





SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN,  
YU, ZA, ZW.

**(84) Bestimmungsstaaten (regional):** ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Veröffentlicht:**

— ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

---

zusätzlich zu der persönlichen Identifikationsnummer (6) eine einmalig zu verwendende persönliche Authentifizierungsnummer (8) angegeben wird und auf der Basis einer Kombination der mitgeteilten persönlichen Identifikationsnummer (6) und der persönlichen Authentifizierungsnummer (8) von einer Datenbank (4) eine Identifikation bereitgestellt wird. Ein Vorteil des erfindungsgemässen Verfahrens liegt in dem Sicherheitsgewinn der Identifikation des Nutzers (2) durch den die Identifikation anfragenden Dritten (3). Neben der Zunahme der Sicherheit nimmt gleichzeitig der Aufwand einer Identifikation eines Nutzers (2) ab.

### Datennetzbasiertes Identifizierungsverfahren

- 5 Die Erfindung betrifft ein Verfahren zur persönlichen Identifizierung eines Nutzers in einem Datennetz durch einen Dritten, bei welchem dem Nutzer eine persönliche Identifikationsnummer zugeordnet ist und seine persönlichen Daten in einer Datenbank registriert sind.

Derartige Identifizierungsverfahren kommen heutzutage weltweit zum Einsatz.  
10 Die zunehmende gewerbliche Nutzung des Internets beispielsweise durch Geldinstitute, Kaufhäuser oder sonstige Dienstleister geht häufig mit der Notwendigkeit einher, den Geschäftspartner zuverlässig zu identifizieren. Der zeitsparende Vorteil des nicht mehr notwendigen persönlichen Kontaktes zwischen den Vertragspartnern hat gleichzeitig zur Folge, daß die Identität des  
15 erklärenden Vertragspartners nicht mehr auf konventionellem Wege überprüft werden kann. Bereits die Kenntnis weniger Daten einer Person, die Personalien und die Bankverbindung betreffend, kann es einem unberechtigten Dritten ermöglichen, unter falscher Identität über das Datennetz wirksame geschäftliche Erklärungen abzugeben. Solche Willenserklärung sind sowohl für den  
20 Identitätsinhaber, als auch für den Erklärungsempfänger in der Regel mit erheblichen Unannehmlichkeiten und bisweilen mit hohen wirtschaftlichen Verlusten verbunden. Die stark ansteigende Kriminalitätsrate auf dem Gebiet des Kreditkartenbetrugs ist nur ein Anzeichen dafür, daß die Sicherheit bisheriger datennetzbasierter Identifizierungsverfahren unzureichend ist.

- 25 Um der beschriebenen Problematik auszuweichen, gehen die verschiedensten Institute dazu über, ihre Geschäftspartner zu Beginn einer meist dauerhaften

Geschäftsbeziehung einmalig sicher zu identifizieren und mit Möglichkeiten auszustatten, welche nachfolgende Identifikationen erleichtern. So ist es zur Zeit beispielsweise üblich, bevor ein Geldinstitut mit einem Kunden Geschäfte über das Internet abwickelt, den Kunden über das Postidentverfahren oder ähnliche  
5 Verfahren eindeutig zu identifizieren und mit einer persönlichen Identifikationsnummer sowie einer Liste einmalig zu verwendender Transaktionsnummern auszustatten. In der Regel müssen Institutionen, welche Geschäfte über das Internet anbieten, jeden einzelnen Kunden derart aufwendig identifizieren und mit den entsprechenden Autorisierungsmöglichkeiten  
10 ausstatten.

Dieses Vorgehen ist sowohl für die gewerbliche Institution, als auch für den Kunden sehr aufwendig, zeitintensiv und kostspielig. Meist betreibt der potentielle Kunde nicht nur eine Geschäftsverbindung über ein Datennetz und muß daher auch entsprechend häufig eine derart aufwendige Identifizierung  
15 über sich ergehen lassen. Für den Fall, daß sich einige der Daten der bereits identifizierten Person ändern, müssen zudem alle Geschäftspartner auf vertraulichem Wege von dieser Änderung informiert werden, beziehungsweise es muß je nach Art der Änderung eine erneute aufwendige und kostspielige persönliche Identifizierung durchgeführt werden.

