(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 20 2008 013 415 U1** 2009.04.23

(12) **Gebrauchsmusterschrift**

(21) Aktenzeichen: **20 2008 013 415.3**
(22) Anmeldetag: **10.10.2008**
(47) Eintragungstag: **19.03.2009**
(43) Bekanntmachung im Patentblatt: **23.04.2009**

(51) Int Cl.[8]: ***H04L 9/32*** (2006.01)
G06Q 50/00 (2006.01)

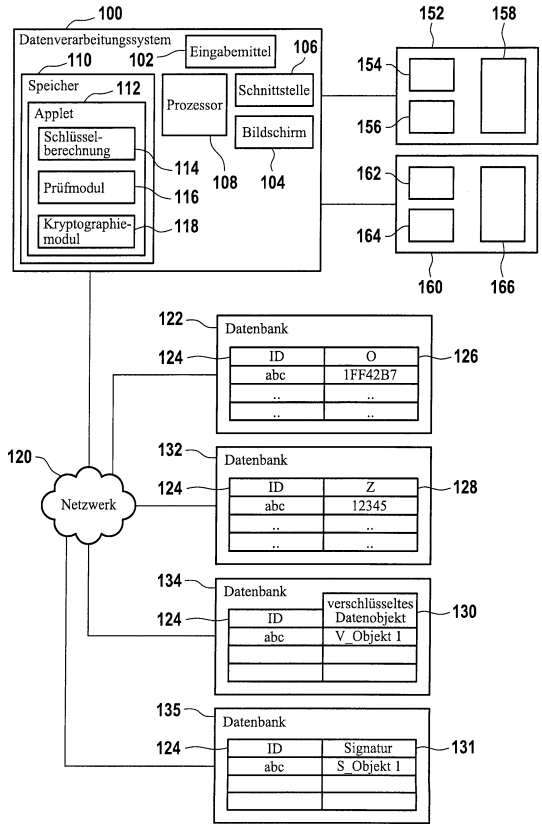
(73) Name und Wohnsitz des Inhabers:
CompuGROUP Holding AG, 56070 Koblenz, DE

(74) Name und Wohnsitz des Vertreters:
Richardt, M., Dipl.-Ing., Pat.-Anw., 65343 Eltville

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Datenverarbeitungssystem zur Bereitstellung von Berechtigungsschlüsseln**

(57) Hauptanspruch: Computerprogrammprodukt (114; 116) mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Bereitstellung von Berechtigungsschlüsseln (154; 156; 162; 164), wobei das Verfahren die folgenden Schritte umfasst:
– Empfang eines weiteren asymmetrischen kryptografischen Schlüsselpaares (162; 164), wobei das weitere asymmetrische Schlüsselpaar Teil einer Schlüsselpaarsequenz ist, wobei das weitere asymmetrische Schlüsselpaar einen weiteren ersten (162) und einen weiteren zweiten (164) Berechtigungsschlüssel umfasst,
– Abrufen eines Chiffrats (150), wobei das Chiffrat dem Schlüsselpaar (154; 156) zugeordnet ist, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar (162; 164) unmittelbar vorangeht, wobei das Chiffrat (150) den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel (156) des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, umfasst,
– Entschlüsseln des initialen ersten Berechtigungsschlüssels mit dem ersten Berechtigungsschlüssel (154) des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht,
– Erzeugen eines weiteren Chiffrats...



Beschreibung

[0001] Die Erfindung betrifft ein Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Bereitstellung von Berechtigungsschlüsseln, ein Computerprogrammprodukt zur Durchführung von Verfahrensschritten zur Entschlüsselung eines Datenobjekts und ein Datenverarbeitungssystem.

[0002] Die elektronische Gesundheitskarte, abgekürzt eGK, soll in Zukunft 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 auch unter anderem die Ermöglichung eines Zugriffs auf einen elektronischen Arztbrief, eine elektronische Krankenakte sowie ein elektronisches Rezept mit Hilfe der elektronischen Gesundheitskarte.

[0003] Beispielsweise können somit medizinische Datenobjekte (MDOs) wie ein elektronischer Arztbrief, eine elektronische Krankenakte oder ein elektronisches Rezept verschlüsselt und digital signiert auf einem zentralen Server gespeichert werden. Eine Verschlüsselung erfolgt dabei vorzugsweise über einen symmetrischen Schlüssel, der für jedes neue medizinische Datenobjekt einer elektronischen Krankenakte wie z. B. ein elektronischer Arztbrief oder ein elektronisches Rezept individuell zufällig erzeugt wird. Der symmetrische Schlüssel selbst wird nach seiner Erstellung beispielsweise mit einem öffentlichen Schlüssel verschlüsselt und zusammen mit den verschlüsselten medizinischen Datenobjekten auf dem zentralen Server abgelegt. Dieser zur Verschlüsselung verwendete öffentliche Schlüssel bildet dabei zusammen mit einem privaten Schlüssel, welcher auf der elektronischen Gesundheitskarte abgespeichert ist, ein kryptografisches asymmetrisches Schlüsselpaar. Damit ist gewährleistet, dass ausschließlich unter Verwendung des geheimen Gesundheitskartenschlüssels ein Zugriff auf die verschlüsselten medizinischen Datenobjekte möglich ist. Bei einem solchen Zugriff erfolgt zunächst eine Entschlüsselung des verschlüsselten symmetrischen Schlüssels mittels des geheimen Gesundheitskartenschlüssels, woraufhin dann mit dem entschlüsselten symmetrischen Schlüssel eine weitere Entschlüsselung der medizinischen Datenobjekte möglich ist. Wurde bei der Erstellung eines MDOs auch eine digitale Signatur mit dem geheimen Gesundheitskartenschlüssel erzeugt, so kann anschließend die Integrität des MDOs und die Authentizität des MDO-Erzeugers über die digitale Signatur verifiziert werden.

[0004] Beispielsweise offenbart die DE 10 2004 051 296 B3 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 zum Beispiel ein MDO einer Patientenakte, von einem Praxis-EDV-System einer Arztpraxis verschlüsselt und digital signiert an einen Datenserver übertragen werden.

[0005] Aus der DE 102 58 769 A1 ist eine weitere Anwendung von Chipkarten für Patientendaten bekannt.

[0006] Bei der Verwendung der elektronischen Gesundheitskarte ergibt sich die Problematik, dass im Falle beispielsweise eines Krankenkassenwechsels und der damit verbundenen Ausgabe einer neuen elektronischen Gesundheitskarte mit entsprechenden neuen asymmetrischen Schlüsselpaaren ein problemloser Zugriff auf eine elektronische Krankenakte nicht mehr möglich ist, welche zuvor unter Verwendung der alten elektronischen Gesundheitskarte verschlüsselt wurde.

[0007] Der Erfindung liegt demgegenüber die Aufgabe zugrunde, ein verbessertes Computerprogrammprodukt zur Durchführung von Verfahrensschritten zur Bereitstellung von Berechtigungsschlüsseln, ein verbessertes Computerprogrammprodukt zur Durchführung von Verfahrensschritten zur Entschlüsselung eines Datenobjekts und ein verbessertes Datenverarbeitungssystem zu schaffen.

[0008] Die der Erfindung zugrunde liegenden Aufgaben werden jeweils mit den Merkmalen der unabhängigen Schutzansprüche gelöst. Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Schutzansprüchen angegeben.

[0009] Erfindungsgemäß betrifft die Erfindung ein Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Bereitstellung von Berechtigungsschlüsseln, wobei das Verfahren den Schritt umfasst des Empfangens eines weiteren asymmetrischen kryptografischen Schlüsselpaares, wobei das weitere asymmetrische Schlüsselpaar Teil einer Schlüsselpaarsequenz ist, wobei das weitere asymmetrische Schlüsselpaar einen weiteren ersten und einen weiteren zweiten Berechtigungsschlüssel umfasst. Daraufhin erfolgt das Abrufen eines Chiffrats, wobei das Chiffrat dem Schlüsselpaar zugeordnet ist, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, wobei das Chiffrat den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel des Schlüsselpaars, welches in der Sequenz von Schlüsselpaar dem weiteren Schlüsselpaar unmittelbar vorangeht, umfasst. Dem folgt das Entschlüsseln des in-

itialen ersten Berechtigungsschlüssels mit dem ersten Berechtigungsschlüssel des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht. Es erfolgt das Erzeugen eines weiteren Chiffrats durch Verschlüsseln des entschlüsselten initialen ersten Berechtigungsschlüssels mit dem zweiten Berechtigungsschlüssel des weiteren Schlüsselpaares. Schließlich erfolgt die Speicherung des weiteren Chiffrats.

[0010] Die Durchführung der genannten Verfahrensschritte hat den Vorteil, dass mit beliebigen asymmetrischen kryptografischen Schlüsselpaaren innerhalb einer Sequenz von Schlüsselpaaren gewährleistet ist, dass Datenobjekte, welche unter Verwendung eines der asymmetrischen kryptografischen Schlüsselpaare der Sequenz von Schlüsselpaaren verschlüsselt wurden, wieder entschlüsselt werden können. Zur Entschlüsselung ist hierfür das zur ursprünglichen Verschlüsselung verwendete „Original" Schlüsselpaar nicht notwendig.

[0011] Bevorzugterweise wird so vorgegangen, dass neue Datenobjekte grundsätzlich mit dem initialen zweiten Berechtigungsschlüssel verschlüsselt werden. Unter Verwendung eines beliebigen Schlüsselpaares der Sequenz von asymmetrischen kryptografischen Schlüsselpaaren kann daraufhin durch entsprechenden Zugriff auf das Chiffrat, welches dem jeweiligen Schlüsselpaar zugeordnet ist, der initiale erste Berechtigungsschlüssel bereitgestellt werden, mit welchem wiederum eine Entschlüsselung des Datenobjekts möglich ist.

[0012] Zur Durchführung der genannten Verfahrensschritte ist zur Verwendung eines neuen bzw. weiteren asymmetrischen kryptografischen Schlüsselpaares für Ver- und Entschlüsselungsvorgänge von Datenobjekten somit lediglich Voraussetzung, dass ein entsprechender Benutzer im Besitz des asymmetrischen kryptografischen Schlüsselpaares ist, welches in der Sequenz von Schlüsselpaaren dem neuen Schlüsselpaar unmittelbar vorangeht. In einem praktischen Beispiel von Gesundheitskarten würde dies damit bedeuten, dass ein Besitzer einer neuen elektronischen Gesundheitskarte zu deren „Aktivierung" lediglich einmalig seine zuvor verwendete alte elektronische Gesundheitskarte zu einem entsprechenden Gesundheitsdienstleister oder allgemein einer vertrauenswürdigen Stelle mitbringt. Unter Verwendung der alten und der neuen elektronischen Gesundheitskarte wird daraufhin das neue Chiffrat erzeugt, mittels welchem es möglich ist, sowohl mit der alten als auch mit der neuen elektronischen Gesundheitskarte auf verschlüsselte Datenobjekte sicher zuzugreifen.

[0013] Nach einer Ausführungsform der Erfindung wird das Chiffrat in einer Datenbank gespeichert. Beispielsweise kann hier eine Datenbank einer zentralen vertrauenswürdigen Stelle zum Einsatz kommen.

[0014] Nach einer weiteren Ausführungsform der Erfindung umfasst das Computerprogrammprodukt ferner Instruktionen zur Durchführung des Schrittes des Erzeugens des weiteren asymmetrischen kryptografischen Schlüsselpaars, wobei die Instruktionen die folgenden Schritte umfassen:

1. Empfang einer eindeutigen Benutzeridentifikation id und einer der Benutzeridentifikation zugeordneten beliebig wählbaren Benutzerkennung pw.
2. Abbildung der Benutzerkennung auf einen Wert durch eine Funktion g. Bei der Funktion g kann es sich um die Identitätsfunktion oder eine nicht triviale Funktion handeln. Unter dem Aspekt der Sicherheit und Vertraulichkeit ist g vorzugsweise als eine kollisionsfreie Einwegfunktion gewählt (sog. one-way Funktion), wie z. B. eine kryptografische Hashfunktion.
3. Erzeugung eines Zufallswertes z.
4. Berechnung des weiteren ersten Datenobjektschlüssels durch Anwendung einer Funktion f auf g(Benutzerkennung) und Z. Beispielsweise werden g(Benutzerkennung), d. h. das Ergebnis der Anwendung der Funktion g auf die Benutzerkennung, und z miteinander verkettet und die Funktion f wird auf das Ergebnis dieser Verkettung angewendet. Z. B. kann f eine kryptografische Hash-Funktion sein, die auf die Konkatenation des Hash-Wertes der Benutzerkennung und des Zufallswertes z angewendet wird.
5. Berechnung des weiteren zweiten Datenobjektschlüssels aus dem weiteren ersten Datenobjektschlüssel, wobei der weitere erste und der weitere zweite Datenobjektschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden. Beispielsweise kann:

• für elliptische Kurven der weitere zweite Datenobjektschlüssel, der ein Punkt auf der elliptischen Kurve ist, durch Multiplikation des ersten Datenobjektschlüssels, der eine ganze Zahl darstellt, mit dem Basispunkt aus den Domainparametern berechnet werden.

• für RSA wird der weitere zweite Datenobjektschlüssel (eine ganze Zahl) derart berechnet, dass er mit dem ersten Datenobjektschlüssel (ebenfalls eine ganze Zahl) eine im RSA-Verfahren definierte Kongruenzrelation erfüllt.

[0015] Die Durchführung der genannten Verfahrensschritte hat den Vorteil, dass hier asymmetrische kryptografische Schlüsselpaare erzeugt werden können, wobei dies unter Verwendung einer beliebig wählbaren Benutzerkennung erfolgt. Die Benutzerkennung selbst geht in den Berechnungsalgorithmus für den weiteren ersten und weiteren zweiten Datenobjektschlüssel ein.

[0016] Im Falle dessen, dass das erfindungsgemäße Computerprogrammprodukt im Rahmen der elektronischen Gesundheitskarte eingesetzt wird, ist Benutzer in der Lage, einen Zugriff auf seine Patientendaten entweder unter Verwendung seiner elektronischen Gesundheitskarte, oder aber unter Verwendung seiner selbst gewählten Benutzerkennung durchzuführen. Entscheidet sich ein Benutzer, zusätzlich neben seiner elektronischen Gesundheitskarte auch noch die Möglichkeit eines passwortgestützten Zugriffs auf seine Patientendaten zu ermöglichen, so wird auch hier vorzugsweise von einer vertrauenswürdigen Stelle einmalig nach Eingabe der Benutzerkennung das entsprechende weitere asymmetrische kryptografische Schlüsselpaar erzeugt und unter Verwendung der zusätzlich im Besitz des Patienten befindlichen elektronischen Gesundheitskarte das Chiffrat erstellt, sodass auf Datenobjekte, welche zuvor unter Verwendung der elektronischen Gesundheitskarte chiffriert wurden, auch mittels der weiter gewählten Benutzerkennung zugegriffen werden kann, wobei dies auch in umgekehrter Reihenfolge gilt.

[0017] Damit unterscheidet sich dieses Verfahren zur Erzeugung eines asymmetrischen kryp-tografischen Schlüsselpaares von gängigen Schlüsselerzeugungsverfahren, bei wel-chen nach heutigem Stand der Technik lediglich eine Zuordnung einer beliebig wählba-ren Benutzerkennung zu einem zugehörigen erzeugten kryptografischen Schlüsselpaar möglich ist, nicht hingegen eine funktionale Berechung von Schlüsselpaaren unter Ver-wendung der beliebig wählbaren Benutzerkennung selbst, bei der die permanente Speicherung der Zuordnung der Benutzerkennung zum Schlüssel entfällt.

[0018] Bei bisher üblichen Verfahren wird eine beliebig gewählte Benutzerkennung oder deren Abbild in einer Tabelle gespeichert und öffentlichen und privaten Schlüsseln eindeutig zugeordnet, wobei lediglich durch administrative und/oder juristische Regelungen fest-gelegt wird, dass unbefugte Personen keinen Zugriff auf den privaten Schlüssel haben dürfen. Diese Vorgehensweise beeinträchtigt die Sicherheit erheblich: Bekommt eine unbefugte Person oder auch eine staatliche Stelle aufgrund von diversen Überwa-chungsgesetzen Zugriff auf die Datenbank, welche die Passwörter den öffentlichen und privaten Schlüsseln zuordnet, so ist diese Person oder Organisation sofort in der Lage, durch Zugriff auf diese einzelne schlüsselverwaltende Institution Zugriff auf alle Daten-Objekte einer Person zu erhalten.

[0019] Damit hat das Verfahren zur Erzeugung eines asymmetrischen kryptografischen Schlüsselpaares den Vorteil, dass nebst der Möglichkeit einer beliebig wählbaren Benutzerkennung keine zentrale Instanz in Besitz der Kombination von Benutzerkennung (z. B. Passwort) und Schlüsselpaaren gelangen kann. Der weitere erste Datenobjektschlüssel lässt sich lediglich unter Kenntnis eines Zufallswertes und der Benutzerkennung berechnen. Die Erzeugung des weiteren zweiten Datenobjektschlüssels erfordert ebenfalls die Kenntnis des Zufallswerts und der Benutzerkennung, wobei die Benutzerkennung vorzugsweise ausschließlich in geheimer Weise in Kenntnis des entsprechenden Benutzers steht. Damit ist es zum Beispiel nicht mehr möglich, durch Beschlagnahmung oder Diebstahl von zentralen Datenbankservern Zugriff auf Datenobjektschlüssel und damit auf verschlüsselte Daten ohne aktives Mithelfen jener Personen zu erhalten, welche in Besitz ihrer privaten, geheimen Benutzerkennungen stehen.

[0020] Ein weiterer Vorteil des erfindungsgemäßen Verfahrens ist, dass selbst bei Wahl der gleichen Benutzerkennung durch verschiedene Benutzer aufgrund des Eingehens des Zufallswertes bei der Erzeugung des weiteren ersten Datenobjektschlüssel sichergestellt werden kann, dass niemals das gleiche Schlüsselpaar verschiedenen Benutzern zugeordnet wird.

