gespeicherte Bilddaten (140) von der Gesundheitskarte (122) an das Lesegerät (110) gesendet werden, wobei die Bilddaten zumindest ein Gesichtsbild des Inhabers der Gesundheitskarte (122) aufweisen, und
- das in den Bilddaten enthaltene Bild visuell am Lesegerät (110) oder an einem an dem Lesegerät (110) angeschlossenen Datenverarbeitungssystem angezeigt wird, um eine Sichtprüfung zu ermöglichen.

10. Kommunikationsverfahren nach Anspruch 8, ferner mit dem Schritt des Authentifizierens des Benutzers der elektronischen Gesundheitskarte (122) gegenüber der elektronischen Gesundheitskarte (122), wobei nach erfolgreicher Zertifikatsüberprüfung die folgenden Schritte ausgeführt werden:
- Senden einer Benutzeridentifikation von der Gesundheitskarte (122) an das Lesegerät,
- Empfang einer Benutzereingabe am Lesegerät, wobei der Benutzer der elektronischen Gesundheitskarte (122) erfolgreich authentifiziert ist, wenn die Benutzeridentifikation mit der Benutzereingabe übereinstimmt.

11. Kommunikationsverfahren nach einem der vorigen Ansprüche 4, 5 oder 10, wobei es sich bei der Benutzeridentifikation um ein biometrisches Merkmal handelt.

12. Kommunikationsverfahren nach Anspruch 1, wobei das Challenge-Response Verfahren ferner die folgenden Schritte umfasst:
- Empfang eines Autorisierungsschlüssels am Lesegerät (110),
- Erzeugung eines Sitzungsschlüssels (132) anhand der Kennung und des Autorisierungsschlüssels am Lesegerät,
- Durchführung des Challenge-Response Verfahrens unter Verwendung des Sitzungsschlüssels (132), wobei der Sitzungsschlüssel ferner auf der elektronischen Gesundheitskarte (122) gespeichert ist.

13. Kommunikationsverfahren nach einem der vorigen Ansprüche 1 oder 12, wobei die Kennung (136) als Strichcode kodiert auf der elektronischen Gesundheitskarte (122) aufgedruckt ist.

14. Elektronische Gesundheitskarte (122), wobei die Gesundheitskarte (122) eine Nahfeld-Funkschnittstelle (128) aufweist und zur Nahfeld-Kommunikation über eine Kommunikationsverbindung mit einem Lesegerät (110) ausgebildet ist, wobei die Gesundheitskarte ferner Mittel zum Anmelden der elektronischen Gesundheitskarte (122) an dem Lesegerät aufweist, wobei die Mittel zum Anmelden der elektronischen Gesundheitskarte (122) an dem Lesegerät (110) umfassen:
- eine optisch lesbare Kennung (136)
- Mittel zur Durchführung eines Challenge-Response Verfahrens zwischen der elektronischen Gesundheitskarte (122) und dem Lesegerät, wobei die Mittel zur Durchführung des Challenge-Response Verfahrens dazu ausgebildet sind, eine Verschlüsselung beim Challenge-Response Verfahren unter Verwendung der Kennung durchzuführen wobei es sich bei der Kennung um einen öffentlichen Gesundheitskartenschlüssel handelt, wobei ferner in der elektronischen Gesundheitskarte (122) ein privater Gesundheitskartenschlüssel elektronisch gespeichert ist, wobei der öffentliche und der private Gesundheitskartenschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden.

15. Elektronische Gesundheitskarte (122) nach Anspruch 14, wobei es sich bei der Funkschnittstelle um einen RFID-Transponder handelt.

16. Elektronische Gesundheitskarte (122) nach einem der vorigen Ansprüche 14 oder 15, ferner mit:
- Mitteln (128) zum Empfang einer Anforderung zur Fernüberprüfung einer Benutzeridentifikation von dem Lesegerät,
- Mittel (130) zur Durchführung der Fernüberprüfung der Benutzeridentifikation.