Ausgehend von den beschriebenen Nachteilen bereits bekannter Verfahren zur Identifizierung von Nutzern in Datennetzen liegt der Erfindung daher die Aufgabe zugrunde, ein Verfahren zu schaffen, welches den Aufwand der  
20 sicheren Identifizierung eines Nutzers in einem Datennetz sowohl für den die Identifikation anfragenden Dritten als auch für den Nutzer entscheidend reduziert, ohne Einbußen bezüglich der Sicherheit der Identifikation hinnehmen zu müssen.  
25

Zur Lösung dieser Aufgabe schlägt die Erfindung ein Verfahren zur persönlichen Identifizierung eines Nutzers in einem Datennetz der eingangs genannten Art vor, bei welchem der Nutzer dem Dritten zusätzlich zu der persönlichen  
30 Identifikationsnummer eine für jeden Identifikationsvorgang zur Verfügung gestellte, einmalig verwendbare persönliche Authentifizierungsnummer mitteilt und daß der Dritte auf der Basis einer Kombination der mitgeteilten persönlichen

Identifikationsnummer und der persönlichen Authentifizierungsnummer von der Datenbank eine Identifikation des Nutzers erhält.

Der besondere Vorteil des erfindungsgemäßen Verfahrens liegt in dem Sicherheitsgewinn der Identifikation des Nutzers durch den die Identifikation anfragenden Dritten. Der Nutzer ist erstmalig in der Lage im Rahmen der  
5 Anbahnung einer längerfristigen Geschäftsbeziehung oder nur für ein einmaliges Geschäft mit der Angabe seiner persönlichen Identifikationsnummer mit einer einmalig verwendbaren persönlichen Authentifizierungsnummer den Geschäftspartner auf sicherem Wege mit den notwendigen Informationen zu  
10 versorgen. Neben der Zunahme der Sicherheit nimmt gleichzeitig der Aufwand einer Identifikation eines Nutzers ab.

Während sich bisher Nutzer, insbesondere bei kurzfristigen Geschäftsbeziehungen, oft lediglich durch die Angabe einer Bankverbindung ihrem Geschäftspartner gegenüber identifizierten, liegt dem erfindungsgemäßen  
15 Verfahren eine Identifikation mit einer persönlichen, mehrfach zu verwendenden Identifikationsnummer und einer einmalig zu verwendenden Authentifizierungsnummer zugrunde. Die mehrmalige Verwendung von Identifizierungsangaben, beispielsweise den Daten einer Kreditkarte, führte bisher immer zu einem gefährlichen Sicherheitsverlust, da diese Daten auch  
20 nach jedem Gebrauch ihre Identifizierungs- und teilweise sogar Autorisierungsfunktion beibehalten haben. Durch das erfindungsgemäße Verfahren werden die übergebenen Informationen nach dem Gebrauch wertlos und stellen keine Gefahr mehr für den Nutzer dar. Gleichzeitig ist auch die anfragende Institution erfindungsgemäß bezüglich der Angaben über den Nutzer  
25 abgesichert ohne eine eigenständige, stets auf aktuellem Stand zu haltende Datenbank mit sicher identifizierten Nutzern zu unterhalten.

Weiterhin ist der Nutzer nicht mehr gezwungen, mit jedem Geschäftspartner gemeinsam eine sichere Geschäftsverbindung einschließlich einer sicheren Identifizierung aufzubauen, sondern kann gemäß dem erfindungsgemäßen  
30 Verfahren eine sichere Identifizierung über die Datenbank vorzugsweise bei jedem einzelnen Geschäft, bzw. Geschäftspartner durchführen lassen.

Sollten sich persönlichen Daten des Nutzers ändern, beispielsweise im Rahmen eines Wohnortwechsels, so kann der Benutzer über eine einmalig durchzuführende Änderungsmitteilung die Daten in der Datenbank ändern und damit gewährleisten, daß sämtliche Geschäftspartner, welche auf die Daten in dieser Datenbank zugreifen, stets mit den korrekten Angaben arbeiten.