[0021] Es sei hier darauf hingewiesen, dass Ausführungsformen des erfindungsgemäßen Ver-fahrens zur Erzeugung eines asymmetrischen kryptografischen Schlüsselpaares auf beliebige Kryptosysteme zur Erzeugung asymmetrischer Schlüsselpaare angewendet werden können, wie zum Beispiel das RSA-, das Rabin- und das Elgamal-Kryptosystem oder kryptografische Verfahren auf elliptischen Kurven. Aus dem weiteren ersten Datenobjektschlüssel, den man basierend auf der Benutzerkennung und dem Zufallswert erhalten hat, wird der weitere zweite Datenobjektschlüssel berechnet, wobei für diese Berechnung solche Verfahren zur Anwendung kommen können.

[0022] Hierzu kann es erforderlich sein, dass der weitere erste Datenobjektschlüssel eine oder mehrere vorgegebene Eigenschaften haben muss und/oder Bedingungen erfüllen muss, die im Rahmen einer Zulässigkeitsprüfung überprüft werden. Wenn sich der weitere erste Schlüssel als für ein gewähltes Verfahren unzulässig erweist, so wird ein neuer Zufallswert generiert, um einen neuen Kandidaten für einen weiteren ersten Datenobjektschlüssel zu erzeugen, der dann wiederum einer Zulässigkeitsprüfung unterzogen wird. Dies wird solange wiederholt, bis ein zulässiger weiterer erster Datenobjektschlüssel gefunden worden ist. In diese Zulässigkeitsprüfung können Beschränkungen eingehen, welche sich direkt aus dem Algorithmus zur Durchführung eines entsprechenden asymmetrischen kryptografischen Schlüsselerzeugungsverfahrens ergeben.

[0023] Darüber hinaus können auch weitere Einschränkungen in die Zulässigkeitsprüfung ein-gehen, welche sich z. B. auf die Entropie des erzeugten

Schlüssels beziehen oder aus aktuellen Erkenntnissen bezüglich der Angreifbarkeit des entsprechenden Schlüsseler-zeugungsverfahrens ergeben. Beispielsweise gibt es für das RSA-Verfahren eine Reihe von allgemein bekannten und regelmäßig ergänzten Beschränkungen, deren Einhaltung bei einer Schlüsselerzeugung von Behördenstellen gefordert wird, um die Angreifbarkeit der erzeugten Schlüsselpaare zu minimieren. Beispielsweise spezifiziert PKCS#1 (Pub-lic Key Cryptography Standards) eine Reihe von kryptografischen Spezifikationen für RSA, welche von öffentlichen und privaten RSA-Schlüsselpaaren eingehalten werden müssen. Der in der Entwicklung befindliche Standard PKCS#13 wird die Anforderungen an die Schlüsselerzeugung auf elliptischen Kurven festsetzen.

[0024] Ein Aspekt der Erfindung ist, dass die Berechnung des weiteren ersten Datenobjektschlüssels unter Verwendung einer Funktion g, angewendet auf die Benutzerkennung pw erfolgt. Nach einer Ausführungsform wird entweder die beliebig wählbare Benutzerkennung als solche empfangen und daraufhin unter Verwendung der Funktion g umgewandelt, oder es wird direkt der Funktionswert g(pw) empfangen.

[0025] Die Berechnung des weiteren ersten Datenobjektschlüssels unter Verwendung des Wertes b = g(pw) und des Zufallswertes z hat den Vorteil, dass somit aus verhältnismäßig unsicheren Benutzerkennungen Eingangswerte berechnet werden können, welche eine hohe Zufälligkeit haben und somit in effektiver Weise bei der Berechnung des ersten Datenobjektschlüssels die Sicherheit desselben weiter erhöhen. Beispielsweise wird für g die kryptografische Hash-Funktion SHA-256 angewendet.

[0026] Nach einer weiteren Ausführungsform der Erfindung wird der weitere erste Datenobjektschlüssel durch Anwenden einer Funktion f auf die Werte b und z berechnet. Beispielsweise kann f als die Anwendung der kryptografischen Hash-Funktion SHA-256 auf die Konkatenation, also Hintereinanderhängung, von b und z definiert sein.

[0027] Durch Anwendung der Funktion f auf den Zufallswert z und den Funktionswert g(pw) wird eine hohe Qualität des weiteren ersten Datenobjektschlüssels gewährleistet. In anderen Worten, der weitere erste Datenobjektschlüssel weist aufgrund der zufälligen Wahl von z ebenfalls eine hohe Zufälligkeit auf, sodass ein Erraten des weiteren ersten Datenobjektschlüssels damit praktisch unmöglich gemacht wird.

[0028] Nach einer Ausführungsform der Erfindung wird das Schlüsselpaar für ein Kryptosystem auf elliptischen Kurven berechnet. Eine elliptische Kurve ist gegeben durch die Gleichung $y^2 = x^3 + ax + b$, wobei die Parameter a und b, wie auch die Koordinaten der Punkte (x, y) auf der Kurve ganze Zahlen aus dem Intervall [0, n – 1] sind. Die Werte a, b, n, sowie ein gewählter Kurvenpunkt P bilden die sogenannten Domain-Parameter der elliptischen Kurve, welche zur Durchführung von kryptografischen Verfahren unter Verwendung des weiteren ersten und weiteren zweiten Schlüssels mit bekannt gegeben werden müssen. Die Anzahl der Punkte, die die Gleichung einer elliptischen Kurve erfüllen, bezeichnet man als die Ordnung der Kurve. Der erste Datenobjektschlüssel stellt eine natürliche Zahl dar, und der weitere zweite Datenobjektschlüssel, ein Punkt auf der Kurve, ist das Ergebnis der Multiplikation des weiteren ersten Datenobjektschlüssels mit dem Kurvenpunkt P der elliptischen Kurve.

[0029] Die Verwendung eines Kryptosystems auf elliptischen Kurven hat folgende Vorteile:

- Der erste Datenobjektschlüssel kann eine beliebige natürliche Zahl aus dem Intervall [1, n – 1] sein. Sie ist an keine weiteren funktionalen Bedingungen gebunden; der Aspekt ihrer Beliebigkeit wird im weiteren Verlauf eine große Rolle spielen.
- Ein Kryptosystem auf elliptischen Kurven zu brechen hat eine sehr hohe Komplexität, die viel höher ist als bei RSA.
- Die Schlüssel sind im Vergleich zu RSA sehr kurz und die Berechnungen auf der Kurve relativ einfach, womit sie vielseitig und effizient implementiert werden können.
- Der weitere zweite Datenobjektschlüssel kann aus dem weiteren ersten Datenobjektschlüssel einfach und jederzeit wieder berechnet werden.

[0030] Über die Funktionen f und g kann sehr effizient aus der Benutzerkennung und dem Zufallswert der weitere erste Datenobjektschlüssel berechnet werden. Damit ist es möglich, durch mathematische Funktionen der gewählten Benutzerkennung das kryptografische Schlüsselpaar zuzuordnen. Wegen dieses funktionellen Zusammenhangs ist hier ein Vorhalten einer tabellarischen Zuordnung von Schlüsselpaar und einer entsprechenden Benutzerkennung nicht notwendig.

[0031] Nach einer weiteren Ausführungsform der Erfindung umfasst das Verfahren den Schritt der Zulässigkeitsprüfung des ersten Datenobjektschlüssels. Im Rahmen der Zulässigkeitsprüfung wird geprüft, ob der weitere erste Datenobjektschlüssel größer als 1 und kleiner als die Ordnung der elliptischen Kurve ist. Bei Erfüllung dieser Prüfbedingung sind der Zufallswert sowie der weitere erste und der weitere zweite Datenobjektschlüssel zulässig. Ist die Prüfbedingung jedoch nicht erfüllt, wird ein neuer Zufallswert gewählt, mit dem ein erneutes Berechnen des weiteren ersten Datenobjektschlüssels erfolgt sowie ein erneutes Durchführen der Zulässigkeitsprüfung dieses Datenobjektschlüssels. Dieser Vorgang wird wiederholt, bis die Zulässigkeitsprüfung bestanden wird.

[0032] Die Zulässigkeitsprüfung kann um weitere Prüfbedingungen erweitert werden, z. B. um die Prüfung, dass der weitere erste Datenobjektschlüssel eine hohe Zufälligkeit aufweist. Hierzu sei angemerkt, dass in der Kryptografie üblicherweise mit algebraischen Strukturen gearbeitet wird, die nur endlich viele Elemente enthalten. Dies hat seine Ursache darin, dass im Falle einer endlichen Anzahl von Elementen viele in den reellen Zahlen harmlose Probleme schwierig werden, sodass elliptische Kurven mit endlich vielen Elementen effektiv für kryptografische Anwendungen verwendet werden können. Für kryptografische Anwendungen ist es nun wichtig, dass die verwendete algebraische Struktur groß genug ist, das heißt, dass die Anzahl der Punkte auf einer elliptischen Kurve, als Ordnung bezeichnet, ausreichend groß ist. In diesem Kontext muss man in Betracht ziehen, dass der erzeugte weitere erste Datenobjektschlüssel größer sein kann als die Ordnung der elliptischen Kurve. Um hier dennoch eine Assoziation zu ermöglichen, ist es üblich, eine Division des weiteren ersten Datenobjektschlüssels modulo der Ordnung der elliptischen Kurve durchzuführen. Damit ergibt sich jedoch eine hohe Wahrscheinlichkeit, dass die resultierende Zahl sich in einem unteren Wertebereich des Intervalls [2, r – 1] (mit r als der Ordnung der elliptischen Kurve) befindet oder sogar 0 oder 1 ist, sodass sich hiermit die Schwierigkeit reduziert, einen in diesem Wertebereich liegenden Punkt der Kurve mathematisch oder durch Ausprobieren herauszufinden. Durch die Durchführung der Zulässigkeitsprüfung wird somit eine Einschränkung des Wertebereichs, in welchem sich der weitere erste Datenobjektschlüssel befindet, zuverlässig vermieden, sodass sich hiermit die Entropie des weiteren ersten Datenobjektschlüssels und damit dessen Zufälligkeit in ausreichendem Maße sicherstellen lässt.

[0033] Ein weiterer Vorteil der Zulässigkeitsprüfung ist, dass hiermit sichergestellt werden kann, dass eine Verträglichkeit des weiteren ersten Datenobjektschlüssels mit entsprechenden Programmbibliotheken für elliptische Kurven, wie sie nach dem Stand der Technik verfügbar sind, zuverlässig gewährleistet werden kann.

[0034] Es sei hier darauf hingewiesen, dass zur Durchführung des Verfahrens zur Erzeugung eines asymmetrischen kryptografischen Schlüsselpaares unter Verwendung einer elliptischen Kurvenfunktion die Durchführung der Zulässigkeitsprüfung nicht zwingend notwendig ist. Auch ohne Anwendung der Zulässigkeitsprüfung lassen sich hier Schlüsselpaare erzeugen, welche jedoch unter Umständen je nach Benutzerkennung und Zufallswert nicht sehr hohen Sicherheitsanforderungen Rechnung tragen können, welche für kryptografische Anwendungen gefordert sein könnten. Die Zulässigkeitsprüfung ist im Falle elliptischer Kurven ein weiterer Schritt, um sicherzustellen, dass die erzeugten Schlüsselpaare eben jenen Sicherheitsanforderungen genügen.

[0035] Nach einer Ausführungsform der Erfindung ist die Bitlänge des Zufallswertes größer oder gleich der Bitlänge der Ordnung der elliptischen Kurve. Außerdem ist nach einer Ausführungsform der Erfindung der Zufallswert so gewählt, dass der Wert des erzeugten weiteren ersten Datenobjektschlüssels kleiner als die Ordnung der elliptischen Kurve ist. Beide Kriterien haben ebenfalls, wie bereits für die Zulässigkeitsprüfung diskutiert, denselben Effekt, nämlich dass somit eine hohe Entropie des weiteren ersten Datenobjektschlüssels gewährleistet werden kann. Damit wird in anderen Worten die Sicherheit des weiteren ersten Datenobjektschlüssels und damit die Sicherheit des Verschlüsselungsverfahrens signifikant erhöht.

[0036] Nach einer Ausführungsform der Erfindung wird das Schlüsselpaar für ein RSA-Kryptosystem berechnet. Ein RSA-Kryptosystem ist gegeben durch eine Zahl n, die das Produkt zweier Primzahlen p und q ist ($n = p \cdot q$), der Zahl d, die der Bedingung $ggT(d, (p-1)\cdot(q-1)) = 1$ genügt und der Zahl e, die der Bedingung $e \cdot d \equiv 1 \bmod (p-1)\cdot(q-1)$ genügt („ggT" steht für größter gemeinsamer Teiler). Nach der Wahl von d und der Berechnung von e müssen die Werte p, q und $(p-1)\cdot(q-1)$ gelöscht werden. Welche der beiden Zahlen e und d der öffentliche und welche der private Schlüssel ist, ist bei RSA grundsätzlich frei wählbar; in dieser Erfindung berechnen die Funktionen f und g aus der Benutzerkennung pw und dem Zufallswert z den weiteren ersten Datenobjektschlüssel d. Über den erweiterten euklidschen Algorithmus wird dann aus dem weiteren ersten Datenobjektschlüssel d der weitere zweite Datenobjektschlüssel e berechnet.

[0037] Die Vorteile des RSA-Verfahrens sind die Tatsachen, dass das Verfahren bei entsprechend lang gewählten Schlüsseln nach wie vor sehr sicher ist und dass es eine hohe Verbreitung besitzt. Jedoch besitzt RSA auch die Nachteile, dass es aufgrund der erforderlichen großen Schlüssellänge im Betrieb langsam ist und moderne Faktorisierungsalgorithmen Anlass zu der Befürchtung geben, dass RSA in nicht allzu ferner Zukunft gebrochen wird.

[0038] Auch für RSA ist es über die Funktionen f und g möglich, aus der Benutzerkennung und dem Zufallswert den weiteren ersten Datenobjektschlüssel zu berechnen. Damit ist es auch für RSA möglich, durch mathematische Funktionen der gewählten Benutzerkennung ein kryptografisches Schlüsselpaar zuzuordnen. Wegen dieses funktionellen Zusammenhangs ist ein Vorhalten einer tabellarischen Zuordnung von Schlüsselpaar und einer entsprechenden Benutzerkennung auch für RSA nicht notwendig.

[0039] Nach einem weiteren Aspekt der Erfindung

umfasst das Verfahren den Schritt der Zulässigkeitsprüfung des ersten RSA-Datenobjektschlüssels. Im Rahmen der Zulässigkeitsprüfung wird geprüft, ob der weitere erste Datenobjektschlüssel d die Bedingungen

- d liegt im Intervall [2, (p – 1)·(q – 1) – 2] und
-

ggT(d, (p – 1)·(q – 1)) = 1

erfüllt. Bei Erfüllung dieser Prüfbedingungen sind der Zufallswert sowie der erste und der weitere zweite Datenobjektschlüssel zulässig. Ist die Prüfbedingung jedoch nicht erfüllt, wird ein neuer Zufallswert z gewählt, mit dem ein erneutes Berechnen des weiteren ersten Datenobjektschlüssels erfolgt sowie ein erneutes Durchführen der Zulässigkeitsprüfung dieses Datenobjektschlüssels. Dieser Vorgang wird wiederholt, bis die Zulässigkeitsprüfung bestanden wird.

[0040] Nach einer weiteren Ausführungsform der Erfindung wird der Zufallswert von einer Datenbank abgerufen, wobei der Zufallswert eindeutig der Benutzeridentifikation zugeordnet ist. Beispielsweise wird bei einer ersten Durchführung des Verfahrens zur Erzeugung des asymmetrischen Schlüsselpaares einmalig ein Zufallswert von einer vertrauenswürdigen Stelle, z. B. einer Zertifizierungsstelle erzeugt, welcher im Falle der Zulässigkeit des weiteren ersten Datenobjektschlüssels für kryptografische Vorgänge einem entsprechenden Benutzer indirekt zugänglich sein muss. Durch Abspeichern des Zufallswerts in einer Datenbank, zugeordnet der eindeutigen Benutzeridentifikation, kann ein Computerprogramm, welches das Verfahren zur Erzeugung von asymmetrischen Schlüsselpaaren ausführt, den Zufallswert über eine sichere Kommunikationsverbindung anhand der Benutzeridentifikation abrufen und dazu verwenden, den entsprechenden ersten und gegebenenfalls auch den weiteren zweiten Datenobjektschlüssel zu generieren.

[0041] Vorzugsweise ist der Zufallswert verschlüsselt in der Datenbank abgelegt. Hierzu kann nach einer Ausführungsform der Erfindung eine symmetrische Verschlüsselung, z. B. unter Verwendung von AES-256, Anwendung finden. Die Verwendung eines verschlüsselten Zufallswertes hat den Vorteil, dass damit Wörterbuchangriffe zur versuchsweisen Entschlüsselung des ersten Schlüssels verhindert werden können.

[0042] Nach einer weiteren Ausführungsform der Erfindung sind die Computerprogrammprodukte durch Applets oder Browser Plugins ausgebildet. Ebenso ist es möglich, die Computerprogrammprodukte als eigenständige Anwendungen für ein Datenverarbeitungssystem bereitzustellen. Die Verwendung eines Applets oder eines Browser Plugins hat den Vorteil, dass bestehende Datenverarbeitungssysteme zur Durchführung des Verfahrens zur Schlüsselerzeugung und konsequenter Weise auch zur Durchführung von kryptografischen Operationen wie Verschlüsselung, Entschlüsselung sowie Erstellung und Verifikation von digitalen Signaturen, nicht umgerüstet werden müssen: Hier genügt lediglich das Laden eines Applets, beispielsweise über das Internet, welches in sicherer Weise die beschriebenen Operationen durchführen kann.