17. Elektronische Gesundheitskarte (122) nach einem der vorigen Ansprüche 14 oder 15, ferner mit:
- Mitteln (128) zum Empfang einer verschlüsselten Benutzeridentifikation von dem Lesegerät,
- Mittel (130) zur Entschlüsselung der empfangenen verschlüsselten Benutzeridentifikation mittels eines privaten Gesundheitskartenschlüssels (134), wobei in der elektronischen Gesundheitskarte (122) der private Gesundheitskartenschlüssel elektronisch gespeichert ist,
- Mittel (130) zur Verifizierung der Benutzeridentifikation, wobei ein Authentifizieren des Nutzers der elektronischen Gesundheitskarte (122) gegenüber der elektronischen Gesundheitskarte (122) erfolgreich ist, wenn die entschlüsselte Benutzeridentifikation verifiziert wurde.

18. Elektronische Gesundheitskarte (122) nach Anspruch 17, ferner mit Mitteln (128) zum Senden eines öffentlichen Gesundheitskartenschlüssels an das Lesegerät.

19. Elektronische Gesundheitskarte (122) nach einem der vorigen Ansprüche 14 oder 15, wobei Daten auf der Gesundheitskarte (122) gespeichert sind, wobei die Gesundheitskarte (122) ferner Mittel (130) aufweist zur Authentifizierung des Lesegeräts und Mittel (130) zur Freigabe von Daten zur Datenübertragung an das Lesegerät, wobei die Mittel zur Freigabe der Daten dazu ausgebildet sind, nach erfolgreicher Authentifizierung die Daten zur Datenübertragung freizugeben.

20. Elektronische Gesundheitskarte (122) nach Anspruch 19, wobei die Mittel zur Authentifizierung ferner aufweisen:
- Mittel zum Empfang eines digitalen Zertifikats (138) von dem Lesegerät (110),
- Mittel zur Überprüfung des Zertifikats,
- Mittel zur Freigabe der Übertragung der Daten an das Lesegerät, wobei die Mittel zur Freigabe der Übertragung dazu ausgebildet sind, nach erfolgreicher Zertifikatsüberprüfung die zur Übertragung vorgesehenen Daten mittels von im Zertifikat spezifizierten Zugriffsberechtigungen zur Übertragung freizu-

geben, wobei das Lesegerät (110) Authentifiziert ist, wenn die Zertifikatsüberprüfung erfolgreich ist.

21. Elektronische Gesundheitskarte (122) nach Anspruch 19 oder 20, mit gespeicherten Bilddaten (140), wobei die Bilddaten zumindest ein Gesichtsbild des Inhabers der Gesundheitskarte (122) aufweisen, und ferner mit Mitteln zum Senden der Bilddaten an das Lesegerät, wobei die Mitteln zum Senden der Bilddaten dazu ausgebildet sind, nach erfolgreicher Zertifikatüberprüfung die Bilddaten zu senden.

22. Elektronische Gesundheitskarte (122) nach Anspruch 20, ferner mit Mitteln (130) zum Authentifizieren des Benutzers der elektronischen Gesundheitskarte (122) gegenüber der elektronischen Gesundheitskarte (122), wobei die Mittel zum Authentifizieren des Benutzers der elektronischen Gesundheitskarte (122) dazu ausgebildet sind, nach erfolgreicher Zertifikatsüberprüfung eine Benutzeridentifikation an das Lesegerät (110) zur Verifikation durch das Lesegerät (110) zu senden.

23. Elektronische Gesundheitskarte (122) nach einem der vorigen Ansprüche 16, 17 oder 22, wobei es sich bei der Benutzeridentifikation um ein biometrisches Merkmal handelt.

24. Elektronische Gesundheitskarte (122) nach Anspruch 14, wobei die Mittel zur Durchführung des Challenge-Response Verfahrens dazu ausgebildet sind, die Verschlüsselung unter Verwendung eines auf der elektronischen Gesundheitskarte (122) gespeicherten Sitzungsschlüssels (132) durchzuführen, wobei der Sitzungsschlüssel aus der Kennung und einem Autorisierungsschlüssels des Lesegeräts ableitbar ist.