Als Datenbank kommen für das erfindungsgemäße Verfahren zentrale Datenbanken oder auch dezentral organisierte, d.h. verteilte Datenbanken in Frage.

Die Datenbank kann außerdem die Fehlerhäufigkeit durch falsche Informationsübermittlung, insbesondere seitens des Nutzers, reduzieren. Schreib- und Lesefehler in unter Zeitdruck ausgefüllten Formularen verlieren durch das erfindungsgemäße Verfahren an Bedeutung.

Besonders vorteilhaft wird das erfindungsgemäße Verfahren, wenn der Nutzer zu seiner persönlichen Identifizierung dem Dritten seine persönliche Identifikationsnummer und die entsprechende persönliche Authentifizierungsnummer über ein öffentliches Datennetz, beispielsweise das Internet, übermittelt. Insbesondere bei Angeboten über das Internet ist dieses Verfahren zweckmäßig, weil der Nutzer in der Lage ist, eine identische Plattform sowohl für die Kenntnisaufnahme und die Beurteilung des Angebotes, als auch für eine etwaige Annahme des Angebotes zu benutzen. Dieses Vorgehen reduziert den erforderlichen Zeitaufwand und minimiert die Wahrscheinlichkeit eines Fehlers. Bisherige Sicherheitsnachteile, insbesondere bei der Übermittlung persönlicher Angaben über öffentliche Datennetze, werden durch das erfindungsgemäße Verfahren beseitigt.

Für den Dritten, welcher Sicherheit bezüglich der Identität des Nutzers erlangen möchte, ist es sinnvoll, wenn der Dritte die von dem Nutzer erhaltene persönliche Identifikationsnummer und die persönliche Authentifizierungsnummer über ein öffentliches Datennetz an die Datenbank übermittelt. Die Nutzung eines öffentlichen Datennetzes, beispielsweise des Internets, für diesen Datentransfer hat den entscheidenden Vorteil, daß die Überprüfung des Nutzers durch den Dritten mit den entsprechenden

Informationen nicht mehr an einen bestimmten Ort gebunden ist. Die erforderliche Infrastruktur, der Zugang zu dem öffentlichen Datennetz, ist nahezu überall vorhanden. Diese Omnipräsens macht die Nutzung der Datenbank besonders kostengünstig. Da hier ebenfalls die identische Plattform  
5 sowohl für die Übermittlung der Angaben von dem Nutzer an den Dritten, als auch zur Überprüfung der Identität des Nutzers genutzt werden kann, wird auch hier der Zeitaufwand und die Fehlerhäufigkeit entscheidend reduziert. Weiterhin ist es möglich, solche Vorgänge automatisch zu archivieren und jederzeit exakt bezüglich der zeitlichen Abfolge und des Inhalts zu reproduzieren. Die Auskunft  
10 bezüglich der Gültigkeit der persönlichen Identifikationsnummer und der persönlichen Authentifizierungsnummer gibt dem Dritten, beispielsweise einem Warenversandhaus, einen sichere Gewähr bezüglich der Vertrauenswürdigkeit des Nutzers und zeigt auf, ob die Identität des Dritten anhand der Datenbank überprüfbar ist.

15 Eine vorteilhafte Weiterbildung der Erfindung sieht vor, daß der Dritte bei jedem Identifikationsvorgang zusätzlich seine eigene persönliche Identifikationsnummer und eine eigene persönliche Authentifizierungsnummer gemeinsam mit der persönlichen Identifikationsnummer des Nutzers und der persönlichen Authentifizierungsnummer des Nutzers an die Datenbank  
20 übermittelt. Dieses Vorgehen erhöht die Sicherheit des erfindungsgemäßen Verfahrens zusätzlich. Weiterhin sind somit alle Vorgänge aufgrund der Einmaligkeit der persönlichen Authentifizierungsnummern eindeutig reproduzierbar.