[0043] Nach einer weiteren Ausführungsform der Erfindung wird das weitere asymmetrische kryptografische Schlüsselpaar von einem tragbaren Datenträger empfangen, wobei das Chiffrat auf dem tragbaren Datenträger gespeichert wird. Beispielsweise handelt es sich bei dem tragbaren Datenträger um eine Chipkarte, ein Ausweisdokument oder um ein mobiles Telekommunikationsgerät wie ein Mobiltelefon oder ein Personal Digital Assistant (PDA).

[0044] In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Entschlüsselung eines Datenobjekts, wobei das Datenobjekt über einen initialen ersten Berechtigungsschlüssel entschlüsselbar ist, wobei der initiale erste Berechtigungsschlüssel zusammen mit einem initialen zweiten Berechtigungsschlüssel ein initiales asymmetrisches kryptografisches Schlüsselpaar bildet, wobei das initiale asymmetrische Schlüsselpaar Teil einer Schlüsselpaarsequenz ist. Das Verfahren umfasst dabei die Schritte des Zugriffs auf einen ersten Berechtigungsschlüssel, wobei der erste Berechtigungsschlüssel zusammen mit einem zweiten Berechtigungsschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bildet, wobei das asymmetrische Schlüsselpaar Teil der Schlüsselpaarsequenz ist. Daraufhin erfolgt das Abrufen eines Chiffrats, wobei das Chiffrat dem asymmetrischen kryptografischen Schlüsselpaar zugeordnet ist, wobei das Chiffrat den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel umfasst. Es erfolgt das Entschlüsseln des verschlüsselten initialen ersten Schlüssels mit dem ersten Berechtigungsschlüssel und das Entschlüsseln des verschlüsselten Datenobjekts über den entschlüsselten initialen ersten Schlüssel.

[0045] Wie bereits oben erwähnt, hat dieses Verfahren den Vorteil, dass eine Entschlüsselung des verschlüsselten Datenobjektes unter Verwendung eines beliebigen asymmetrischen Schlüsselpaares durchgeführt werden kann, welches Teil der Schlüsselpaarsequenz ist. Es spielt hierbei keine Rolle, mit welchem asymmetrischen Schlüsselpaar des Satzes von asymmetrischen Schlüsselpaaren der Schlüsselpaarsequenz zuvor eine Verschlüsselung des Datenobjekts erfolgt ist. Abhängig von dem zur Entschlüsselung nun verwendeten asymmetrischen kryptografischen Schlüsselpaar wird ein entsprechendes Chif-

frat abgerufen, mittels welchem der initiale erste Schlüssel extrahiert werden kann, unter Verwendung dessen schließlich das Datenobjekt entschlüsselt werden kann.

[0046] Nach einer weiteren Ausführungsform der Erfindung umfasst das Computerprogrammprodukt ferner Instruktionen zur Durchführung des Schritts des Empfangens einer dem asymmetrischen kryptografischen Schlüsselpaar zugeordneten Schlüsselpaarkennung, wobei das Chiffrat anhand der Schlüsselpaarkennung abgerufen wird. Beispielsweise wird das Chiffrat von einer Datenbank abgerufen. Alternativ dazu ist es zum Beispiel möglich, dass das asymmetrische Schlüsselpaar zusammen mit dem Chiffrat auf einem tragbaren Datenträger, wie zum Beispiel einer Chipkarte, gespeichert ist.

[0047] Nach einer weiteren Ausführungsform der Erfindung umfasst das Computerprogrammprodukt ferner Instruktionen zur Durchführung des Schritts einer Signaturüberprüfung des Datenobjekts, wobei die Signaturüberprüfung die Schritte umfasst des Lesens einer dem Datenobjekt zugeordneten Signatur und der Verifizierung der Signatur des Datenobjekts, wobei die Verifikation mit dem zweiten Berechtigungsschlüssel erfolgt.

[0048] Die Durchführung einer zusätzlichen Signaturüberprüfung im Falle einer zuvor erfolgten Signierung des Datenobjekts mit dem ersten Berechtigungsschlüssel hat den Vorteil, dass hiermit verifiziert werden kann, dass das Datenobjekt seit dem ursprünglichen Verschlüsselungsvorgang nicht unbefugt modifiziert wurde.

[0049] Nach einer weiteren Ausführungsform der Erfindung ist das Datenobjekt mit einem symmetrischen Datenobjektschlüssel verschlüsselt, wobei der symmetrische Datenobjektschlüssel mit dem initialen zweiten Berechtigungsschlüssel verschlüsselt ist, wobei das Entschlüsseln des verschlüsselten Datenobjekts in diesem Fall den weiteren Schritt umfasst des Entschlüsselns des verschlüsselten symmetrischen Datenobjektschlüssels mit dem entschlüsselten initialen ersten Berechtigungsschlüssel und dem Entschlüsseln des verschlüsseltes Datenobjekts mit dem entschlüsselten symmetrischen Schlüssel.

[0050] Die zusätzliche Verwendung des symmetrischen Datenobjektschlüssels zur Verschlüsselung des Datenobjekts hat den Vorteil, dass ...

[0051] Nach einer weiteren Ausführungsform der Erfindung umfasst der Zugriff auf den ersten Berechtigungsschlüssel den Schritt des Empfangens einer Benutzeridentifikation und einer der Benutzeridentifikation zugeordneten Benutzerkennung. Dem folgen das Abrufen eines der Benutzeridentifikation zugeordneten Zufallswerts von einer weiteren Datenbank und das Berechnen des ersten Berechtigungsschlüssels, wobei in die Berechnung der Zufallswert und die Benutzerkennung eingehen.

[0052] Nach einer weiteren Ausführungsform der Erfindung umfasst die Signaturüberprüfung ferner den Schritt des Berechnens des zweiten Berechtigungsschlüssels aus dem ersten Berechtigungsschlüssel mittels eines asymmetrischen kryptografischen Schlüsselerzeugungsverfahrens, wobei der erste und der zweite Berechtigungsschlüssel das asymmetrische kryptografische Schlüsselpaar bilden.

[0053] Nach einer weiteren Ausführungsform der Erfindung wird der Zufallswert über eine sichere Kommunikationsverbindung von der weiteren Datenbank abgerufen. Dabei ist es möglich, dass die Datenbank, von welcher das Chiffrat abgerufen wird, und von welcher der Zufallswert abgerufen wird, identisch ist.

[0054] Nach einer weiteren Ausführungsform der Erfindung ist der Zufallswert verschlüsselt in der weiteren Datenbank abgespeichert.

[0055] Nach einer weiteren Ausführungsform der Erfindung handelt es sich bei dem Datenobjekt um ein medizinisches Datenobjekt.

[0056] In einem weiteren Aspekt betrifft die Erfindung ein Computerprogrammprodukt mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Erzeugung einer digitalen Signatur eines Datenobjekts, wobei das Verfahren den Empfang der Benutzeridentifikation und einer der Benutzeridentifikation zugeordneten Benutzerkennung umfasst. Ferner umfasst das Verfahren das Abrufen eines der Benutzeridentifikation zugeordneten Zufallswertes von einer zweiten Datenbank. Es folgt das Berechnen eines weiteren ersten Datenobjektschlüssels, wobei in die Berechnung der Zufallswert und die Benutzerkennung eingehen, wobei der weitere erste und der weitere zweite Datenobjektschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden. Nach der Berechnung des weiteren ersten Datenobjektschlüssels erfolgt die Erzeugung der digitalen Signatur, in die der weitere erste Datenobjektschlüssel und beispielsweise der kryptografische Hash-Wert des Datenobjekts einfließen. Die digitale Signatur wird zusammen mit der Kennung des Datenobjekts in der ersten Datenbank abgespeichert.

[0057] In einem weiteren Aspekt betrifft die Erfindung ein Datenverarbeitungssystem zur Bereitstellung von Berechtigungsschlüsseln, wobei das Datenverarbeitungssystem Mittel zum Empfang eines weiteren asymmetrischen kryptografischen Schlüsselpaares umfasst, wobei das weitere asymmetrische

Schlüsselpaar Teil einer Schlüsselpaarsequenz ist, wobei das weitere asymmetrische Schlüsselpaar einen weiteren ersten und einen weiteren zweiten Berechtigungsschlüssel umfasst. Das Datenverarbeitungssystem umfasst ferner Mittel zum Abrufen eines Chiffrats, wobei das Chiffrat dem Schlüsselpaar zugeordnet ist, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, wobei das Chiffrat den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, umfasst. Das Datenverarbeitungssystem umfasst ferner Mittel zum Verschlüsseln des initialen ersten Berechtigungsschlüssels mit dem ersten Berechtigungsschlüssel des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht und Mittel zum Erzeugen eines weiteren Chiffrats durch Verschlüsseln des entschlüsselten initialen ersten Berechtigungsschlüssels mit dem zweiten Berechtigungsschlüssel des weiteren Schlüsselpaars. Ferner umfasst das Datenverarbeitungssystem Mittel zur Speicherung des weiteren Chiffrats.

[0058] Vorzugsweise handelt es sich bei dem Datenverarbeitungssystem um ein Datenverarbeitungssystem einer vertrauenswürdigen Stelle, z. B. einer Zertifizierungsstelle oder eines Trust-Centers. Alternativ ist es auch möglich, eine entsprechende, vorzugsweise portable Hardwareeinheit bereitzustellen, welche als vertrauenswürdige Stelle das Datenverarbeitungssystem umfasst. In einer weiteren Alternative kann es sich bei der vertrauenswürdigen Stelle um den Client selbst handeln, welcher die kryptografischen Operationen vornimmt.

[0059] Nach einer weiteren Ausführungsform der Erfindung handelt es sich bei dem Datenverarbeitungssystem um ein Datenverarbeitungssystem, das auf einem separaten, gesicherten Hardwaremodul abläuft. Hierbei kann z. B. ein Trusted Platform Module (TPM) zum Einsatz kommen.

[0060] Im Folgenden werden Ausführungsformen der Erfindung anhand von Zeichnungen näher erläutert. Es zeigen:

[0061] Fig. 1: ein Blockdiagramm eines Datenverarbeitungssystems,

[0062] Fig. 2: ein Flussdiagramm eines Verfahrens zur Bereitstellung von Berechtigungsschlüsseln und zur Verschlüsselung von Daten,

[0063] Fig. 3: ein Flussdiagramm eines Verfahrens zur Entschlüsselung von Daten,

[0064] Fig. 4: ein Flussdiagramm eines Verfahrens zur asymmetrischen Verschlüsselung von Daten,

[0065] Fig. 5: ein Flussdiagramm eines Verfahrens zur Entschlüsselung von Daten mittels eines asymmetrischen Schlüsselverfahrens,

[0066] Fig. 6: ein Flussdiagramm eines Verfahrens zur Berechnung von asymmetrischen Schlüsseln nach dem RSA-Verfahren,

[0067] Fig. 7: ein weiteres Flussdiagramm eines Verfahrens zur hierarchischen Bereitstellung von Berechtigungsschlüsseln und zur Verschlüsselung von Daten,

[0068] Fig. 8: ein weiteres Flussdiagramm zum Entschlüsseln von Datenobjekten.

[0069] Die Fig. 1 zeigt ein Datenverarbeitungssystem **100**. Das Datenverarbeitungssystem umfasst Eingabemittel **102**, wie zum Beispiel eine Tastatur, eine Maus, ein Pin-pad, Mittel zur Erfassung von biometrischen Merkmalen, wie zum Beispiel einen Fingerabdruckscanner oder einen Irisscanner. Ferner umfasst das Datenverarbeitungssystem **100** einen Bildschirm **104** sowie eine Schnittstelle **106**, welche zum Beispiel zur Kommunikation mit einem Netzwerk **120**, wie dem Internet, verwendet werden kann. Ferner umfasst das Datenverarbeitungssystem **100** einen Prozessor **108**, welcher dazu ausgebildet ist, ausführbare Instruktionen zur Durchführung von Verfahrensschritten auszuführen. Diese Instruktionen sind beispielsweise in Form eines Applets **112** im Speicher **110** enthalten.

[0070] Beispielsweise kann das Datenverarbeitungssystem **100** zur Erzeugung von asymmetrisch kryptografischen Schlüsselpaaren und zur anschließenden Verschlüsselung und Entschlüsselung von Datenobjekten sowie zur Erzeugung und Verifikation von digitalen Signaturen und für weitere kryptografische Operationen verwendet werden. Dies erfordert zunächst eine Berechnung von Schlüsselpaaren, was beispielsweise mittels des Moduls **114** des Applets **112** erfolgen kann. Zur Berechnung von Schlüsseln wird hierbei mittels des Moduls **114** wie folgt vorgegangen: Über die Eingabemittel **102** wird zunächst eine beliebig wählbare Benutzerkennung von einem Benutzer erhalten. Aus der Benutzerkennung wird daraufhin ein erster Datenobjektschlüssel berechnet, wobei in die Berechnung ein Zufallswert, welcher durch das Datenverarbeitungssystem **100** erzeugt wird, und die Benutzerkennung eingehen. Bei dem hier berechneten ersten Datenobjektschlüssel handelt es sich um einen privaten Schlüssel des Benutzers, wobei es möglich ist, dass zur Verwendung des ersten Datenobjektschlüssels in kryptografischen Anwendungen zusätzliche Parameter mit veröffentlicht werden müssen, um den ersten Datenobjektschlüssels für die Durchführung kryptografischer Operationen zu nutzen. Wie bereits oben angemerkt, ist es im Falle von elliptischen Kurven notwendig, zusätzlich

zum ersten und zweiten Datenobjektschlüssel auch die Domainparameter der elliptischen Kurve zur Verfügung zu stellen, welche in Kombination mit dem ersten und zweiten Datenobjektschlüssel die Anwendung kryptografischer Operationen möglich macht. Ähnlich gilt für RSA, dass die natürliche Zahl n mit veröffentlicht werden muss, um kryptografische Operationen durchführen zu können.

[0071] Nach Berechnung des ersten Datenobjektschlüssels erfolgt eine Prüfung des Datenobjektschlüssels mittels des Prüfmoduls **116**. Diese Prüfung dient einer Zulässigkeitsprüfung des ersten Datenobjektschlüssels, nämlich, ob der erzeugte erste Datenobjektschlüssel verschiedenen Sicherheitsaspekten genügt.

[0072] Beispielsweise wird bei elliptischen Kurven der öffentliche Schlüssel, d. h. der zweite Datenobjektschlüssel, aus dem ersten privaten Datenobjektschlüssel berechnet, indem ein Kurvenpunkt einer elliptischen Kurve mit dem geheimen Schlüssel multipliziert wird. In diesem Fall besteht die Zulässigkeitsprüfung des ersten Datenobjektschlüssels darin, zu prüfen, ob der erste Datenobjektschlüssel größer als 1 und kleiner als die Ordnung der elliptischen Kurve ist, wobei bei Erfüllung dieser Prüfbedingung der Zufallswert und der erste und zweite Datenobjektschlüssel zulässig sind. Ist dies jedoch nicht der Fall, muss ein neuer erster Datenobjektschlüssel und folglich auch ein neuer zweiter Datenobjektschlüssel berechnet werden, indem ein neuer Zufallswert gewählt wird und das Verfahren zur Schlüsselberechnung mittels des Moduls **114** sowie das Verfahren zur Prüfung der erzeugten Schlüssel mittels des Moduls **116** wiederholt durchgeführt wird.

[0073] Der zur Schlüsselberechnung verwendete Zufallswert wird daraufhin in einer Datenbank **132** abgelegt und gegebenenfalls verschlüsselt. Dies erfolgt beispielsweise so, dass für den entsprechenden Benutzer eine eindeutige Benutzeridentifikation vergeben wird, wobei dieser Benutzeridentifikation **124** in einer Tabelle der Datenbank **132** der zuvor erzeugte Zufallswert **128** zugeordnet wird. Im vorliegenden Beispiel der **Fig. 1** ist der Benutzerkennung „abc" der Zufallswert Z mit dem Wert „12345" zugeordnet. Wie bereits oben erwähnt, wird hier vorzugsweise der Zufallswert in verschlüsselter Form in der Datenbank **132** gespeichert, um zuverlässig Wörterbuchangriffe auf den ersten Datenobjektschlüssel zu verhindern.

[0074] In einer weiteren Datenbank **122** ist ebenfalls der Benutzeridentifikation **124** der mittels des Schlüsselberechnungsmoduls **114** erzeugte öffentliche Schlüssel **126** zugeordnet abgespeichert. Beispielsweise ist wiederum der Benutzeridentifikation „abc" der öffentliche Schlüssel „1FF42B7" zugeordnet.

[0075] Im Folgenden sei angenommen, dass in einer Datenbank **134** ebenfalls der Benutzeridentifikation **124** zugeordnet ein Datenobjekt **130** verschlüsselt gespeichert ist. Das Datenobjekt ist dabei mit dem öffentlichen Schlüssel **126** verschlüsselt, welcher in der Datenbank **122** abgelegt ist. Zur Entschlüsselung des Datenobjekts **130** wird nun wie folgt vorgegangen: Über die Eingabemittel **102** gibt ein Benutzer seine Benutzeridentifikation und die in der Benutzeridentifikation gewählte Benutzerkennung ein. Daraufhin erfolgt mittels des Moduls **114** die Berechnung des ersten Datenobjektschlüssels unter Verwendung des Zufallswertes **128**, welcher anhand der Benutzeridentifikation **124** von der Datenbank **132** abgerufen wird. In diese Berechnung des ersten Datenobjektschlüssels gehen, wie bereits oben erwähnt, der Zufallswert **128** und die Benutzerkennung ein, welche zuvor über die Eingabemittel **102** in das Datenverarbeitungssystem eingegeben wurde.

[0076] Mittels des nun so erzeugten geheimen und privaten Datenobjektschlüssels ist es nun möglich, das Datenobjekt **130** zu entschlüsseln.

[0077] In einer Datenbank **135** kann zumindest eine Signatur **131** S_Objekt 1 des Datenobjekts sowie optional das Datenobjekt **130** selbst gespeichert sein. Das Datenobjekt **130** ist dabei mit dem geheimen Schlüssel signiert, welcher dem öffentlichen Schlüssel **126** zugeordnet ist. Die Verifikation der Signatur erfolgt dementsprechend mit dem öffentlichen Schlüssel **126**.