25. Elektronische Gesundheitskarte (122) nach einem der vorigen Ansprüche 14 oder 24, wobei die Kennung als Strichcode (136) kodiert auf der elektronischen Gesundheitskarte (122) aufgedruckt ist.

26. Elektronische Gesundheitskarte (122) nach einem der vorigen Ansprüche 14 bis 25, wobei es sich bei der Elektronischen Gesundheitskarte (122) um eine Chipkarte handelt.

27. Lesegerät, wobei das Lesegerät (110) eine Nahfeld-Funkschnittstelle (106) aufweist und zur Nahfeld-Kommunikation über eine Kommunikationsverbindung mit einer elektronischen Gesundheitskarte (122) ausgebildet ist, wobei das Lesegerät ferner Mittel zum Anmelden der elektronischen Gesundheitskarte (122) aufweist, wobei die Mittel zum Anmelden der elektronischen Gesundheitskarte (122) umfassen:
- Mittel zum Lesen einer auf der elektronischen Gesundheitskarte (122) aufgedruckten Kennung (136)
- Mittel zur Durchführung eines Challenge-Response Verfahrens zwischen der elektronischen Gesundheitskarte (122) und dem Lesegerät, wobei die Mittel zur Durchführung des Challenge-Response Verfahrens dazu ausgebildet sind, eine Verschlüsselung beim Challenge-Response Verfahren unter Verwendung der Kennung durchzuführen, wobei es sich bei der Kennung um einen öffentlichen Gesundheitskartenschlüssel handelt.

28. Lesegerät (110) nach Anspruch 27, wobei es sich bei der Funkschnittstelle um eine RFID-Sende-Empfangseinheit handelt.

29. Lesegerät (110) nach einem der vorigen Ansprüche 27 oder 28, ferner mit:
- Mittel zum Empfang einer Benutzeridentifikation,
- Mittel zur Übertragung einer Anforderung zur Fernüberprüfung der Benutzeridentifikation an die elektronische Gesundheitskarte (122).

30. Lesegerät (110) nach einem der vorigen Ansprüche 27 oder 28, ferner mit:
- Mittel zum Empfang einer Benutzeridentifikation,
- Mitteln zum Verschlüsseln der Benutzeridentifikation mit einem öffentlichen Gesundheitskartenschlüssel der Gesundheitskarte (122),
- Mitteln zum Senden der verschlüsselten Benutzeridentifikation an die elektronische Gesundheitskarte (122).

31. Lesegerät (110) nach Anspruch 30, ferner mit Mitteln zum Abruf des öffentlichen Gesundheitskartenschlüssels von der Gesundheitskarte (122) oder von einer externen Datenbank (118).

32. Lesegerät (110) nach Anspruch 27 oder 28, ferner mit Mitteln zur Authentisierung gegenüber der elektronischen Gesundheitskarte (122), wobei die Mittel zum Authentifizieren Mittel zum Senden eines digitalen Zertifikats (138) an die elektronische Gesundheitskarte (122) umfassen, wobei das Zertifikat Zugriffsberechtigungen auf Daten der Gesundheitskarte (122) umfasst.

33. Lesegerät (110) nach Anspruch 32, ferner mit
- Mitteln zum Empfang von in der Gesundheitskarte (122) gespeicherten Bilddaten, wobei die Bilddaten zumindest ein Gesichtsbild des Inhabers der Gesundheitskarte (122) aufweisen, und
- Mitteln (108) zum visuellen Anzeigen des in den Bilddaten enthaltenen Bildes.