Da die Verbindung zwischen dem Dritten und der Datenbank vorzugsweise  
25 auch über ein öffentliches Datennetz besteht, ist es sinnvoll, wenn die an die Datenbank übermittelten Daten und die von der Datenbank zur Verfügung gestellten Daten verschlüsselt sind. Der Aufwand des Verschlüsseln lastet damit zwar nicht mehr auf dem Nutzer, die Sicherheit ist auf diese Weise dennoch gewährleistet.

30 Eine weitere vorteilhafte Möglichkeit, die Daten der Datenbank zu nutzen, ergibt sich, wenn der Dritte die vom Nutzer empfangene persönliche Identifikationsnummer, die persönliche Authentifizierungsnummer und weitere

zu überprüfende Daten des Nutzers über das Datennetz an einen Server, über den die in der Datenbank enthaltenen Informationen abgefragt werden, übermittelt, der Server die zu überprüfenden Daten mit den Daten der Datenbank vergleicht und das Ergebnis dieser Überprüfung dem  
5 auskunftersuchenden Dritten mitgeteilt wird. Auf diese Weise wird bei Vorlage der persönlichen Identifikationsnummer und einer persönlichen Authentifizierungsnummer eines Nutzers der Zugriff auf die persönlichen Daten dieses Nutzers ausgeschlossen. Es ist lediglich das Ergebnis einer Überprüfung erhältlich, wodurch das Risiko des Datenmißbrauchs reduziert wird. Für den  
10 Nutzer bedeutet dies ein besonders hohes Maß an Sicherheit bezüglich seiner persönlichen Daten in der Datenbank, welche nicht bekannt gegeben werden. Für den Dritten, beispielsweise ein Warenversandhaus, ist das Ergebnis einer Identitätsüberprüfung oft ausreichend, um einer kriminellen Machenschaft, beispielsweise einer Bestellung zu einer falschen Adresse, entgegenzuwirken.  
15 Der Nutzer behält die volle Kontrolle über seine persönlichen Daten und der Dritte bekommt die Möglichkeit zur Verifikation der übermittelten Angaben.

Um den Aufwand der Identitätsfeststellung eines Nutzers auf ein Minimum zu reduzieren, sieht eine vorteilhafte Weiterbildung des erfindungsgemäßen Verfahrens vor, daß der Dritte durch die Angabe der Kombination von persönlicher  
20 Identifikationsnummer und der persönlichen Authentifizierungsnummer den Lesezugriff auf einen Teil der in der Datenbank abgelegten persönlichen Daten des Nutzers erhält. Für den Nutzer reduziert sich dadurch der Aufwand einer Geschäftsverbindung mit dem Dritten in der Weise, daß der Nutzer beispielsweise beim Abschluß eines Kaufvertrags für die Annahme eines  
25 Angebotes lediglich das angenommene Angebot spezifizieren muß und seine persönliche Identifikationsnummer mit einer persönlichen Authentifizierungsnummer an den Dritten übermitteln muß. Für die Bestellung bei einem Warenversandhaus können sich die Angaben auf eine Bestellnummer, die persönliche Identifikationsnummer und die persönliche  
30 Authentifizierungsnummer reduzieren. Das bisher notwendige aufwendige Ausfüllen von Formularen, beispielsweise zur Ersterfassung oder Aktualisierung von Kundendaten, entfällt, da sämtliche Daten auf der Datenbank bereitgehalten werden. Auf der Seite des Dritten ist der Aufwand ebenfalls erheblich reduziert, da alle wesentlichen Punkte mit einem Minimum an Datenfluß geregelt werden.

Weiterhin kann der Dritte für Nutzer der Datenbank eine nachhaltige Informationsablage, welche regelmäßig auf aktuellen Stand gebracht werden muß, unterlassen, da im Rahmen jeglichen geschäftlichen Kontaktes sämtliche relevanten Daten von der Datenbank bereitgestellt werden. Ein Warenversandhaus  
5 könnte beispielsweise auf die Aktualisierung eines Kundenverzeichnisses für Bestellvorgänge völlig verzichten.