[0078] An dieser Stelle sei angemerkt, dass die beliebig wählbare Benutzerkennung, welche über die Eingabemittel **102** in das Datenverarbeitungssystem **100** eingegeben wird, beispielsweise eine Zahlenkombination, eine Zahlen-Buchstaben-Kombination oder auch ein biometrisches Merkmal sein kann. Beispielsweise kann im Falle der Verwendung eines biometrischen Merkmals aus den biometrischen Daten eine Bitfolge in eindeutiger Weise berechnet werden, welche daraufhin als Benutzerkennung in die Schlüsselberechnung mittels des Moduls **114** eingehen kann.

[0079] Ferner sei angemerkt, dass insbesondere bei der Ver- und Entschlüsselung von medizinischen Datenobjekten durch das Datenverarbeitungssystem **100** beispielsweise wie folgt vorgegangen wird: Über die Schnittstelle **106** wird beispielsweise ein medizinisches Datenobjekt von einem bildgebenden medizinischen instrument wie einem Röntgengerät empfangen. Röntgendaten sind typischerweise Bilddaten, welche umfangreiche Datenmengen darstellen. Das Datenverarbeitungssystem erzeugt einen zufälligen symmetrischen Schlüssel, mit welchem diese medizinischen Röntgendaten verschlüsselt werden. Daraufhin werden diese verschlüsselten Daten auf der Datenbank **134** mit der eindeutigen Benutzeridentifikation **124** assoziiert abgelegt. Daraufhin er-

folgt eine Verschlüsselung des erzeugten symmetrischen Schlüssels mit dem öffentlichen Schlüssel **126**. Dieser so verschlüsselte symmetrische Schlüssel wird ebenfalls auf der Datenbank **134** mit der Benutzeridentifikation **124** und den verschlüsselten Daten assoziiert abgelegt.

[0080] Zur Entschlüsselung wird nun der verschlüsselte symmetrische Schlüssel mittels des Kryptografiemoduls **118** entschlüsselt, indem der entsprechende private Schlüssel unter Verwendung der Benutzerkennung wie oben beschrieben erzeugt und für die Entschlüsselung verwendet wird. Mit dem so erhaltenen symmetrischen Schlüssel ist es daraufhin möglich, das verschlüsselte Datenobjekt **130** zu entschlüsseln.

[0081] Vorzugsweise werden Datenobjekte **130** in der Datenbank **134** jeweils einzeln verschlüsselt abgespeichert. Selbst im Falle eines Satzes von semantisch zusammengehörenden Datenobjekten wird vorzugsweise jedes einzelne Datenobjekt für sich verschlüsselt in der Datenbank **134** abgespeichert, so dass im Falle eines Abrufens eines einzelnen Datenobjekts eine Übertragung dieses verschlüsselten Datenobjekts **130** an das Datenverarbeitungssystem **100** erfolgt, woraufhin dort seine Entschlüsselung vorgenommen wird. Würde man im Gegensatz dazu für semantisch zusammengehörende Datenobjekte, die in einem einzigen Datenobjekt zusammengefasst, verschlüsselt und abgespeichert wären, aus Gründen der Minimierung des zu transportierenden Datenvolumens die Entschlüsselung in der Datenbank vornehmen, so hätte der Betreiber Zugriff auf die entschlüsselten Datenobjekte. Dahingegen hat die oben beschriebene Vorgehensweise den Vorteil, dass zu keinem Zeitpunkt die Datenbank **134**, bzw. deren Betreiber Zugriff auf entschlüsselte Schlüssel oder Datenobjekte erhält.

[0082] Das Datenverarbeitungssystem **100** ist ferner dazu ausgebildet, um Berechtigungsschlüssel in hierarchischer Weise bereitzustellen und diese zur Ver- und Entschlüsselungsvorgängen von Datenobjekten zu verwenden. Im Folgenden sei ohne Beschränkung der Allgemeinheit angenommen, dass beispielsweise ein Benutzer im Besitz einer Chipkarte **152** ist, auf welcher ein privater Berechtigungsschlüssel **154** und ein öffentlicher Berechtigungsschlüssel **156** abgespeichert ist. Soll nun ein neues Datenobjekt verschlüsselt werden, kann hierfür das obig beschriebene Verfahren unter Verwendung eines zusätzlichen symmetrischen Schlüssels zum Einsatz kommen, mit welchem ein Datenobjekt verschlüsselt wird. Das so mit dem symmetrischen Schlüssel verschlüsselte Datenobjekt **130** wird zusammen mit der eindeutigen Benutzeridentifikation **124** assoziiert in der Datenbank **134** abgelegt.

[0083] Abweichend von obiger Beschreibung erfolgt jedoch nach einer weiteren Ausführungsform der Erfindung nun eine Verschlüsselung des symmetrischen Schlüssels mit einem initialen öffentlichen Schlüssel, welcher beispielsweise in der Datenbank **122** als initialer öffentlicher Schlüssel **126** abgelegt ist. Außerdem ist beispielsweise ebenfalls auf der Datenbank **122** ein Chiffrat **150** abgelegt. Dieses Chiffrat **150** ist dabei eindeutig der Chipkarte **152** zuordenbar.

[0084] Findet nun ein solcher Verschlüsselungsvorgang des obig erwähnten symmetrischen Schlüssels statt, wird zunächst der eindeutigen Benutzeridentifikation **124** zugeordnete initiale Berechtigungsschlüssel in Form eines öffentlichen Schlüssels **126** von der Datenbank **122** abgerufen. Mittels des Kryptografiemoduls **118** erfolgt daraufhin eine Verschlüsselung des symmetrischen Schlüssels mit dem initialen öffentlichen Berechtigungsschlüssel. Dieser verschlüsselte symmetrische Schlüssel wird daraufhin in der Datenbank **134** mit dem verschlüsselten Datenobjekt **130** assoziiert abgelegt.

[0085] Für einen Entschlüsselungsvorgang des verschlüsselten Datenobjektes **130** wird eine Entschlüsselung des symmetrischen Datenobjektschlüssels benötigt. Dies erfordert die Kenntnis des privaten initialen Berechtigungsschlüssels, welche zusammen mit dem initialen öffentlichen Berechtigungsschlüssel ein asymmetrisches kryptografisches Schlüsselpaar bildet. Zum Erhalt des privaten initialen Berechtigungsschlüssels dient nun das Chiffrat **150**, welches der Chipkarte **152** zugeordnet ist. Das Chiffrat enthält in verschlüsselter Weise den initialen privaten Berechtigungsschlüssel, welcher mit dem öffentlichen Berechtigungsschlüssel **156** der Chipkarte **152** zuvor verschlüsselt wurde. Unter Verwendung der Schnittstelle **106** ist nun das Kryptografiemodul **118** in der Lage, aus dem Chiffrat **150** unter Verwendung des privaten Berechtigungsschlüssels **154** der Chipkarte **152** den initialen privaten Berechtigungsschlüssel zu extrahieren. Mittels dieses initialen privaten Berechtigungsschlüssels ist daraufhin das Kryptografiemodul **118** in der Lage, den verschlüsselten symmetrischen Schlüssel, welcher mit dem verschlüsselten Datenobjekt **130** assoziiert ist, zu entschlüsseln, um daraufhin mit dem so erhaltenen symmetrischen Schlüssel das verschlüsselte Datenobjekt **130** selbst zu entschlüsseln.

[0086] Nun sei angenommen, dass ein Benutzer der Chipkarte **152** diese Chipkarte durch eine neue Chipkarte **160** ersetzen möchte, bzw. neben der Chipkarte **152** eine zusätzliche Chipkarte **160** zur Durchführung von Ver- und Entschlüsselungsvorgängen von Datenobjekten einsetzen möchte. Dies erfordert eine hierarchische Bereitstellung von Berechtigungsschlüsseln, was wie folgt geschieht:
Es sei angenommen, dass sich auf der Chipkarte **160** bereits ein neuer privater Berechtigungsschlüssel

162 und ein neuer öffentlicher Berechtigungsschlüssel **164** befinden. Angemerkt sei hier, dass sich dieses Vorhandensein von Berechtigungsschlüsseln **162** und **164** auf einer Chipkarte **160** ohne Weiteres durch das obig beschriebene Verfahren zur Erzeugung von Datenobjektschlüsseln ersetzen lässt, welche mittels einer beliebig wählbaren Benutzerkennung in das Datenverarbeitungssystem **100** eingegeben werden. Im letzteren Fall würde die Chipkarte **160** wegfallen – ein Bereitstellen von Datenobjektschlüsseln würde unter Verwendung der besagten Benutzerkennung durch das Datenverarbeitungssystem **100** selbst erfolgen. Im Folgenden sei jedoch angenommen, dass ohne Beschränkung der Allgemeinheit ein Benutzer zusätzlich die Chipkarte **160** mit den Berechtigungsschlüsseln **162** und 164 zum Einsatz bringen möchte. Hierzu werden nach einer bevorzugten Ausführungsform der Erfindung entweder in einer vom Datenverarbeitungssystem mittels des Bildschirms angegebenen Reihenfolge die Chipkarten **152** und **160** in ein entsprechendes Lesegerät des Datenverarbeitungssystems **100** eingeführt, oder aber das Datenverarbeitungssystem **100** ist in der Lage, gleichzeitig beide Chipkarten **152** und **160** zu lesen. Im Folgenden sei angenommen, dass ein gleichzeitiger Zugriff auf die Chipkarten **152** und **160** möglich ist.

[0087] Nachdem ein Benutzer die beiden Chipkarten **152** und **160** in entsprechende Lesegeräte des Datenverarbeitungssystems **100** eingeführt hat, liest das Datenverarbeitungssystem **100** das Chiffrat **150** aus der Datenbank **122** aus, welches der „alten Chipkarte" **152** zugeordnet war. Wie bereits oben im Detail beschrieben, ist damit das Datenverarbeitungssystem **100** in der Lage, den initialen privaten Berechtigungsschlüssel aus dem Chiffrat unter Verwendung des privaten Berechtigungsschlüssels **154** zu extrahieren. Der so gewonnene initiale private Berechtigungsschlüssel wird daraufhin mit dem öffentlichen Berechtigungsschlüssel **164** der neuen Chipkarte **160** verschlüsselt. Dieser verschlüsselte initiale Berechtigungsschlüssel bildet wiederum ein neues Chiffrat **150**, welches mit der Chipkarte **160** assoziiert in der Datenbank **122** abgelegt wird. Die Chiffratberechnung erfolgt dabei mit dem Modul **114**.

[0088] Eine Verschlüsselung von Daten erfolgt nun wie obig im Detail beschrieben unter Verwendung des symmetrischen Schlüssels, welcher grundsätzlich, unabhängig vom Einsatz der Chipkarte **152** oder **160** mit dem initialen öffentlichen Schlüssel **126** verschlüsselt und mit dem entsprechenden verschlüsselten Datenobjekt **130** assoziiert in der Datenbank **134** abgelegt wird. Erfolgt nun in umgekehrter Reihenfolge ein Entschlüsselungsvorgang eines verschlüsselten Datenobjektes **130**, so kann dies entweder unter Verwendung der Chipkarte **152** oder der Chipkarte **160** erfolgen. In beiden Fällen wird jeweils der Chipkarte zugeordnete private Schlüssel **154** bzw. 162 dazu verwendet, um das der jeweilig verwendeten Chipkarte zugeordnete Chiffrat zu entschlüsseln. Der so erhaltene initiale private Schlüssel kann nun wiederum dazu verwendet werden, um einen Entschlüsselungsvorgang des symmetrischen Datenobjektschlüssels vorzunehmen, welcher mit dem verschlüsselten Datenobjekt **130** in der Datenbank **134** assoziiert abgelegt ist.

[0089] Es sei hier darauf hingewiesen, dass vorzugsweise die privaten Schlüssel **154** und **162** nie die Chipkarten **152** und **160** verlassen. Aus diesem Grund weisen die Chipkarten **152** und **160** entsprechende Hardware- oder Softwaremodule **158** bzw. **166** auf, mit welchen entsprechende Kryptografievorgänge, wie beispielsweise Entschlüsselungsvorgänge des Chiffrats **150** vorgenommen werden können. Ebenfalls sollte vorzugsweise eine Verschlüsselung des initialen privaten Schlüssels in den Modulen **158** bzw. 166 selbst erfolgen, sodass der durch die Chipkarten **152** und **160** extrahierte initiale erste Berechtigungsschlüssel nie diese Chipkarten verlässt, sodass ein Missbrauch des initialen privaten Berechtigungsschlüssels ausgeschlossen ist.

[0090] Die Fig. 2 zeigt ein Verfahren zur Durchführung von Verfahrensschritten zur Bereitstellung von Berechtigungsschlüsseln als auch zur Verschlüsselung eines Datenobjekts. Das Verfahren beginnt im Schritt **200**, in welchem ein neuer privater Schlüssel G_i und öffentlicher Schlüssel O_i erzeugt wird. Dies kann beispielsweise durch Wahl einer neuen Benutzerkennung wie obig beschrieben oder durch Bereitstellung einer neuen Chipkarte erfolgen, in welcher bereits ein neuer privater Berechtigungsschlüssel G_i und ein neuer öffentlicher Berechtigungsschlüssel O_i eingespeichert ist. In Schritt **202** wird überprüft, ob ein initialer privater Berechtigungsschlüssel mit Index i = 0 verfügbar ist. Typischerweise wird dies lediglich dann der Fall sein, wenn bisher außer dem initialen privaten Berechtigungsschlüssel und dem zugehörigen initialen öffentlichen Berechtigungsschlüssel keine weiteren asymmetrischen kryptographischen Schlüsselpaare erzeugt wurden. Allerdings sei im Folgenden auch hier wieder ohne Beschränkung der Allgemeinheit angenommen, dass bereits ein Satz von verschiedenen asymmetrischen Schlüsselpaaren existiert, welche Teil einer Schlüsselpaarsequenz sind. Dementsprechend existieren zum Zeitpunkt der Erzeugung des privaten Schlüssels G_i und des öffentlichen Schlüssels O_i insgesamt außerdem dem initialen Schlüsselpaar i – 1 weitere asymmetrische kryptografische Schlüsselpaare.

[0091] Es sei angenommen, dass der initiale private Berechtigungsschlüssel mit Index 0 G_0 nicht verfügbar ist, sodass nach Schritt **202** der Schritt **204** erfolgt, in welchem ein Chiffrat, welches der Chipkarte mit Index i – 1 zugeordnet ist, von einer Datenbank abgerufen wird. Alternativ ist es auch möglich, dass

dieses Chiffrat auf der Chipkarte, welches dem Index i – 1 zugeordnet ist, abgespeichert ist.

[0092] Daraufhin wird in Schritt **206** unter Verwendung des privaten Berechtigungsschlüssels der Chipkarte mit Index i – 1 das Chiffrat entschlüsselt. Durch Entschlüsseln des Chiffrats erhält man in Schritt **206** den initialen privaten Berechtigungsschlüssel. Dieser initiale private Berechtigungsschlüssel G_0 wird daraufhin in Schritt **208** erneut verschlüsselt, wobei hier eine Verschlüsselung unter Verwendung des neuen öffentlichen Schlüssels O_i stattfindet. Das so erhaltene neue Chiffrat wird in Schritt **210** der neuen Chipkarte zugeordnet in einer Datenbank abgespeichert.

[0093] Der direkte Übergang von Schritt **202** nach Schritt **208** ist üblicherweise nur dann notwendig, wenn die neue Chipkarte mit den Schlüsseln G_i und O_i die Chipkarte mit Index i = 1 ist.

[0094] Nachdem in den Schritten **200** bis **210** eine hierarchische Bereitstellung von Berechtigungsschlüsseln erfolgt ist, folgt in den Schritten **212** bis **234** ein Verschlüsselungsvorgang von Datenobjekten. In anderen Worten, müssen die Schritte **200** bis **210** lediglich einmalig bei Ausgabe einer neuen Chipkarte mit neuen asymmetrischen Schlüsseln durchgeführt werden, wohingegen die Schritte **212** bis **234** für jeden Verschlüsselungsvorgang von Datenobjekten durchgeführt werden müssen.

[0095] In Schritt **212** wird nun ein neues Datenobjekt erzeugt. Daraufhin erfolgt in Schritt **214** die Erzeugung eines symmetrischen Schlüssels s, welcher in Schritt **216** dazu verwendet wird, um das Datenobjekt des Schritts **212** zu verschlüsseln. In Schritt **218** erfolgt das Abrufen des initialen öffentlichen Berechtigungsschlüssels O_0 aus einer öffentlichen Datenbank, wobei in Schritt **230** dieser initiale öffentliche Berechtigungsschlüssel zur Verschlüsselung des symmetrischen Schlüssels, welcher in Schritt **214** erhalten wurde, verwendet wird.

[0096] Schließlich erfolgt eine Speicherung des verschlüsselten Datenobjektes und des verschlüsselten symmetrischen Schlüssels in einer entsprechenden Patientendatenbank in Schritt **234**.

[0097] Der Schritt **232**, welcher nach Schritt **230** folgt, ist ein optionaler Schritt, in welchem die Möglichkeit besteht, das Datenobjekt zusätzlich zu signieren, um so einem unbefugten Missbrauch und einer Manipulation des Datenobjektes vorzubeugen. Eine solche digitale Signierung erfolgt vorzugsweise mit dem privaten Berechtigungsschlüssel G_i der aktuell verwendeten Chipkarte. Wurde der Schritt **232** durchgeführt, wird die digitale Signatur zusätzlich in Schritt **234** zusammen mit dem verschlüsselten Datenobjekt und dem verschlüsselten symmetrischen Schlüssel abgespeichert.