34. Lesegerät (110) nach Anspruch 32, ferner mit Mitteln (114) zum Authentifizieren des Benutzers der elektronischen Gesundheitskarte (122) gegenüber der elektronischen Gesundheitskarte (122), mit:
- Mitteln zum Empfangen einer Benutzeridentifikation von der Gesundheitskarte (122),
- Mitteln zum Empfang einer Benutzereingabe,

- Mitteln zur Überprüfung der Benutzereingabe, wobei der Benutzer der elektronischen Gesundheitskarte (122) erfolgreich authentifiziert ist, wenn die Benutzeridentifikation mit der Benutzereingabe übereinstimmt.

35. Lesegerät (110) nach einem der vorigen Ansprüche 29, 30 oder 34, es sich bei der Benutzeridentifikation um ein biometrisches Merkmal handelt.

36. Lesegerät (110) nach Anspruch 27, wobei die Mittel zur Durchführung des Challenge-Response Verfahrens ferner umfassen:
- Mittel zum Empfang eines Autorisierungsschlüssels,
- Mittel (114) zur Erzeugung eines Sitzungsschlüssels anhand der Kennung und des Autorisierungsschlüssels,
- Mittel (114) zum Verschlüsseln der Zufallskennung mittels des Sitzungsschlüssels.

37. Lesegerät (110) nach einem der vorigen Ansprüche 27 bis 36, wobei es sich bei dem Lesegerät (110) um einen Konnektor handelt.

38. Computerprogrammprodukt (114; 130) mit von einem Prozessor ausführbaren Instruktionen zur Durchführung der Verfahrensschritte nach einem der vorigen Ansprüche 1 bis 13.