Eine weitere vorteilhafte Variante des erfindungsgemäßen Verfahrens sieht vor, daß der Nutzer nach erfolgter Identifikation eine Bestätigung dieser Identifikation von der Datenbank erhält. Eine derartige Bestätigung verleiht dem Nutzer eine  
10 zusätzliche Sicherheit bezüglich der bestimmungsgemäßen Verwendung seiner Daten. Ein nicht von ihm autorisierter Vorgang würde auf diese Weise aufgedeckt werden und etwaige Sicherheitslücken beim Nutzer oder in dem System würden über diesen Informationsrückfluß im nachhinein erkannt. Mit Hilfe der äußerst zeitnahen Kommunikation in Form von SMS-Nachrichten,  
15 elektronischer Post und ähnlichen Verfahren hat der Benutzer sogar die Möglichkeit im Falle eines Fehlers oder Mißbrauchs beispielsweise Stornierungen von Warensendungen vorzunehmen.

Da der Umfang der Informationen, welche dem Dritten aus der Datenbank zur Verfügung gestellt werden, um den jeweils angestrebten Zweck der  
20 Informationsübermittlung zu verwirklichen, stets unterschiedlich ist und stark von der Art der geschäftlichen Verbindung zwischen dem Nutzer und dem Dritten abhängt, ist es zweckmäßig, wenn die persönliche Identifikationsnummer und/oder die persönliche Authentifizierungsnummer eine Kodierung enthält, durch die bestimmt wird, welche Daten des Nutzers überprüft werden können,  
25 bzw. auf welche Teile der in der Datenbank registrierten persönlichen Daten der Dritte Zugriff erhält. Handelt es sich beispielsweise um einen kostenfreien Service, welcher jedoch die Kenntnis der Adresse des Nutzers voraussetzt, kann der Nutzer dem Dritten beispielsweise die persönliche Identifikationsnummer mit einer persönlichen Authentifizierungsnummer  
30 zukommen lassen, welche eine Auskunftserteilung oder Überprüfung von Angaben, beispielsweise bezüglich der Bankverbindung, ausschließt. Von besonderer Bedeutung ist hierbei eine Kodierung der persönlichen Identifikationsnummer und/oder der persönlichen Authentifizierungsnummer,

welche im Rahmen eines Kaufvertrages die möglichen Zahlungsmodi von vorne herein festlegt.

Da es sich bei der Adresse und dem Namen des Nutzers um Daten handelt, welche im täglichen Verkehr häufig angegeben werden müssen, ist es sinnvoll  
5 den Namen und/oder die Adresse des Nutzers in der Datenbank zu registrieren.

Weiterhin ist es von Vorteil, wenn in der Datenbank Angaben aus dem Personalausweis des Nutzers registriert sind. Insbesondere beim Umgang mit öffentlichen Behörden kann die Angabe von Daten des Personalausweises von Nutzen sein. Ebenso kann auch die Angabe der Steuernummer, der Sozialversicherung  
10 sicherungsnummer und sonstiger Identnummern von Bedeutung sein.

Eine vorteilhafte Weiterbildung des erfindungsgemäßen Verfahrens sieht vor, daß in der Datenbank biometrische Daten des Nutzers registriert sind. Dies eröffnet beispielsweise die Möglichkeit, eine biometrische Identifizierung eines Nutzers überprüfen zu lassen oder bei der Einrichtung eines biometrischen  
15 Identifizierungssystems der einrichtenden Institution die Aufnahme der biometrischen Daten zu ersparen und diese mittels einer persönlichen Identifikationsnummer und einer persönlichen Authentifizierungsnummer zu dem Zugriff auf die Datenbank zu ermächtigen.