[0098] Die Fig. 3 zeigt ein Flussdiagramm zum Entschlüsseln von Datenobjekten. Im Folgenden sei angenommen, dass dem Datenobjekt eine digitale Signatur hinzugefügt wurde. Damit erfolgt in Schritt **600** das Abrufen des verschlüsselten Datenobjektes, des verschlüsselten symmetrischen Schlüssels und der digitalen Signatur. In Schritt **602** wird überprüft, ob der initiale private Berechtigungsschlüssel verfügbar ist. Dies kann beispielsweise dann der Fall sein, wenn außer dem initialen Berechtigungsschlüssel keine weiteren Schlüssel in einer Sequenz ausgegeben wurden. Ist dies der Fall, wird in Schritt **610** dieser initiale private Berechtigungsschlüssel empfangen und in Schritt **612** erfolgt eine Entschlüsselung des verschlüsselten symmetrischen Datenobjektschlüssels mittels des initialen privaten Berechtigungsschlüssels. Dies ist möglich, da der symmetrische Datenobjektschlüssel s zuvor mit dem initialen öffentlichen Berechtigungsschlüssel O_0 verschlüsselt wurde, vgl. hierzu Schritt **230** der Fig. 2.

[0099] Nachdem in Schritt **612** der symmetrische Schlüssel entschlüsselt wurde, erfolgt daraufhin in Schritt **614** eine Entschlüsselung des Datenobjekts mit dem so erhaltenen symmetrischen Schlüssel s. In Schritt **616** wird überprüft, ob zu dem Datenobjekt eine Signatur verfügbar ist. Ist dies der Fall, erfolgt in Schritt **618** eine Signaturüberprüfung unter Verwendung des öffentlichen Berechtigungsschlüssels der Chipkarte, welche ursprünglich zur Signierung des Datenobjektes herangezogen wurde. Hierzu ist nicht zwingenderweise das Vorliegen dieser Chipkarte selbst notwendig, da der öffentliche Berechtigungsschlüssel dieser Chipkarte ohne Weiteres auf einem öffentlichen Server abgelegt sein kann.

[0100] Ergibt sich in Schritt **602**, dass der initiale private Berechtigungsschlüssel nicht verfügbar ist, typischerweise weil bereits eine Sequenz von zusätzlichen Berechtigungsschlüsseln bereitgestellt wurde, wird unter Verwendung eines beliebigen dieser Berechtigungsschlüsselpaare, welche augenblicklich zur Verfügung stehen, das Verfahren in Schritt **604** fortgesetzt. Im Folgenden sei angenommen, dass es sich hierbei um das Berechtigungsschlüsselpaar mit Index i handelt. Das Berechtigungsschlüsselpaar mit Index i umfasst einen privaten Berechtigungsschlüssel G_i, welcher in Schritt **604** empfangen wird. Daraufhin wird in Schritt **606** entweder aus der Chipkarte selbst, welche Träger des privaten Berechtigungsschlüssels i ist, ein entsprechendes diesem Index zugeordnetes Chiffrat C_{i_G0} abgerufen, oder das Abrufen dieses Chiffrats erfolgt in Schritt **606** von einer externen Datenbank. Daraufhin erfolgt in Schritt **608** eine Entschlüsselung dieses Chiffrats mit dem in Schritt **604** empfangenen privaten Berechtigungsschlüssels G_i. Dadurch erhält man in Schritt **608** den initialen privaten Berechtigungsschlüssel G_0. Dieser

initiale private Berechtigungsschlüssel G_0 kann daraufhin in Schritt **612** dazu verwendet werden, den verschlüsselten symmetrischen Schlüssel zu entschlüsseln. Anschließend folgen, wie bereits angesprochen, die Schritte **614** bis **620**, wobei in Schritt **620** das Verfahren endet.

[0101] Es sei hier noch angemerkt, dass in den Schritten **610** und **604** vom „Empfang" von privaten Schlüsseln die Rede ist. Dies soll jedoch nicht so verstanden werden, dass eine Übertragung der privaten Schlüssel über ein Medium, wie zum Beispiel ein Netzwerk, stattfindet. Vielmehr sollten vorzugsweise die Schritte **604** bis **612** bzw. **610** und **612** auf einer Chipkarte bzw. in einem Datenverarbeitungssystem selbst erfolgen, ohne dass ein unbefugter Benutzer dazu in der Lage ist, G_0 oder G_i in irgendeiner Weise abzufangen bzw. auszulesen.

[0102] Die Fig. 4 zeigt das Verfahren zur Erzeugung eines asymmetrischen Schlüsselpaares und seiner beispielhaften Verwendung zur Verschlüsselung von Datenobjekten und zur Verifikation digitaler Signaturen von Datenobjekten. In Schritt **300** wird eine eindeutige Benutzeridentifikation empfangen. Daraufhin erfolgt in Schritt **302** eine Überprüfung, ob ein öffentlicher Schlüssel existiert, welcher der in Schritt **300** empfangenen Benutzeridentifikation zugeordnet ist. Ist dies der Fall, wird in Schritt **304** überprüft, ob ein Zugriff auf diesen öffentlichen Schlüssel möglich ist. Ist dies möglich, wird in Schritt **306** der öffentliche Schlüssel abgerufen, und das Datenobjekt kann beispielsweise im Schritt **308** mittels des öffentlichen Schlüssels verschlüsselt werden oder es kann im Schritt **328** die digitale Signatur eines Datenobjekts verifiziert werden.

[0103] Ergibt die Prüfung in Schritt **304** hingegen, dass ein Zugriff auf den öffentlichen Schlüssel nicht möglich ist, dann muss der öffentliche Schlüssel erzeugt werden. Dies erfolgt beginnend mit Schritt **310**, in welchem entweder eine frei wählbare Benutzerkennung empfangen und die Funktion g auf diese Benutzerkennung angewendet wird oder es wird bereits der Wert g(Benutzerkennung) empfangen. Daraufhin folgt Schritt **312**, in welchem ein Zufallswert von einer entsprechenden Datenbank anhand der Benutzeridentifikation abgerufen wird. Durch Anwendung der Funktion f auf den Zufallswert und g(Benutzerkennung) erfolgt im Schritt **314** die Berechnung des privaten Schlüssels. Aus dem privaten Schlüssel wird schließlich in Schritt **316** der öffentliche Schlüssel berechnet, wobei der private und der öffentliche Schlüssel ein asymmetrisches kryptografisches Schlüsselpaar bilden.

[0104] Die Berechnung des öffentlichen Schlüssels im Schritt **316** erfolgt beispielsweise bei elliptischen Kurven dadurch, dass der öffentliche Schlüssel durch Multiplikation des privaten Schlüssels mit einem Kurvenpunkt einer elliptischen Kurve berechnet wird. Dem Verwender des Verschlüsselungsverfahrens der Fig. 3 muss in diesem Fall ein Teil der zur Erzeugung des öffentlichen Schlüssels verwendeten Domainparameter bekannt sein.

[0105] Nach Berechnung des öffentlichen Schlüssels in Schritt **316** erfolgt wiederum in Schritt **308** eine Verschlüsselung des Datenobjektes mittels des öffentlichen Schlüssels oder in Schritt **328** die Verifikation einer digitalen Signatur eines Datenobjekts.

[0106] Ergibt sich im Prüfschritt **302**, dass kein öffentlicher Schlüssel existiert, so erfordert dies eine initiale Erzeugung eines asymmetrischen Schlüsselpaars. Dies geschieht, indem in Schritt **318** entweder eine frei wählbare Benutzerkennung empfangen und die Funktion g auf diese Benutzerkennung angewendet wird oder es wird bereits der Wert g(Benutzerkennung) empfangen.

[0107] Daraufhin erfolgt in Schritt **320** die Erzeugung einer Zufallszahl, woraufhin in Schritt **322**, wie bereits für Schritt **314** beschrieben, ein Kandidat für einen privaten Schlüssel erzeugt wird, indem die Funktion f auf g(Benutzerkennung) und die Zufallszahl angewendet wird.

[0108] In Schritt **324** erfolgt eine Zulässigkeitsprüfung, welche beispielsweise im Falle des elliptischen Kurvenverfahrens aus der Prüfung, ob der private Datenobjektschlüssel größer als 1 und kleiner als die Ordnung der elliptischen Kurve ist, besteht. Wird die Zulässigkeitsprüfung bestanden, so sind in Schritt **324** der Zufallswert sowie der private Schlüssel zulässig. Daraufhin kann in Schritt **326** die Berechnung des öffentlichen Schlüssels durchgeführt werden, worauf beispielsweise in Schritt **308** die Datenverschlüsselung oder in Schritt **328** die Verifikation der digitalen Signatur erfolgt.

[0109] Stellt sich hingegen in Schritt **324** heraus, dass der in Schritt **322** berechnete Kandidat für einen privaten Datenobjektschlüssel nicht zulässig ist, dann wird in Schritt **320** erneut eine Zufallszahl erzeugt, woraufhin die Schritte **322** und **324** wiederum durchgeführt werden. Dies geschieht so lange, bis die Zulässigkeitsprüfung in Schritt **324** erfolgreich ist, woraufhin der Schritt **326** mit der Berechnung des öffentlichen Schlüssels und beispielsweise der Schritt **308** mit der Datenverschlüsselung oder der Schritt **328** mit der Verifikation der digitalen Signatur durchgeführt werden.

[0110] In der Fig. 5 ist nun angenommen, dass, wie in der Fig. 4 gezeigt, in Schritt **322** der private Schlüssel berechnet wurde und in Schritt **326** beispielsweise unter Verwendung einer elliptischen Kurve der öffentliche Schlüssel berechnet wurde. Die Fig. 5 zeigt ein Verfahren zur Entschlüsselung eines

Datenobjekts. Das Verfahren beginnt wiederum mit Schritt **400**, dem Empfang einer eindeutigen Benutzeridentifikation. Außerdem wird daraufhin in Schritt **402** ein HASH-Wert einer Benutzerkennung empfangen. Unter Verwendung der Benutzeridentifikation wird in Schritt **404** von einer externen Datenbank eine Zufallszahl abgerufen, woraus unter Verwendung des HASH-Werts der Benutzerkennung in Schritt **406** ein privater Schlüssel berechnet werden kann. Dieser private Schlüssel kann nun dazu verwendet werden, um die mit dem öffentlichen Datenobjektschlüssel verschlüsselten Daten in Schritt **408** zu entschlüsseln.

[0111] Die Fig. 6 zeigt ein Flussdiagramm eines Verfahrens zur Berechung eines asymmetrischen Schlüsselpaares nach dem RSA-Verfahren. Das Verfahren beginnt mit Schritt **506**, in dem zwei Primzahlen p und q gemäß den aktuellen Sicherheitsanforderungen für RSA gewählt werden. Die beiden Zahlen werden miteinander multipliziert und das Ergebnis n genannt. Auf n wird anschließend die Eulersche φ-Funktion angewendet, so dass man den Wert φ(n) erhält.

[0112] Im folgenden Schritt **500** wird eine Benutzerkennung empfangen, auf die die Funktion g angewendet wird, oder es wird direkt der Funktionswert g(Benutzerkennung) empfangen. Darauf folgt Schritt **502**, in welchem ein Zufallswert erzeugt wird. Durch Anwendung der Funktion f auf den Zufallswert und g(Benutzerkennung) erfolgt im Schritt **504** die Berechnung eines Kandidaten für den privaten Schlüssel d.

[0113] In Schritt **508** erfolgt eine Zulässigkeitsprüfung, wobei die Zulässigkeitsprüfung im Falle des RSA Verfahrens mehrstufig verläuft. So wird zunächst in Schritt **508** geprüft, ob d im Intervall [2, φ(n) – 2] liegt.

[0114] Ergibt der Prüfschritt **508**, dass die Prüfbedingung nicht erfüllt ist, springt das Verfahren zu Schritt **502** zurück, wo ein neuer Zufallswert erzeugt wird. Daraufhin folgen wiederum die Schritte **504** mit dem erneuten Berechnen eines Kandidaten für den privaten Schlüssel e anhand des neuen Zufallswerts und dem erneuten Prüfen des Kandidaten d in Schritt **508**. Diese Schleife der Schritte **502**, **504** und **508** wiederholt sich so lange, bis die Prüfbedingung in Schritt **508** erfüllt ist. Erst dann setzt sich das Verfahren mit Schritt **510** fort.

[0115] Schritt **510** umfasst einen weiteren Prüfschritt, nämlich ob φ(n) und der Schlüsselkandidat d teilerfremd sind, d. h ggT(d, φ(n)) = 1. Ist dies nicht der Fall, springt das Verfahren wieder zurück zu Schritt **502** und ein neuer Zufallswert wird erzeugt, gefolgt von den Schritten **504**, **508**, **510**. Auch diese Schleife der Schritte **502**, **504**, **508** und **510** wiederholt sich so lange, bis die Prüfbedingung in Schritt **510** erfüllt ist. Erst dann setzt sich das Verfahren mit Schritt **512** fort. Vorzugsweise wird der Prüfschritt **508** vor dem Prüfschritt **510** durchgeführt, da der Rechenaufwand für Schritt **508** wesentlich geringer ist als der Rechenaufwand für Schritt **510**.

[0116] In Schritt **512** erfolgt schließlich die Berechnung des öffentlichen Schlüssels e, so dass e die Kongruenz-Beziehung $e \cdot d \equiv 1 \bmod \varphi(n)$ mit $e \in [1, \varphi(n) - 1]$ erfüllt. Zur Verwendung des privaten Schlüssels d in kryptografischen Verfahren muss auch n bekannt gegeben werden.

[0117] Im abschließenden Schritt **514** werden die Zahlen p, q, und φ (n) verworfen, d. h. gelöscht.

[0118] Neben den Prüfschritten **508** und **510** können weitere Prüfschritte zum Einsatz kommen, um so die Sicherheit des erzeugten asymmetrischen Schlüsselpaares zu erhöhen.

[0119] Die Fig. 7 zeigt ein weiteres Flussdiagramm eines Verfahrens zur hierarchischen Bereitstellung von Berechtigungsschlüsseln und zur Verschlüsselung von Daten. Das Verfahren beginnt in dem Schritt **700**, in welchem ein neuer privater Schlüssel Gi und ein neuer öffentlicher Schlüssel Oi erzeugt werden. Der neue private Schlüssel Gi und der neue öffentliche Schlüssel Oi können dabei auf einer neuen Chipkarte gespeichert sein. Daraufhin erfolgt in Schritt **702** das Abrufen eines privaten Schlüssels Gi – 1, welcher in der Sequenz von Berechtigungsschlüsseln dem Paar von Berechtigungsschlüsseln unmittelbar vorangeht, welches in Schritt **700** erzeugt wurde. In einem praktischen Beispiel von Chipkarten würde in Schritt **700** das neue Schlüsselpaar Gi und Oi von einer neuen Chipkarte abgerufen, wohingegen in Schritt **702** der private Vorgänger-Berechtigungsschlüssel Gi – 1 von einer Vorgänger-Chipkarte abgerufen wird. Daraufhin wird in Schritt **704** dieser private Vorgänger-Schlüssel Gi – 1 mit dem öffentlichen Schlüssel Oi der neuen Chipkarte verschlüsselt. Das sich so ergebende Chiffrat wird in Schritt **706** in einer Datenbank abgelegt.

[0120] Nachdem in den Schritten **700** bis **706** eine hierarchische Bereitstellung von Berechtigungsschlüsseln erfolgt ist, folgt in den Schritten **708** bis **720** ein Verschlüsselungsvorgang von Datenobjekten. In anderen Worten müssen die Schritte **700** bis **706** lediglich einmalig bei Ausgabe einer neuen Chipkarte mit neuen asymmetrischen Schlüsseln Gi und Oi durchgeführt werden, wohingegen die Schritte **708** bis **720** für jeden Verschlüsselungsvorgang von Datenobjekten durchgeführt werden müssen. In Schritt **708** wird nun ein neues Datenobjekt erzeugt. Daraufhin erfolgt in Schritt **710** die Erzeugung eines symmetrischen Schlüssels s, welcher in Schritt **712** dazu verwendet wird, um das Datenobjekt des Schrittes

708 zu verschlüsseln. In Schritt **714** erfolgt das Abrufen des initialen öffentlichen Berechtigungsschlüssels O0 aus einer öffentlichen Datenbank, wobei in Schritt **716** dieser initiale öffentliche Berechtigungsschlüssel zur Verschlüsselung des symmetrischen Schlüssels s, welcher in Schritt **710** erhalten wurde, verwendet wird.

[0121] Schließlich erfolgt eine Speicherung des verschlüsselten Datenobjekts und des verschlüsselten symmetrischen Schlüssels in einer entsprechenden Patientendatenbank in Schritt **720**.

[0122] Der Schritt **718**, welcher nach Schritt **716** folgt, ist ein optionaler Schritt, in welchem die Möglichkeit besteht, das Datenobjekt zusätzlich zu signieren, um so einem unbefugten Missbrauch und einer Manipulation des Datenobjekts vorzubeugen. Eine solche digitale Signierung erfolgt vorzugsweise mit dem privaten Berechtigungsschlüssel Gi der aktuell verwendeten Chipkarte. Wurde der Schritt **718** durchgeführt, wird die digitale Signatur zusätzlich in Schritt **720** zusammen mit dem verschlüsselten Datenobjekt und dem verschlüsselten symmetrischen Schlüssel abgespeichert.

[0123] Die Fig. 8 zeigt ein weiteres Flussdiagramm zum Entschlüsseln von Datenobjekten. Im Folgenden sei angenommen, dass dem Datenobjekt eine digitale Signatur zugefügt wurde. Damit erfolgt in Schritt **800** das Abrufen des verschlüsselten Datenobjekts, des verschlüsselten symmetrischen Schlüssels und der digitalen Signatur. In Schritt **802** wird überprüft, ob der initiale private Berechtigungsschlüssel verfügbar ist. Dies kann beispielsweise dann der Fall sein, wenn außer dem initialen Berechtigungsschlüssel keine weiteren Schlüssel in einer hierarchischen Sequenz ausgegeben wurden. Ist dies der Fall, wird in Schritt **804** dieser initiale private Berechtigungsschlüssel G0 empfangen und in Schritt **806** erfolgt eine Entschlüsselung des verschlüsselten symmetrischen Datenobjektschlüssels mittels des initialen privaten Berechtigungsschlüssels G0. Dies ist möglich, dass der symmetrische Datenobjektschlüssel s zuvor mit dem initialen öffentlichen Berechtigungsschlüssel O0 verschlüsselt wurde, vgl. hierzu Schritt **716** der Fig. 7.