Es folgen 5 Seiten Zeichnungen

Anhängende Zeichnungen

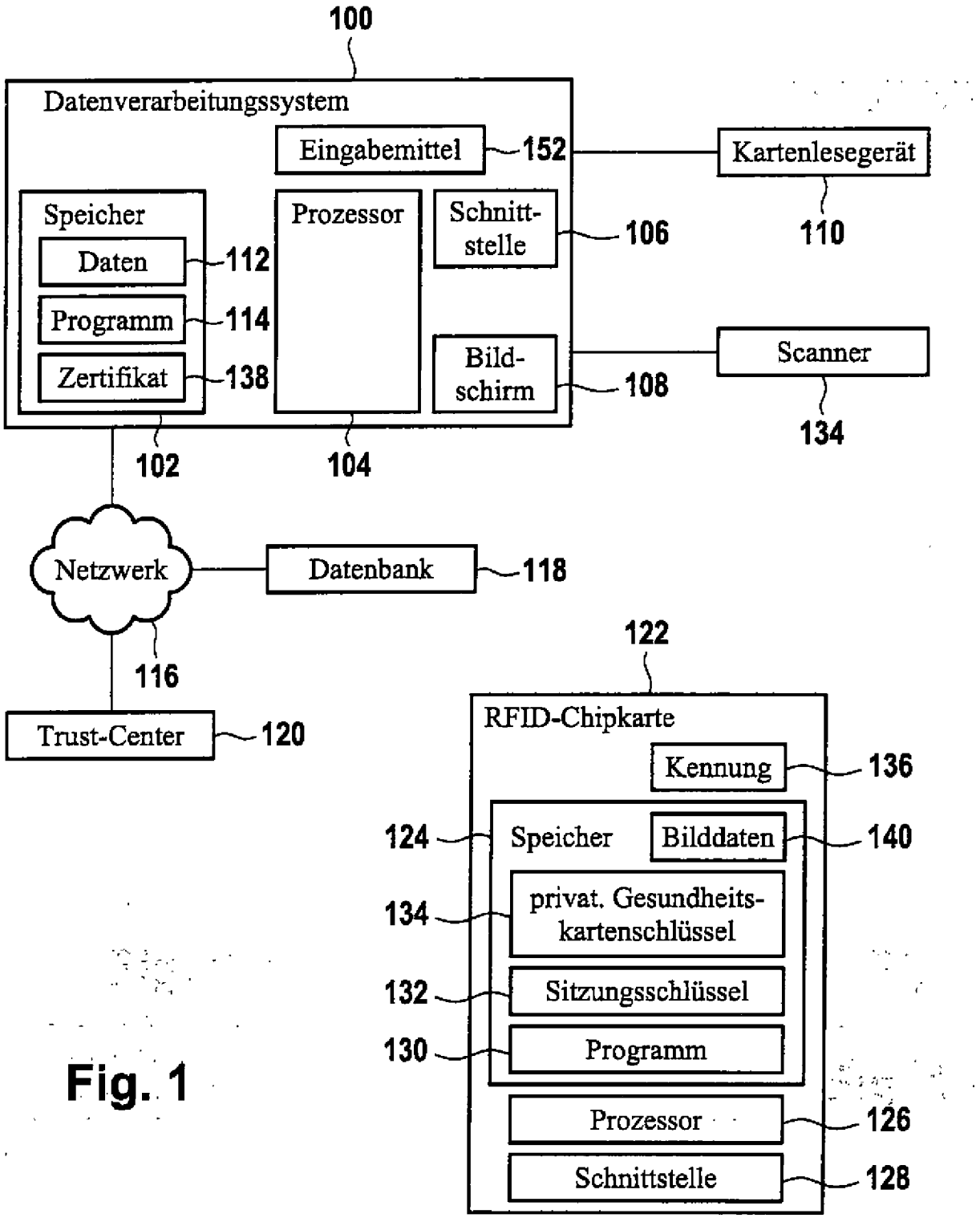


Fig. 1

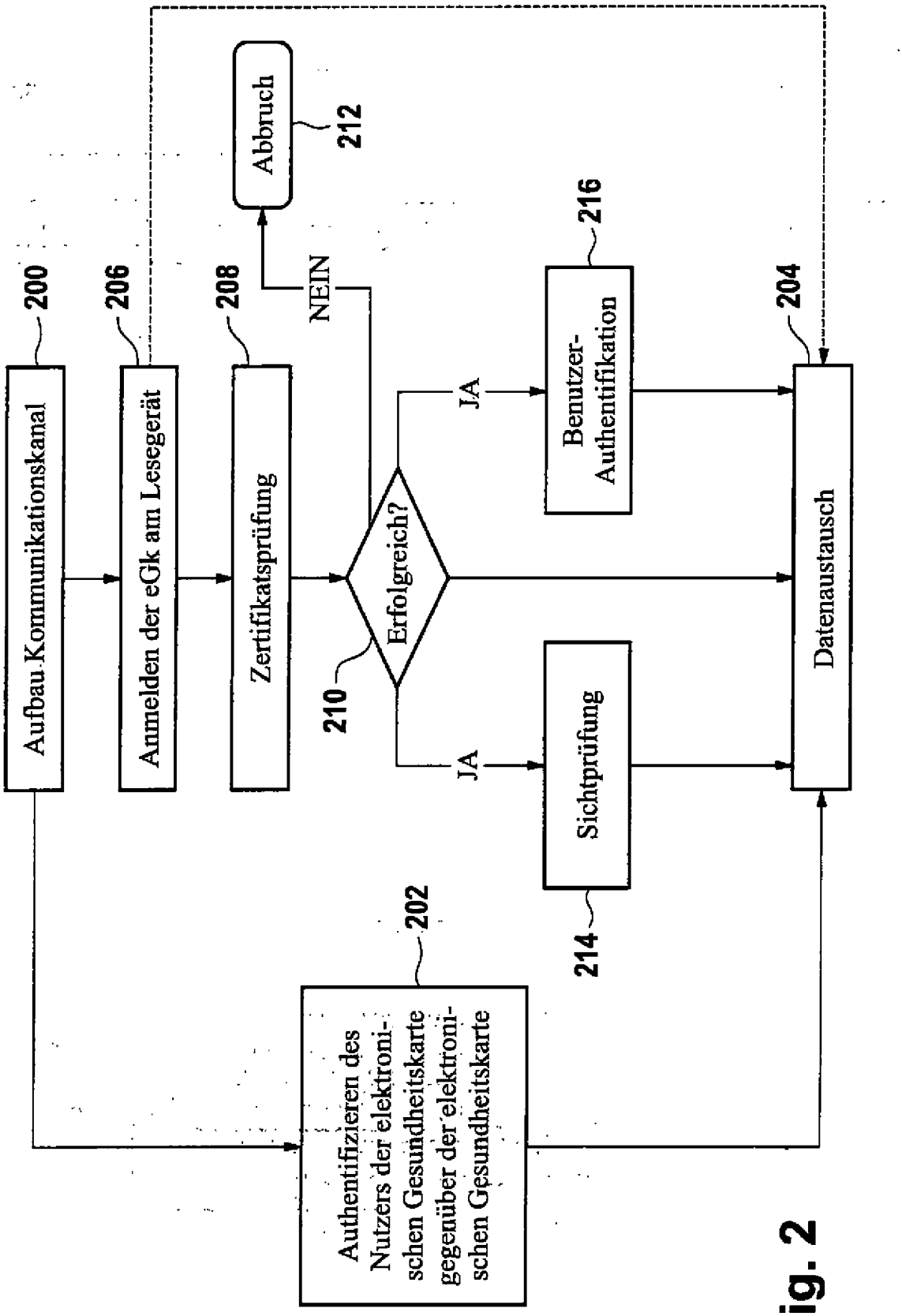

Aufbau Kommunikationskanal
200
Anmelden der eGk am Lesegerät
206
Zertifikatsprüfung
208
Abbruch
212
NEIN
Erfolgreich?
210
JA
Benutzer-Authentifikation
216
JA
Sichtprüfung
214
Datenaustausch
204
Authentifizieren des Nutzers der elektronischen Gesundheitskarte gegenüber der elektronischen Gesundheitskarte
202