Bisweilen kann es im Rahmen einer derartig effizienten, auf das nötigste  
20 reduzierten Korrespondenz zwischen dem Nutzer, dem Dritten und der Datenbank zu dem Erfordernis eines persönlichen Kontaktes zwischen dem Dritten und dem Nutzer kommen. Zu diesem Zweck ist es sinnvoll, wenn die Datenbank auch Kontaktinformationen zu dem jeweiligen Nutzer enthält. Bei diesen Angaben kann es sich beispielsweise um Telefonnummern, Adressen  
25 elektronischer Post, Faxnummern und ähnliches handeln.

Ein häufig auftretendes Problem ist die sichere Übermittlung von Bankverbindungen und/oder Kreditkarten-Daten des Nutzers an einen Dritten. Insbesondere bei der Übermittlung der Kreditkartendaten kann ein Sicherheitsmangel ungünstige wirtschaftliche Folgen haben. Daher ist es sinnvoll, wenn die  
30 Datenbank auch Informationen über Bankverbindungen und/oder Kreditkarten-

Daten des Nutzers enthält. Auch hier kann aufgrund der Ablage dieser Informationen in der zentral oder auch dezentral organisierten Datenbank stets die notwendige Aktualität dieser Angaben mit geringem Aufwand gewährleistet werden. Die Sicherheit kann zudem aufgrund der Zugriffsbeschränkung durch die persönliche Identifikationsnummer in Kombination mit der persönlichen Authentifizierungsnummer stets gewährleistet werden. Darüber hinaus ist der Nutzer nicht mehr gezwungen sich eine Vielzahl verschiedener Kennungen und persönlicher Identnummern zu merken, da diese sicher in der Datenbank abgelegt werden und der Zugriff bei Bedarf stets erfindungsgemäß durch die Angabe der persönlichen Identnummer in Kombination mit einer persönlichen Authentifizierungsnummer erfolgt.

Im folgenden wird das erfindungsgemäße Verfahren anhand eines speziellen Beispiels unter Bezugnahme auf Abbildungen zur Verdeutlichung näher erläutert. Es zeigen:

- |    |         |  |
|----|---------|--|
| 15 | Fig. 1: | Ein Datennetz als Plattform für das erfindungsgemäße Verfahren,            |
|    | Fig. 2: | Ein Ablaufschema als Beispiel für das erfindungsgemäße Verfahren,          |
| 20 | Fig. 3: | Ein weiteres Ablaufschema als Beispiel für das erfindungsgemäße Verfahren, |
|    | Fig. 4: | Ein Beispiel für eine kodierte persönliche Authentifizierungsnummer.       |

In Figur 1 ist das Internet als Plattform für das erfindungsgemäße Verfahren mit der Bezugsziffer 1 versehen. Einige Elemente dieses öffentlichen Datennetzes, welche für das erfindungsgemäße Verfahren eine besondere Rolle spielen, sind gesondert dargestellt. Im einzelnen handelt es sich dabei um Nutzer 2 bzw. Kunden, den die Identifikation anfragenden Dritten 3, bzw. ein Warenversandhaus und eine zentrale Datenbank 4, in welcher die persönlichen Daten der Nutzer 2 abgelegt sind.

Zunächst veranlaßt der Nutzer 2 einmalig eine Registrierung seiner persönlichen Daten 5 in der zentralen Datenbank 4. Eine Bestätigung dieser Registrierung erhält der Nutzer 2 gemeinsam mit einer persönlichen Identifizierungsnummer (IDNR) 6 und einer Liste 7 einmalig verwendbarer persönlicher Authentifizierungsnummern (PAN) 8 über ein Postidentverfahren.

Nachdem die Identität des Nutzers 2 sicher festgestellt wurde, unterbreitet das Warenversandhaus dem Nutzer 2 Angebote 9 zum Abschluß eines Kaufvertrages über eine Ware 10.