[0124] Nachdem in Schritt **806** der symmetrische Schlüssel entschlüsselt wurde, erfolgt daraufhin in Schritt **808** eine Entschlüsselung des Datenobjekts mit dem so erhaltenen symmetrischen Schlüssel s. In Schritt **810** wird überprüft, ob zu dem Datenobjekt eine Signatur verfügbar ist. Ist dies der Fall, erfolgt in Schritt **812** eine Signaturüberprüfung unter Verwendung des öffentlichen Berechtigungsschlüssels der Chipkarte, welche ursprünglich zur Signierung des Datenobjekts herangezogen wurde. Hierzu ist nicht notwendigerweise das Vorliegen dieser Chipkarte selbst notwendig, da der öffentliche Berechtigungsschlüssel dieser Chipkarte ohne Weiteres auf einem öffentlichen Server abgelegt sein kann.

[0125] Ergibt sich in Schritt **802**, dass der initiale Berechtigungsschlüssel nicht direkt verfügbar ist, typischerweise weil bereits eine Sequenz von zusätzlichen Berechtigungsschlüsseln bereitgestellt wurde, wird unter Verwendung eines beliebigen dieser Berechtigungsschlüsselpaare, welche augenblicklich zur Verfügung stehen, das Verfahren in Schritt **816** fortgesetzt. Im Folgenden sei angenommen, dass es sich bei dem zur Entschlüsselung des Datenobjekts verfügbaren Berechtigungsschlüsselpaar um das Schlüsselpaar mit Index i handelt. Das Berechtigungsschlüsselpaar mit Index i umfasst einen privaten Berechtigungsschlüssel Gi, welcher in Schritt **816** empfangen wird. Darauf wird in Schritt **818** ein Zählindex n = i gesetzt. Daraufhin folgt Schritt **820** mit dem Abrufen eines Chiffrats, welches zuvor bei Aktivierung der Chipkarte mit dem neuen Satz von Berechtigungsschlüsseln mit Index i erzeugt wurde, von einer externen Datenbank. Bei diesem Chiffrat, welches in Schritt **820** abgerufen wird, handelt es sich um das Chiffrat, welches in der Fig. 7 in Schritt **704** erzeugt wurde und in Schritt **706** in dieser Datenbank abgespeichert wurde.

[0126] Nachdem nun in Schritt **820** das Chiffrat von der Datenbank abgerufen wurde, erfolgt in Schritt **822** das Entschlüsseln des Chiffrats mit dem gegenwärtig verfügbaren privaten Berechtigungsschlüssel mit Index n, d. h. im vorliegenden Schritt Index n = i. in anderen Worten wird der private Berechtigungsschlüssel der zur Entschlüsselung verwendeten Chipkarte dazu verwendet, um das Chiffrat zu entschlüsseln. Dieser Entschlüsselungsvorgang in Schritt **822** liefert den privaten Berechtigungsschlüssel mit Index n – 1, d. h. Index i – 1, oder in anderen Worten der private Berechtigungsschlüssel der Vorgänger-Chipkarte in der Sequenz von Chipkarten, welche der Chipkarte mit Index i unmittelbar vorangeht.

[0127] In Schritt **824** wird überprüft, ob der Laufindex n = 1 ist. In diesem Fall würde nämlich der private Berechtigungsschlüssel, welcher in Schritt **822** aus dem Chiffrat extrahiert wurde, dem initialen privaten Berechtigungsschlüssel G0 entsprechen. Ist dies der Fall, erfolgt nach Schritt **824** die Durchführung der Schritte **806** bis **814**, wie obig beschrieben.

[0128] Im Folgenden sei jedoch angenommen, dass sich in Schritt **824** ergibt, dass n größer als 1 ist, sodass nach Schritt **824** der Schritt **826** mit der Erniedrigung des Laufindex n um 1 erfolgt, d. h. n = i – 2. Nach Schritt **826** wiederholt sich das Verfahren der Schritte **820** bis **824** wie obig beschrieben.

[0129] Dies bedeutet, dass in Schritt **820** nun das Chiffrat von der externen Datenbank abgerufen wird,

welches dem Index i – 2 zugeordnet ist. Unter Verwendung des in der vorigen Schleife erhaltenen privaten Berechtigungsschlüssels mit Index i – 1 lässt sich nun das soeben in Schritt **820** abgerufene Chiffrat wiederum entschlüsseln, woraus in Schritt **822** der private Berechtigungsschlüssel mit Index i – 2 erhalten wird. Dem folgt wiederum Schritt **824** mit der Überprüfung, ob der Laufindex 1 beträgt, d. h. ob der in Schritt **822** erhaltene private Berechtigungsschlüssel dem initialen privaten Berechtigungsschlüssel G0 entspricht. Ist dies der Fall, folgt Schritt **806**, wohingegen bei Nichterfüllung dieser Bedingung Schritt **826** mit der Erniedrigung des Laufindex n um 1 erfolgt.

[0130] Somit wird durch Durchführung der Schritte **820** bis **826** in rekursiver Weise unter sequenziellem Abrufen von entsprechenden Chiffraten der initiale private Berechtigungsschlüssel G0 extrahiert, um damit eine Entschlüsselung des verschlüsselten symmetrischen Schlüssels vorzunehmen.

Bezugszeichenliste

100 Datenverarbeitungssystem
102 Eingabemittel
104 Bildschirm
106 Schnittstelle
108 Prozessor
110 Speicher
112 Applet
114 Modul
116 Modul
118 Modul
120 Netzwerk
122 Datenbank
124 Benutzeridentifikation
126 öffentlicher Schlüssel
128 Zufallszahl
130 verschlüsseltes Datenobjekt
132 Datenbank
134 Datenbank
150 Chiffrat
152 Chipkarte
154 privater Schlüssel
156 öffentlicher Schlüssel
158 Hardwaremodul
160 Chipkarte
162 privater Schlüssel
164 öffentlicher Schlüssel
166 Hardwaremodul
200 Applet
202 Modul
204 Modul
206 Modul
208 Datenverarbeitungssystem
210 Schnittstelle
212 Prozessor
214 Speicher
216 Programm
218 Modul
220 Modul
222 Modul

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102004051296 B3 **[0004]**
- DE 10258769 A1 **[0005]**

Schutzansprüche

1. Computerprogrammprodukt (**114**; **116**) mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Bereitstellung von Berechtigungsschlüsseln (**154**; **156**; **162**; **164**), wobei das Verfahren die folgenden Schritte umfasst:
– Empfang eines weiteren asymmetrischen kryptografischen Schlüsselpaares (**162**; **164**), wobei das weitere asymmetrische Schlüsselpaar Teil einer Schlüsselpaarsequenz ist, wobei das weitere asymmetrische Schlüsselpaar einen weiteren ersten (**162**) und einen weiteren zweiten (**164**) Berechtigungsschlüssel umfasst,
– Abrufen eines Chiffrats (**150**), wobei das Chiffrat dem Schlüsselpaar (**154**; **156**) zugeordnet ist, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar (**162**; **164**) unmittelbar vorangeht, wobei das Chiffrat (**150**) den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel (**156**) des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, umfasst,
– Entschlüsseln des initialen ersten Berechtigungsschlüssels mit dem ersten Berechtigungsschlüssel (**154**) des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht,
– Erzeugen eines weiteren Chiffrats (**150**) durch Verschlüsseln des entschlüsselten initialen ersten Berechtigungsschlüssels mit dem zweiten Berechtigungsschlüssel (**164**) des weiteren Schlüsselpaares,
– Speicherung des weiteren Chiffrats (**150**).

2. Computerprogrammprodukt nach Anspruch 1, wobei das Chiffrat (**150**) in einer Datenbank (**122**) gespeichert wird.

3. Computerprogrammprodukt nach Anspruch 1 oder 2, ferner mit Instruktionen zur Durchführung des Schritts des Erzeugens des weiteren asymmetrischen kryptografischen Schlüsselpaares, wobei das Verfahren die folgenden Schritte umfasst:
– Empfang einer beliebig wählbaren Benutzerkennung,
– Berechnen des weiteren ersten Berechtigungsschlüssels, wobei in die Berechnung ein Zufallswert (**128**) und die Benutzerkennung eingeht,
– Berechnen des weiteren zweiten Berechtigungsschlüssels aus dem weiteren ersten Berechtigungsschlüssel mittels eines asymmetrischen kryptografischen Schlüsselerzeugungsverfahrens, wobei der weitere erste und der weitere zweite Berechtigungsschlüssel das weitere asymmetrische kryptografische Schlüsselpaar bilden.

4. Computerprogrammprodukt nach Anspruch 3, wobei das Verfahren des weiteren umfasst:
a) Durchführen einer Zulässigkeitsüberprüfung (**324**) des weiteren ersten Berechtigungsschlüssels mittels einer Prüfbedingung, wobei die Prüfbedingung die Verwendbarkeit des weiteren ersten Berechtigungsschlüssels zur Erzeugung des weiteren zweiten Berechtigungsschlüssels aus dem weiteren ersten Berechtigungsschlüssel mittels eines asymmetrischen kryptografischen Schlüsselerzeugungsverfahrens umfasst,
b) wenn die Prüfbedingung erfüllt ist, Berechnen des weiteren zweiten Berechtigungsschlüssels aus dem weiteren ersten Berechtigungsschlüssel,
c) wenn die Prüfbedingung nicht erfüllt ist, erneutes Berechnen eines weiteren ersten Berechtigungsschlüssels mit einem neuen Zufallswert (**128**) und erneutes Durchführen des Schritts a).

5. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 oder 4, wobei die Berechnung des weiteren ersten Datenobjektschlüssels unter Verwendung einer Funktion g, die auf die Benutzerkennung angewendet wird, erfolgt, wobei es sich bei der Funktion g vorzugsweise um eine Einwegfunktion, wie z. B. eine kryptografische Hash-Funktion, handelt.

6. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 bis 5, wobei die Benutzerkennung als Funktionswert einer Funktion g, die auf die Benutzerkennung angewendet wurde, empfangen wird, wobei es sich bei der Funktion g vorzugsweise um eine Einwegfunktion, wie z. B. eine kryptografische Hash-Funktion, handelt.

7. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 bis 6, wobei der weitere erste Datenobjektschlüssel berechnet wird durch Anwenden einer Funktion f auf den Zufallswert (**128**) und g(Benutzerkennung).

8. Computerprogrammprodukt nach Anspruch 7, wobei es sich bei der Funktion f um eine Einwegfunktion handelt, z. B. eine kyptografische Hash-Funktion.

9. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 bis 8, wobei es sich bei dem asymmetrischen kryptografischen Schlüsselerzeugungsverfahren um ein Verfahren auf elliptischen Kurven handelt, wobei der weitere zweite Schlüssel durch Multiplikation des ersten Schlüssels mit einem Kurvenpunkt einer elliptischen Kurve berechnet wird.

10. Computerprogrammprodukt nach Anspruch 9, wobei es sich bei der Prüfbedingung um die Bedingung handelt, dass der weitere erste Berechtigungsschlüssel größer als eins und kleiner als die Ordnung der elliptischen Kurve ist.

11. Computerprogrammprodukt nach einem der Ansprüche 9 oder 10, wobei es sich bei der Prüfbe-

dingung um die Bedingung handelt dass die Bitlänge des Zufallswerts (**128**) größer oder gleich der Bitlänge der Ordnung der elliptischen Kurve ist.

12. Computerprogrammprodukt nach einem der Ansprüche 9 bis 11, wobei es sich bei der Prüfbedingung um die Bedingung handelt, dass der Zufallswert (**128**) so gewählt ist, dass der Wert des erzeugten weiteren ersten Berechtigungsschlüssels kleiner als die Ordnung der elliptischen Kurve ist.

13. Computerprogrammprodukt nach einem der Ansprüche 3 bis 8, wobei es sich bei dem asymmetrischen kryptografischen Schlüsselerzeugungsverfahren um ein RSA-Verfahren handelt, wobei es sich bei der Prüfbedingung um die Bedingung handelt, dass die Eulersche φ-Funktion des für das RSA-Schlüsselerzeugungsverfahren verwendeten Modulus n und der weitere erste Schlüssel teilerfremd sind.

14. Computerprogrammprodukt nach Anspruch 13, wobei es sich bei der Prüfbedingung ferner um die Bedingung handelt, dass der weitere erste Berechtigungsschlüssel einen Wert zwischen 2 und den Wert der φ-Funktion des für das RSA-Schlüsselerzeugungsverfahren verwendeten Moduls n minus 2 aufweist.

15. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 bis 14, wobei der Zufallswert (**128**) von einer weiteren Datenbank (**132**) abgerufen wird, wobei der Zufallswert (**128**) eindeutig der Benutzeridentifikation (**124**) zugeordnet ist.

16. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 bis 15, wobei das Computerprogrammprodukt durch ein Applet (**112**) oder ein Browser-Plugin ausgebildet ist oder eine eigenständige Anwendung ist, die auf einem Rechner einer vertrauenswürdigen Stelle läuft oder eine eingebettete Anwendung ist, die in einem gesicherten Hardware-Modul läuft.

17. Computerprogrammprodukt nach einem der vorigen Ansprüche 3 bis 16, wobei das weitere asymmetrische kryptografische Schlüsselpaar von einem tragbaren Datenträger (**160**) empfangen wird, wobei das Chiffrat auf dem tragbaren Datenträger gespeichert wird.

18. Computerprogrammprodukt nach Anspruch 17, wobei es sich bei dem tragbaren Datenträger um eine Chipkarte handelt.

19. Computerprogrammprodukt (**114**; **116**) mit von einem Prozessor ausführbaren Instruktionen zur Durchführung von Verfahrensschritten zur Entschlüsselung eines Datenobjekts (**130**), wobei das Datenobjekt über einen initalen ersten Berechtigungsschlüssel entschlüsselbar ist, wobei der initale erste Berechtigungsschlüssel zusammen mit einem initialen zweiten Berechtigungsschlüssel ein initales asymmetrisches kryptografisches Schlüsselpaar bildet, wobei das initiale asymmetrische Schlüsselpaar Teil einer Schlüsselpaarsequenz ist, wobei das Verfahren die folgenden Schritte umfasst:
– Zugriff auf einen ersten Berechtigungsschlüssel (**154**), wobei der erste Berechtigungsschlüssel zusammen mit einem zweiten Berechtigungsschlüssel (**156**) ein asymmetrisches kryptografisches Schlüsselpaar bildet, wobei das asymmetrische Schlüsselpaar Teil der Schlüsselpaarsequenz ist,
– Abrufen eines Chiffrats (**150**), wobei das Chiffrat dem asymmetrischen kryptografischen Schlüsselpaar zugeordnet ist, wobei das Chiffrat den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel umfasst,
– Entschlüsseln des verschlüsselten initialen ersten Schlüssels mit dem ersten Berechtigungsschlüssel,
– Entschlüsseln des verschlüsselten Datenobjekts (**130**) über den entschlüsselten initialen ersten Schlüssel.

20. Computerprogrammprodukt nach Anspruch 19, ferner mit Instruktionen zur Durchführung des Schritts des Empfangens einer dem asymmetrischen kryptografischen Schlüsselpaar zugeordneten Schlüsselpaarkennung, wobei das Chiffrat (**150**) anhand der Schlüsselpaarkennung abgerufen wird.

21. Computerprogrammprodukt nach Anspruch 19 oder 20, wobei das Chiffrat (**150**) von einer Datenbank (**122**) abgerufen wird.

22. Computerprogrammprodukt nach Anspruch 19 oder 20, wobei das asymmetrische Schlüsselpaar zusammen mit dem Chiffrat (**150**) auf einem tragbaren Datenträger (**152**; **160**) gespeichert ist.

23. Computerprogrammprodukt nach einem der vorigen Ansprüche 19 bis 22, ferner mit Instruktionen zur Durchführung des Schritts einer Signaturüberprüfung (**618**) des Datenobjekts, wobei die Signaturüberprüfung die Schritte umfasst:
– Lesen einer dem Datenobjekt zugeordneten Signatur,
– Verifizierung der Signatur des Datenobjekts, wobei die Verifikation mit dem zweiten Berechtigungsschlüssel erfolgt.

24. Computerprogrammprodukt nach einem der vorigen Ansprüche 19 bis 23, wobei das Datenobjekt mit einem symmetrischen Datenobjektschlüssel verschlüsselt ist, wobei der symmetrische Datenobjektschlüssel mit dem initalen zweiten Berechtigungsschlüssel verschlüsselt ist, wobei das Entschlüsseln des verschlüsselten Datenobjekts die folgenden weiteren Schritte umfasst:
– Entschlüsseln des verschlüsselten symmetrischen

Datenobjektschlüssels mit dem entschlüsselten initialen ersten Berechtigungsschlüssel,
– Entschlüsseln des verschlüsselten Datenobjekts mit dem entschlüsselten symmetrischen Schlüssel.

25. Computerprogrammprodukt nach einem der vorigen Ansprüche 19 bis 24, wobei der Zugriff auf den ersten Berechtigungsschlüssel die folgenden Schritte umfasst:
– Empfang einer Benutzeridentifikation (**124**) und einer der Benutzeridentifikation (**124**) zugeordneten Benutzerkennung,
– Abrufen eines der Benutzeridentifikation (**124**) zugeordneten Zufallswertes von einer weiteren Datenbank,
– Berechnen des ersten Berechtigungsschlüssels, wobei in die Berechnung der Zufallswert (**128**) und die Benutzerkennung eingehen.

26. Computerprogrammprodukt nach Anspruch 25, wobei die Signaturüberprüfung ferner den Schritt umfasst des Berechnens des zweiten Berechtigungsschlüssels aus dem ersten Berechtigungsschlüssel mittels eines asymmetrischen kryptografischen Schlüsselerzeugungsverfahrens, wobei der erste und der zweite Berechtigungsschlüssel das asymmetrische kryptografische Schlüsselpaar bilden.