Fig. 2

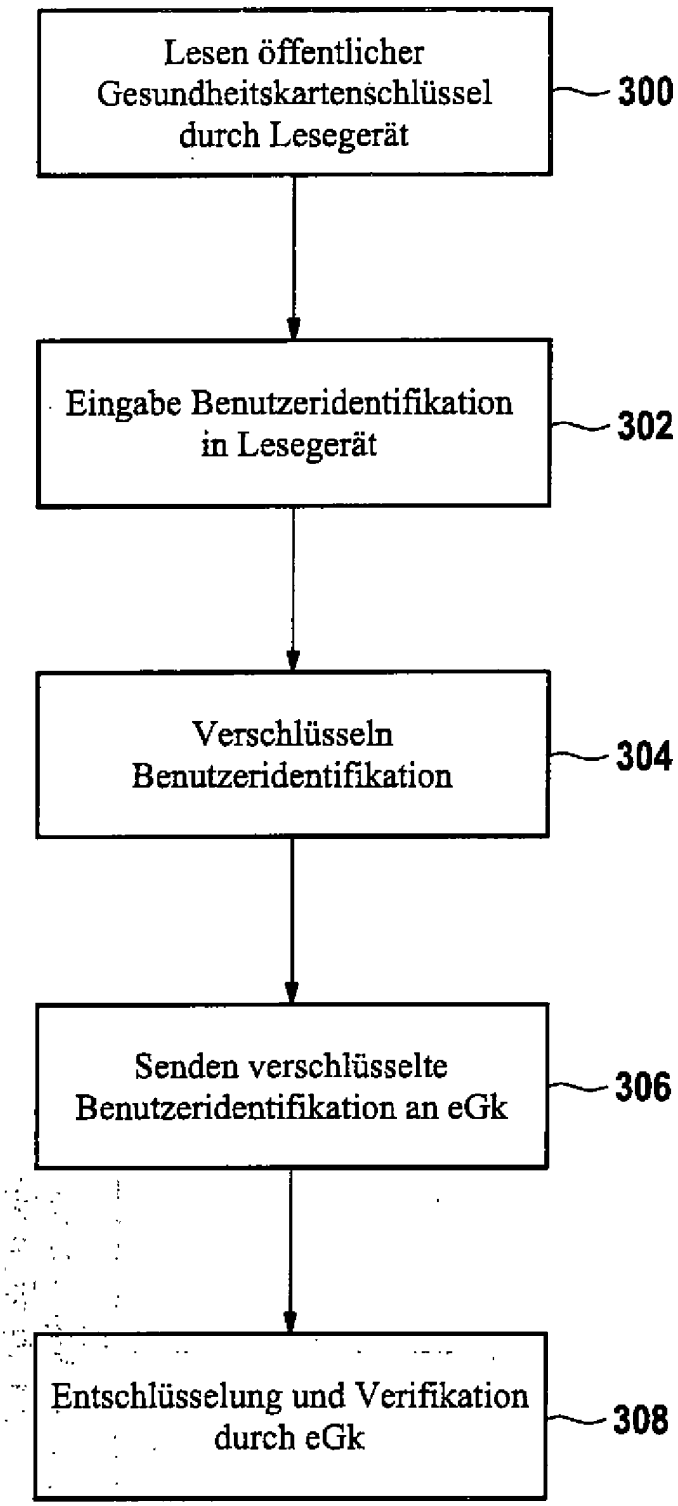

Lesen öffentlicher Gesundheitskartenschlüssel durch Lesegerät
300
Eingabe Benutzeridentifikation in Lesegerät
302
Verschlüsseln Benutzeridentifikation
304
Senden verschlüsselte Benutzeridentifikation an eGk
306
Entschlüsselung und Verifikation durch eGk
308