Auf eines der Angebote 9 entschließt sich der Nutzer 2 zum Kauf der Ware 10, welche die Spezifikationen 11 aufweist. Um dem Warenversandhaus seinen Entschluß zur Annahme des Angebots 9 verbindlich mitzuteilen, versendet der Nutzer 2 seine persönliche Identnummer (IDNR) 6 eine persönliche Authentifizierungsnummer (PAN) 8 gemeinsam mit den Spezifikationen 11 der Ware 10 an das Warenversandhaus. Die persönliche Authentifizierungsnummer (PAN) 8 enthält hier eine Kodierung, welche das Warenversandhaus zum Lesezugriff auf die Daten des Nutzers 2 in der zentralen Datenbank 4 ermächtigt. Zu diesem Zweck übermittelt das Warenversandhaus die erhaltene persönliche Identnummer (IDNR) 6 gemeinsam mit der persönlichen Authentifizierungsnummer (PAN) 8 an die zentrale Datenbank 4, welche nach Überprüfung der Identität des Nutzers 2, die Daten 12 an das Warenversandhaus übermittelt. Gleichzeitig ermächtigt die Kodierung in der persönlichen Authentifizierungsnummer (PAN) 8 das Warenversandhaus zur Abbuchung der Rechnungssumme für die bestellte Warensendung unter Verwendung der Bankverbindung des Nutzers 2, welche ebenfalls in der zentralen Datenbank 4 registriert ist. Der Nutzer 2 erhält auf herkömmlichem Warenversandweg 13 seine Ware 10.

Die Figur 3 zeigt ein weiteres Beispiel für das erfindungsgemäße Verfahren. Hier entschließt sich der Nutzer 2 auf ein Angebot 9 zum Kauf der Ware 10 und wählt als Zahlungsmodus die Kreditkarte. Da das Geschäft über das Internet abgewickelt wird, kann der Nutzer 2 keine händische Unterschrift leisten, hat jedoch mit seinem Geldinstitut die Vereinbarung getroffen, daß für solche Fälle eine persönliche Authentifizierungsnummer (PAN) 8 zu übermitteln ist. der

Nutzer übermittelt dem Verkaufsinstitut 16 die persönliche Identifikationsnummer (IDNR) 6, die persönliche Authentifizierungsnummer (PAN) 8, die Spezifikationen 11 zu der Ware 10 und die Kreditkartennummer (CCNR) 17 über das öffentliche Datennetz. Um die  
5 Zahlung des Kaufpreises 18 in die Wege zu leiten, wird dieser gemeinsam mit der persönlichen Identifikationsnummer (IDNR) 6 des Nutzers 2 und der persönlichen Authentifizierungsnummer (PAN) 8 des Nutzers 2 an ein Kreditinstitut, also den bei der zentralen Datenbank 4 nach einer Identifizierung anfragenden Dritten 3 übermittelt. Der Dritte 3 sendet über eine sichere  
10 Verbindung die übermittelte persönliche Identifikationsnummer (IDNR) 6 des Nutzers 2 und die persönliche Authentifizierungsnummer (PAN) 8 des Nutzers 2 und eine eigene persönliche Identifikationsnummer (IDNR) 14 mit einer eigenen persönlichen Authentifizierungsnummer (PAN) 15 an die zentrale Datenbank 4, welche die Gültigkeit der Kombination der persönlichen  
15 Identifikationsnummer (IDNR) 6 des Nutzers 2 mit der persönlichen Authentifizierungsnummer (PAN) 8 des Nutzers 2 überprüft. Ist das Ergebnis dieser Überprüfung positiv, übermittelt die zentrale Datenbank 4 die Bestätigung an den die Identifikation anfragenden Dritten 3 und die Zahlung wird in die Wege geleitet.

20 In Figur 4 ist ein Aufbau einer kodierten persönlichen Authentifizierungsnummer (PAN) 8 dargestellt. Die persönliche Authentifizierungsnummer (PAN) 8 besteht hier aus neun Zahlen 20 und drei Buchstaben 21, welche nur mit angegeben werden, wenn der anfragende Dritte 3 Auskünfte, die Bankverbindung des Nutzers 2 betreffend, erhalten soll.