27. Computerprogrammprodukt nach Anspruch 25 oder 26, wobei der Zufallswert (**128**) über eine sichere Kommunikationsverbindung von der weiteren Datenbank (**132**) abgerufen wird.

28. Computerprogrammprodukt nach einem der vorigen Ansprüche 25 bis 27, wobei der Zufallswert (**128**) verschlüsselt in der weiteren Datenbank (**132**) abgespeichert ist.

29. Computerprogrammprodukt nach einem der vorigen Ansprüche 19 bis 28, wobei es sich bei dem Datenobjekt um ein medizinisches Datenobjekt handelt.

30. Computerprogrammprodukt nach einem der vorigen Ansprüche 19 bis 29, wobei das Computerprogrammprodukt durch ein Applet (**112**) oder ein Browser-Plugin ausgebildet ist, oder eine eigenständige Anwendung ist, die auf einem Rechner einer vertrauenswürdigen Stelle läuft oder eine eingebettete Anwendung ist, die in einem gesicherten Hardware-Modul läuft.

31. Datenverarbeitungssystem (**100**) zur Bereitstellung von Berechtigungsschlüsseln, wobei das Datenverarbeitungssystem folgendes umfasst:
– Mittel zum Empfang eines weiteren asymmetrischen kryptografischen Schlüsselpaares (**162**; **164**), wobei das weitere asymmetrische Schlüsselpaar Teil einer Schlüsselpaarsequenz ist, wobei das weitere asymmetrische Schlüsselpaar einen weiteren ersten (**162**) und einen weiteren zweiten (**164**) Berechtigungsschlüssel umfasst,
– Mittel zum Abrufen eines Chiffrats (**150**), wobei das Chiffrat dem Schlüsselpaar (**154**; **156**) zugeordnet ist, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, wobei das Chiffrat den initialen ersten Schlüssel verschlüsselt mit dem zweiten Berechtigungsschlüssel des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht, umfasst,
– Mittel zum Entschlüsseln des initialen ersten Berechtigungsschlüssels mit dem ersten Berechtigungsschlüssel (**154**) des Schlüsselpaars, welches in der Sequenz von Schlüsselpaaren dem weiteren Schlüsselpaar unmittelbar vorangeht,
– Mittel zum Erzeugen eines weiteren Chiffrats (**150**) durch Verschlüsseln des entschlüsselten initialen ersten Berechtigungsschlüssels mit dem zweiten Berechtigungsschlüssel (**164**) des weiteren Schlüsselpaares,
– Mittel zur Speicherung des weiteren Chiffrats.

32. Datenverarbeitungssystem nach Anspruch 31, wobei es sich bei dem Datenverarbeitungssystem um ein Datenverarbeitungssystem einer vertrauenswürdigen Stelle handelt.

Es folgen 8 Blatt Zeichnungen

Anhängende Zeichnungen

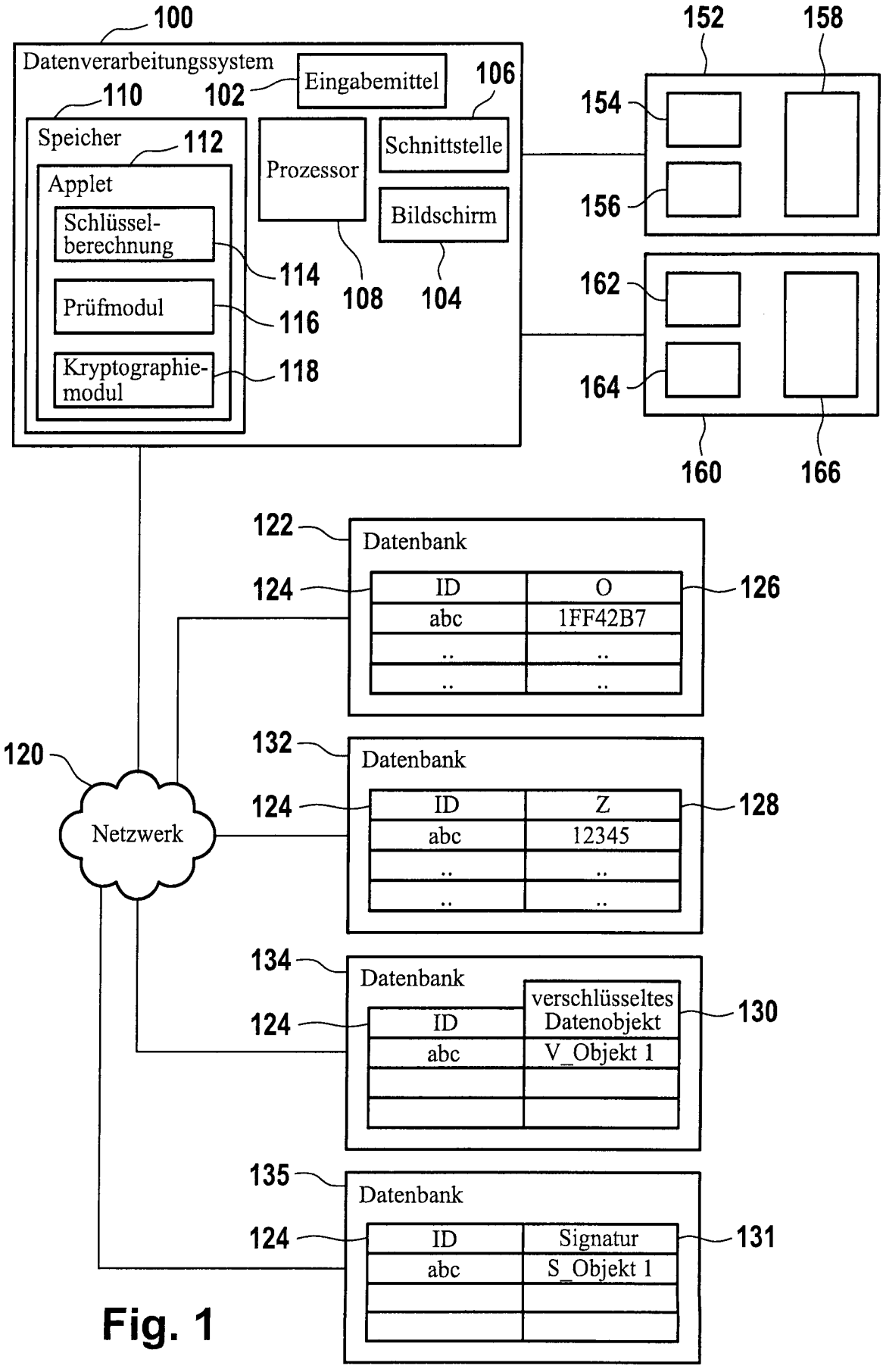


Fig. 1

Fig. 2

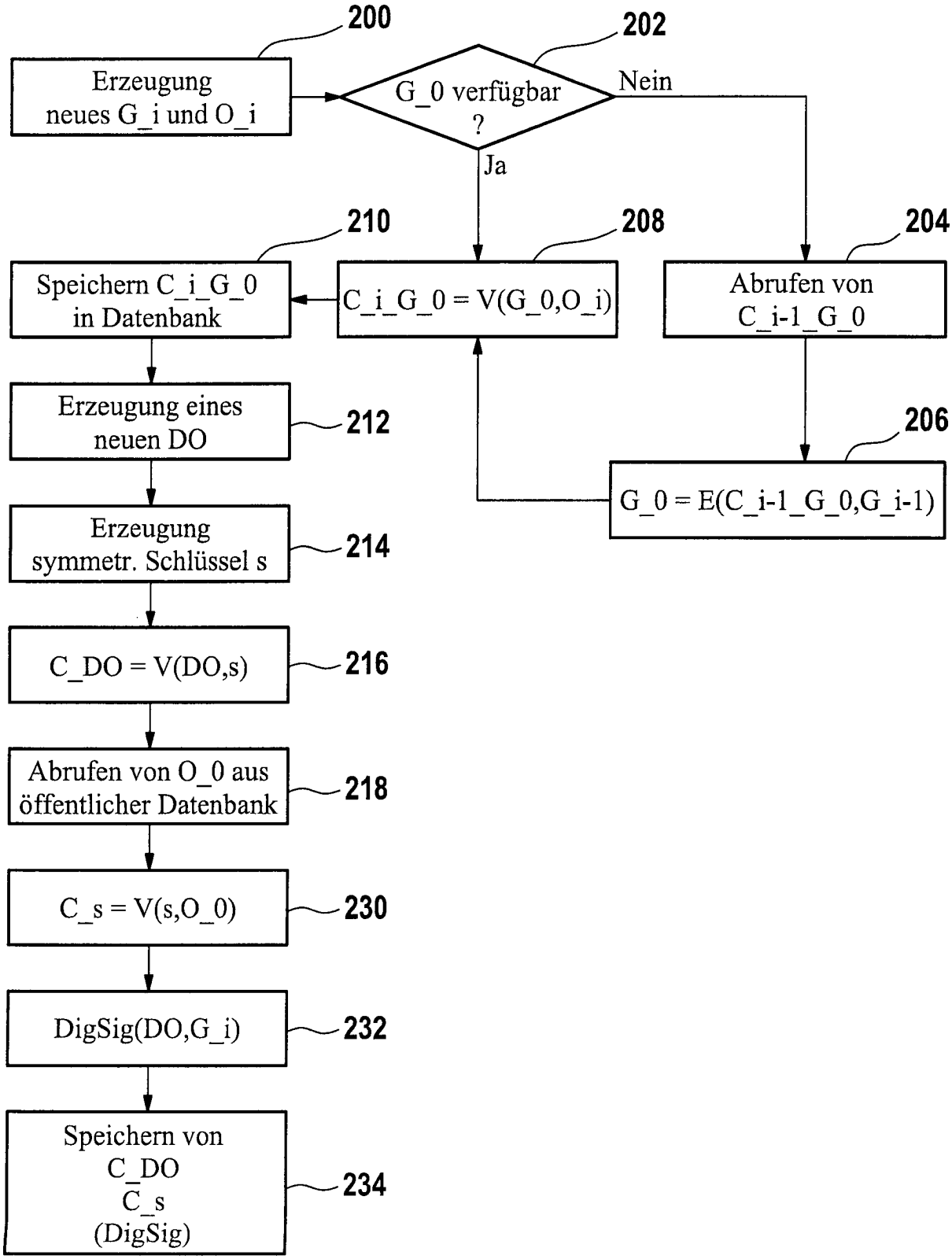

200
Erzeugung neues G_i und O_i
202
G_0 verfügbar ?
Nein
Ja
210
Speichern C_i_G_0 in Datenbank
208
C_i_G_0 = V(G_0,O_i)
204
Abrufen von C_i-1_G_0
Erzeugung eines neuen DO
212
206
G_0 = E(C_i-1_G_0,G_i-1)
Erzeugung symmetr. Schlüssel s
214
C_DO = V(DO,s)
216
Abrufen von O_0 aus öffentlicher Datenbank
218
C_s = V(s,O_0)
230
DigSig(DO,G_i)
232
Speichern von C_DO C_s (DigSig)
234

Fig. 3

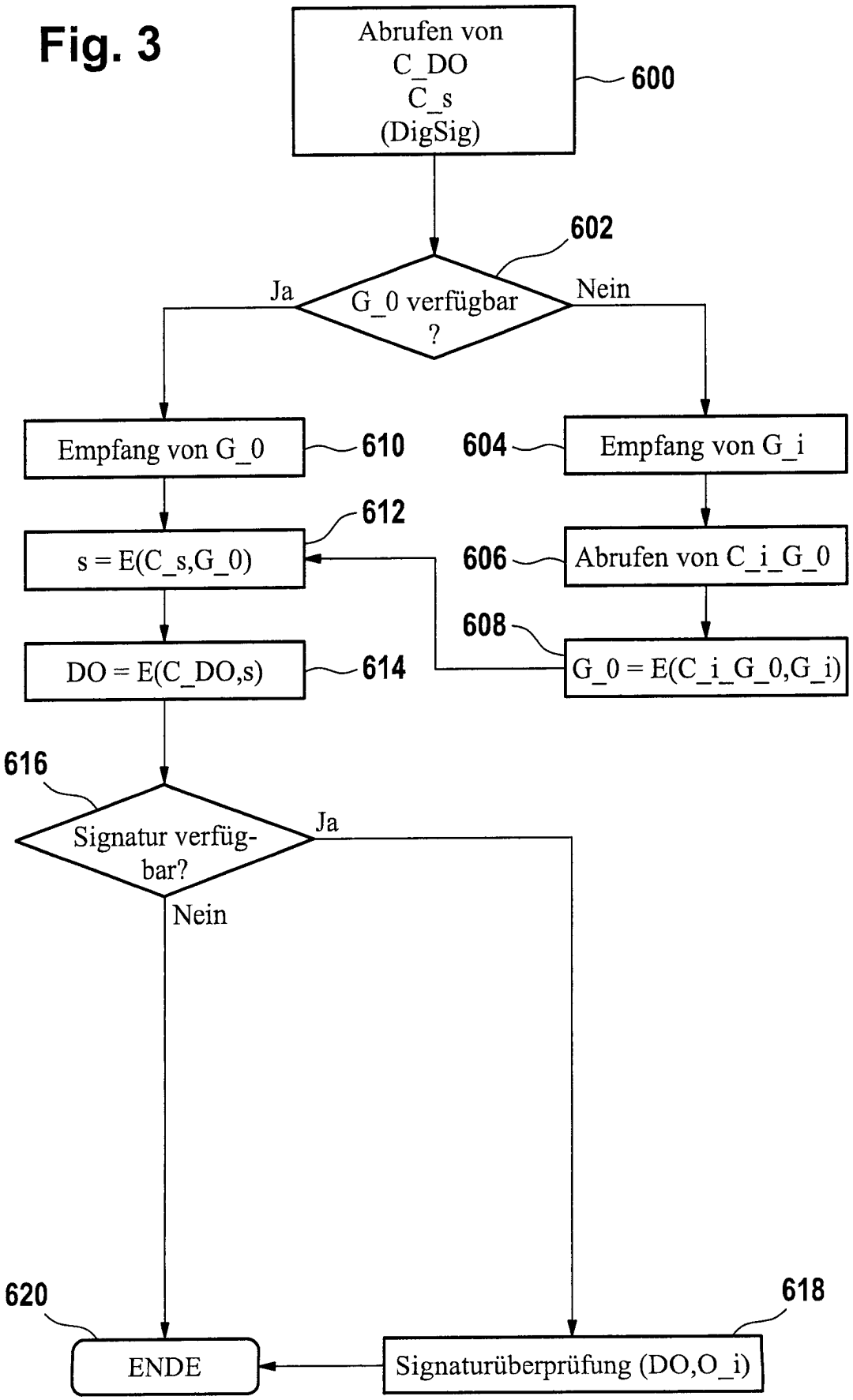

Abrufen von C_DO C_s (DigSig)
600
602
G_0 verfügbar ?
Ja
Nein
Empfang von G_0
610
604
Empfang von G_i
612
s = E(C_s,G_0)
606
Abrufen von C_i_G_0
608
DO = E(C_DO,s)
614
G_0 = E(C_i_G_0,G_i)
616
Signatur verfügbar?
Ja
Nein
620
618
ENDE
Signaturüberprüfung (DO,O_i)

Fig. 4

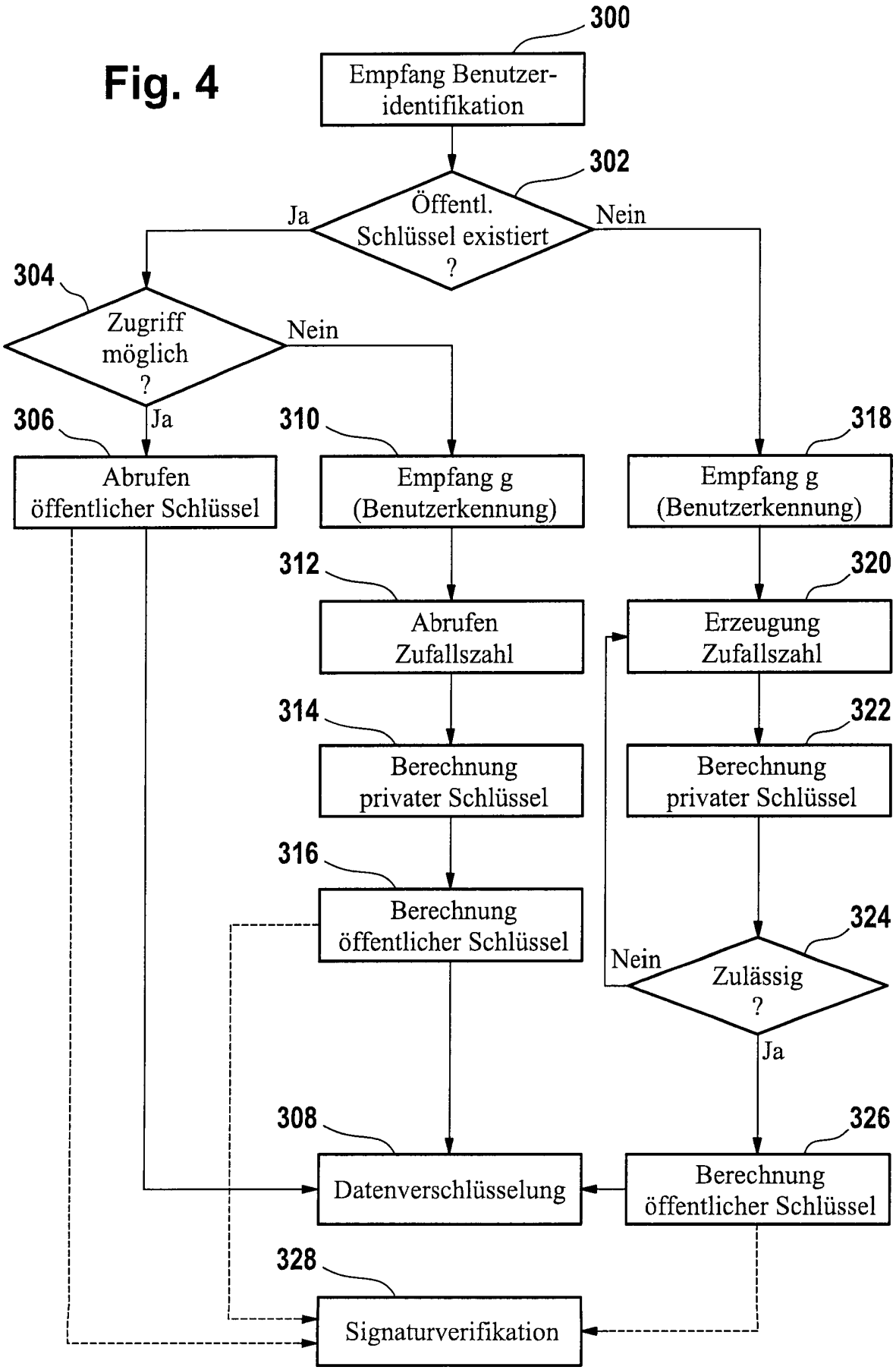

300
Empfang Benutzer-identifikation
302
Öffentl. Schlüssel existiert ?
Ja
Nein
304
Zugriff möglich ?
Nein
Ja
306
Abrufen öffentlicher Schlüssel
310
Empfang g (Benutzerkennung)
318
Empfang g (Benutzerkennung)
312
Abrufen Zufallszahl
320
Erzeugung Zufallszahl
314
Berechnung privater Schlüssel
322
Berechnung privater Schlüssel
316
Berechnung öffentlicher Schlüssel
324
Nein
Zulässig ?
Ja
308
Datenverschlüsselung
326
Berechnung öffentlicher Schlüssel
328
Signaturverifikation