Fig. 3

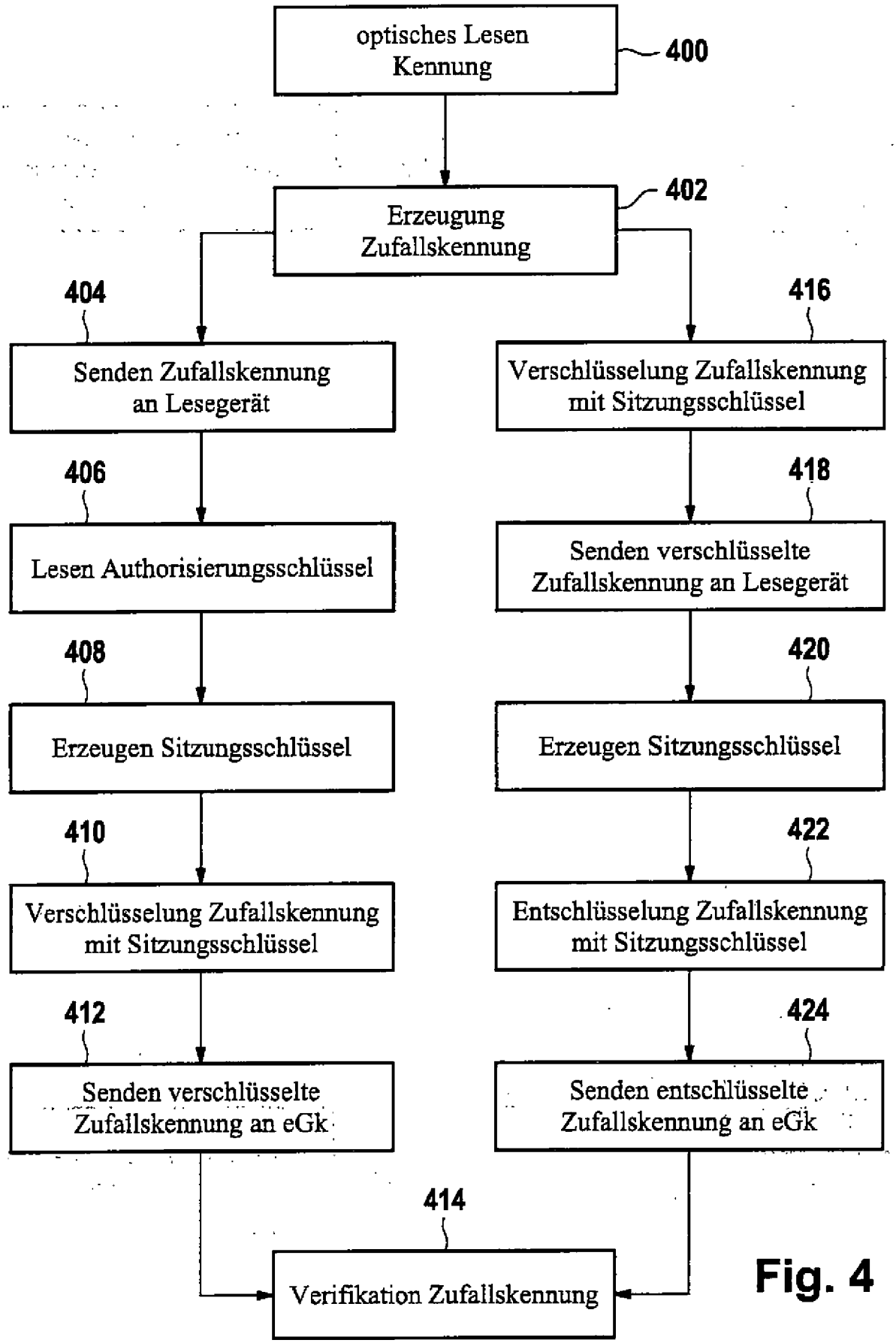

optisches Lesen Kennung
400
Erzeugung Zufallskennung
402
404
Senden Zufallskennung an Lesegerät
406
Lesen Authorisierungsschlüssel
408
Erzeugen Sitzungsschlüssel
410
Verschlüsselung Zufallskennung mit Sitzungsschlüssel
412
Senden verschlüsselte Zufallskennung an eGk
416
Verschlüsselung Zufallskennung mit Sitzungsschlüssel
418
Senden verschlüsselte Zufallskennung an Lesegerät
420
Erzeugen Sitzungsschlüssel
422
Entschlüsselung Zufallskennung mit Sitzungsschlüssel
424
Senden entschlüsselte Zufallskennung an eGk
414
Verifikation Zufallskennung

Fig. 4

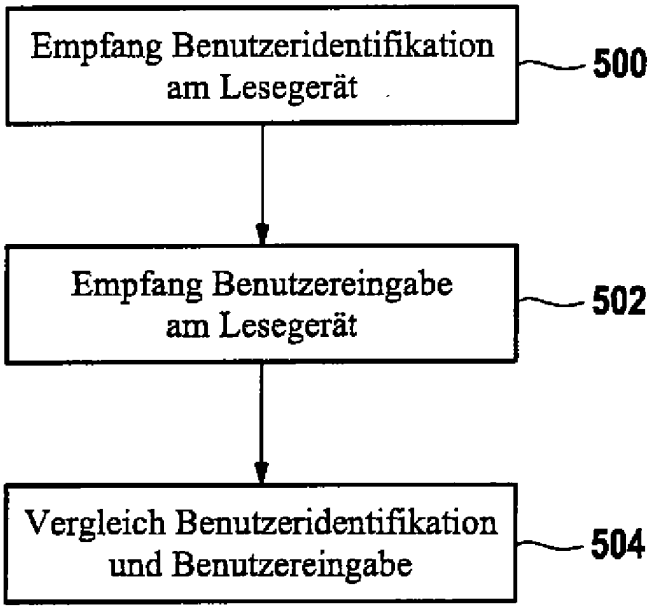

Empfang Benutzeridentifikation am Lesegerät
500
Empfang Benutzereingabe am Lesegerät
502
Vergleich Benutzeridentifikation und Benutzereingabe
504

Fig. 5