Fig. 5

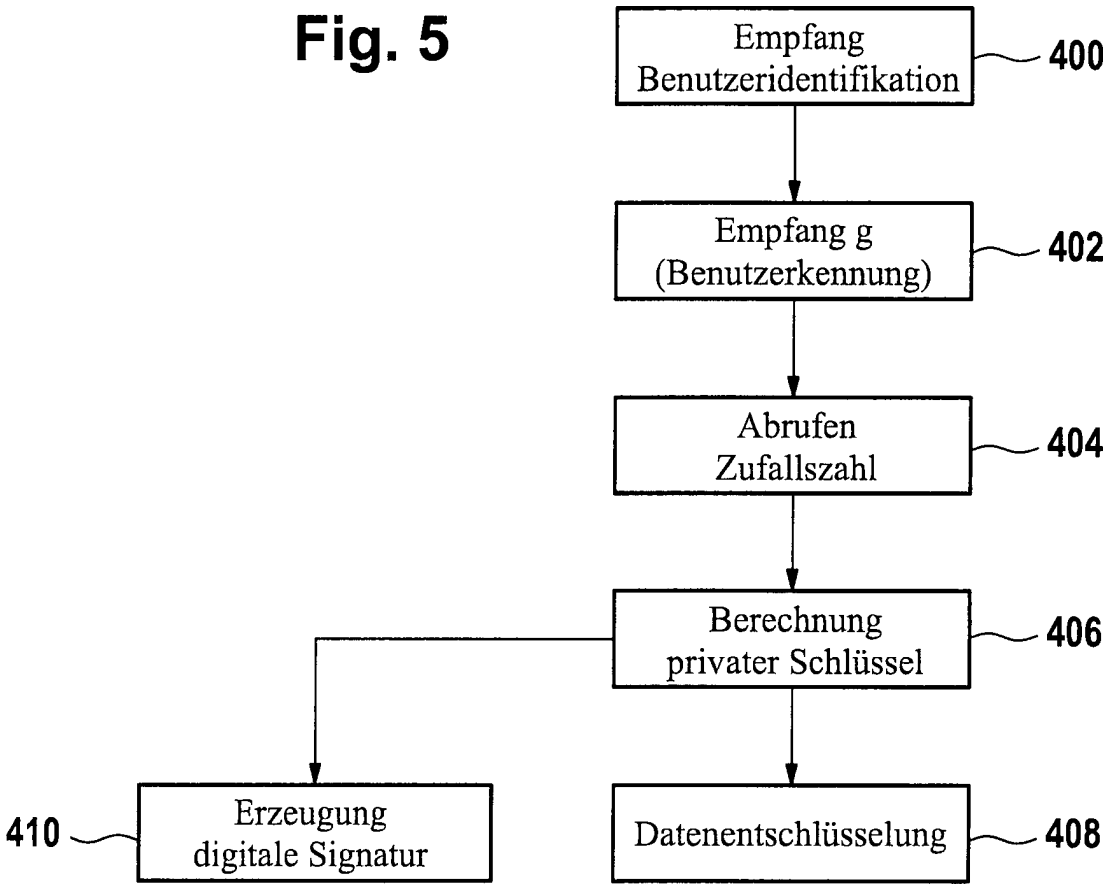

Empfang Benutzeridentifikation
400
Empfang g (Benutzerkennung)
402
Abrufen Zufallszahl
404
Berechnung privater Schlüssel
406
Erzeugung digitale Signatur
410
Datenentschlüsselung
408

Fig. 6

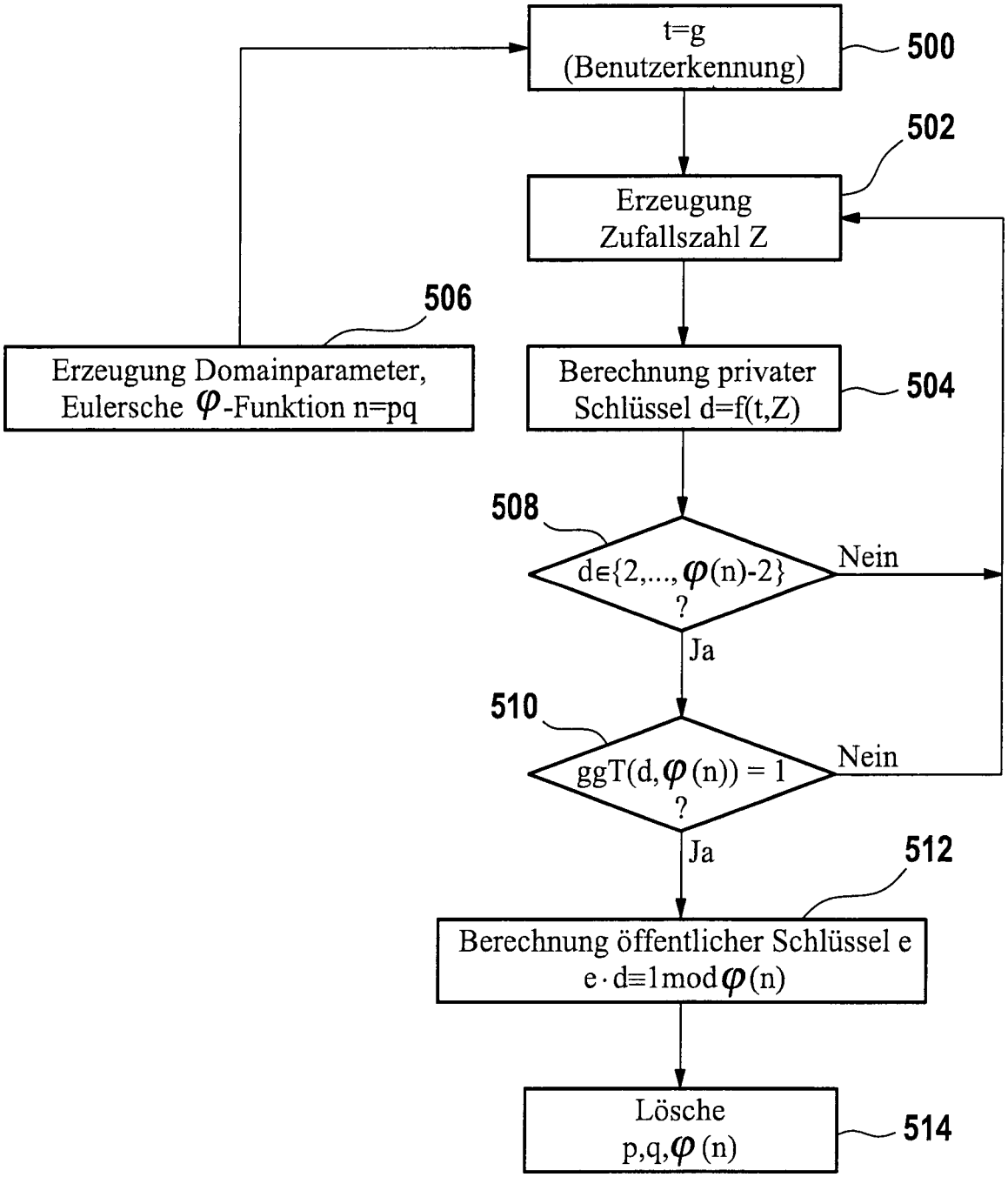

t=g
(Benutzerkennung)
500
502
Erzeugung
Zufallszahl Z
506
Erzeugung Domainparameter,
Eulersche φ-Funktion n=pq
Berechnung privater
Schlüssel d=f(t,Z)
504
508
dϵ{2,...,φ(n)-2}
?
Nein
Ja
510
ggT(d,φ(n)) = 1
?
Nein
Ja
512
Berechnung öffentlicher Schlüssel e
e·d≡1mod φ(n)
Lösche
p,q,φ(n)
514

Fig. 7

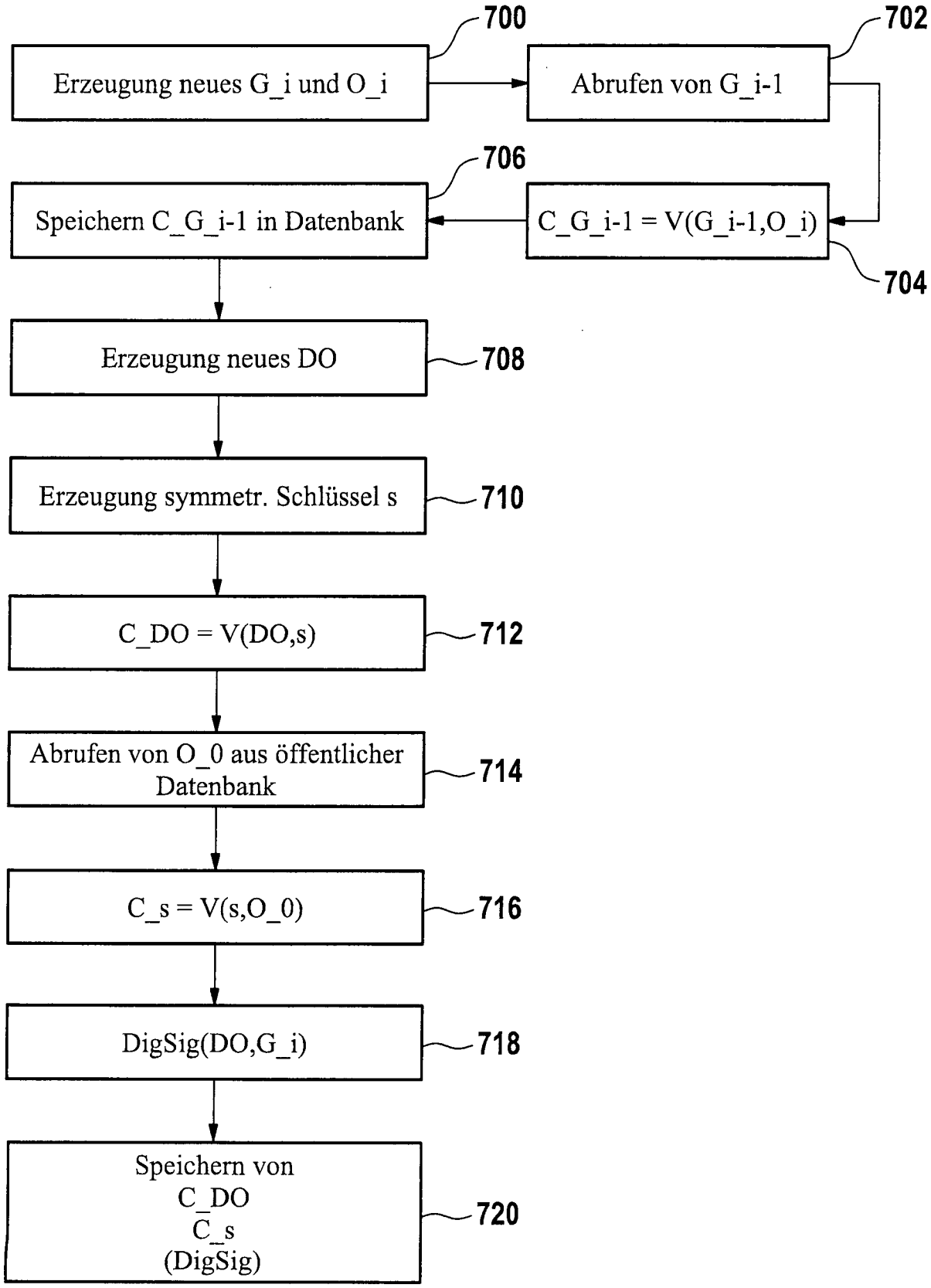
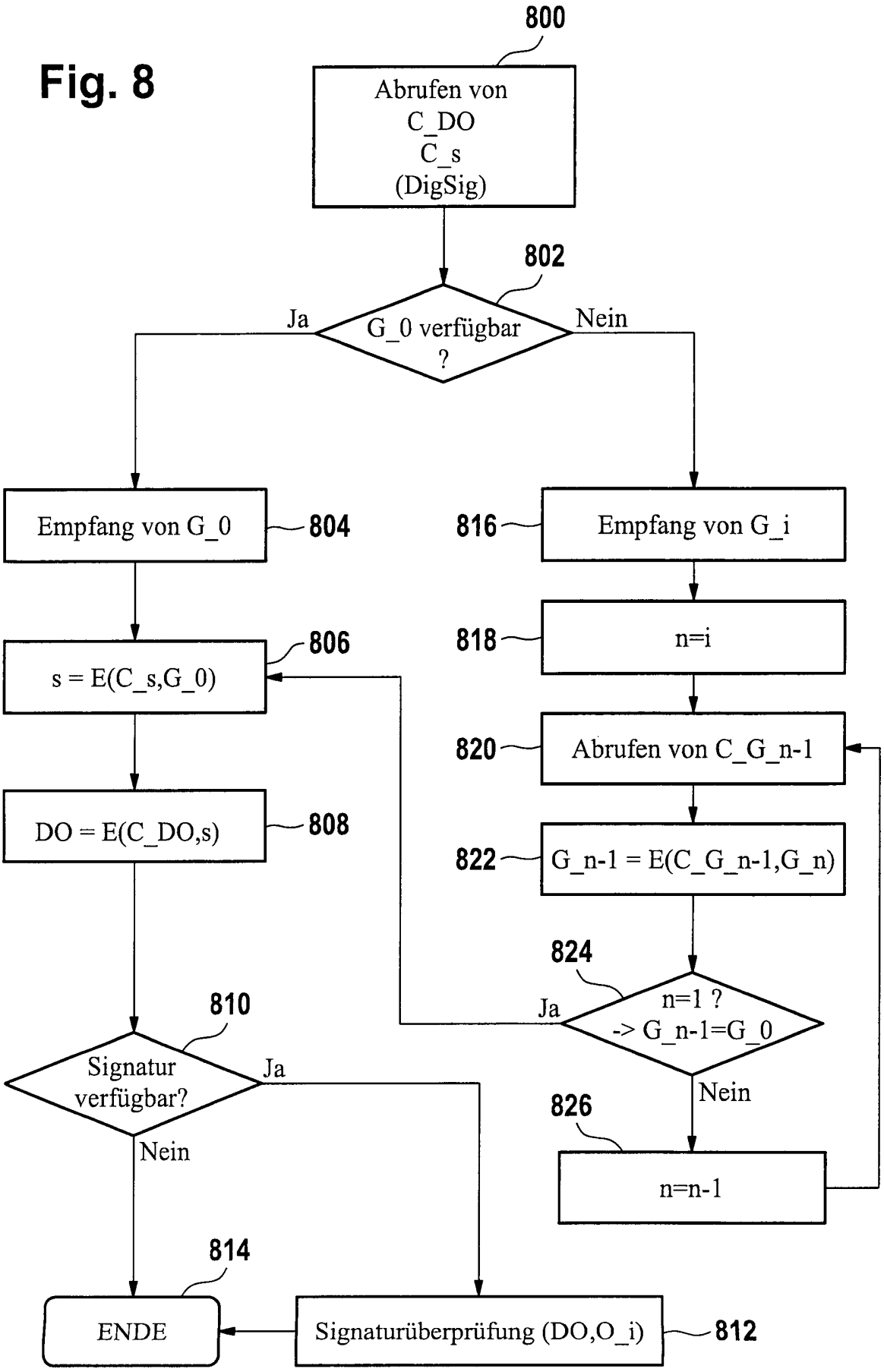

Erzeugung neues G_i und O_i
700
Abrufen von G_i-1
702
Speichern C_G_i-1 in Datenbank
706
C_G_i-1 = V(G_i-1,O_i)
704
Erzeugung neues DO
708
Erzeugung symmetr. Schlüssel s
710
C_DO = V(DO,s)
712
Abrufen von O_0 aus öffentlicher Datenbank
714
C_s = V(s,O_0)
716
DigSig(DO,G_i)
718
Speichern von
C_DO
C_s
(DigSig)
720

Fig. 8


800
Abrufen von C_DO C_s (DigSig)
802
G_0 verfügbar ?
Ja
Nein
Empfang von G_0
804
s = E(C_s,G_0)
806
DO = E(C_DO,s)
808
Signatur verfügbar?
810
Ja
Nein
816
Empfang von G_i
818
n=i
820
Abrufen von C_G_n-1
822
G_n-1 = E(C_G_n-1,G_n)
824
n=1 ? -> G_n-1=G_0
Ja
Nein
826
n=n-1
814
ENDE
Signaturüberprüfung (DO,O_i)
812