### Patentansprüche

1. Verfahren zur persönlichen Identifizierung eines Nutzers (2) in einem Datennetz durch einen Dritten (3), bei welchem dem Nutzer (2) eine persönliche Identifikationsnummer (IDNR) (6) zugeordnet ist und seine persönlichen Daten in einer Datenbank (4) registriert sind, d a d u r c h g e k e n n z e i c h n e t , daß der Nutzer (2) dem Dritten (3) zusätzlich zu der persönlichen Identifikationsnummer (IDNR) (6) eine für jeden Identifikationsvorgang zur Verfügung gestellte, einmalig verwendbare persönliche Authentifizierungsnummer (PAN) (8) mitteilt und daß der Dritte (3) auf der Basis einer Kombination der mitgeteilten persönlichen Identifikationsnummer (IDNR) (6) und der persönlichen Authentifizierungsnummer (PAN) (8) von der Datenbank (4) eine Identifikation des Nutzers (2) erhält.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Nutzer (2) zu seiner persönlichen Identifizierung dem Dritten (3) seine persönliche Identifikationsnummer (IDNR) (6) und eine persönliche Authentifizierungsnummer (PAN) (8) über ein öffentliches Datennetz übermittelt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Dritte (3) die von dem Nutzer (2) erhaltene persönliche Identifikationsnummer (IDNR) (6) die persönliche Authentifizierungsnummer (PAN) (8) über ein öffentliches Datennetz an die Datenbank (4) übermittelt.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Dritte (3) bei jedem Identifikationsvorgang zusätzlich seine eigene persönliche Identifikationsnummer (IDNR) (14) und eine eigene persönliche Authentifizierungsnummer (PAN) (15) gemeinsam mit der persönlichen Identifikationsnummer (IDNR) (6) des Nutzers und der persönlichen Authentifizierungsnummer (PAN) (8) des Nutzers an die Datenbank übermittelt.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die an die Datenbank (4) übermittelten Daten und die von der Datenbank (4) zur Verfügung gestellten Daten verschlüsselt sind.

10 6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Identifikation des Nutzers (2) nur eine Bestätigung der Gültigkeit der Kombination der übermittelten persönlichen Identifikationsnummer (IDNR) (6) und der persönlichen Authentifizierungsnummer (PAN) (7) gegenüber dem Dritten (3) beinhaltet.

15 7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Identifikation des Nutzers (2) eine Bestätigung der Gültigkeit und Richtigkeit der Kombination der übermittelten persönlichen Identifikationsnummer (IDNR) (6) und der persönlichen Authentifizierungsnummer (PAN) (7) und weiteren übermittelten persönlichen Daten des Nutzers gegenüber dem Dritten  
20 beinhaltet.

8. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Dritte (3) durch die Angabe der Kombination von persönlicher Identifikationsnummer (IDNR) (6) und der persönlichen Authentifizierungsnummer (PAN) (8) den Lesezugriff auf einen Teil der in der  
25 Datenbank (4) abgelegten persönlichen Daten des Nutzers (2) erhält.

9. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Nutzer (2) nach erfolgter Identifikation eine Bestätigung dieser Identifikation von der Datenbank (4) erhält.

10. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die persönliche Identifikationsnummer (IDNR) (6) und/oder die persönliche Authentifizierungsnummer (PAN) (8) eine Kodierung enthält, durch die bestimmt wird, welche Daten des Nutzers (2) überprüft werden können, beziehungsweise auf welche Teile der in der Datenbank (4) registrierten persönlichen Daten der Dritte (3) Zugriff erhält.

11. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in der Datenbank (4) der Name und/oder die Adresse des Nutzers (2) registriert ist.

12. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in der Datenbank (4) Angaben aus dem Personalausweises des Nutzers (2) registriert sind.

13. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in der Datenbank (4) biometrische Daten des Nutzers (2) registriert sind.

14. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in der Datenbank (4) Kontaktinformationen zu dem Nutzer (2) registriert sind.

15. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß in der Datenbank (4) Bankverbindungen und/oder Kreditkarten-Daten des Nutzers (2) registriert sind.

16. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die persönliche Identifikationsnummer (IDNR) (6) und/oder die persönliche Authentifizierungsnummer (PAN) (8) sowohl aus Zahlen als auch aus Buchstaben besteht.

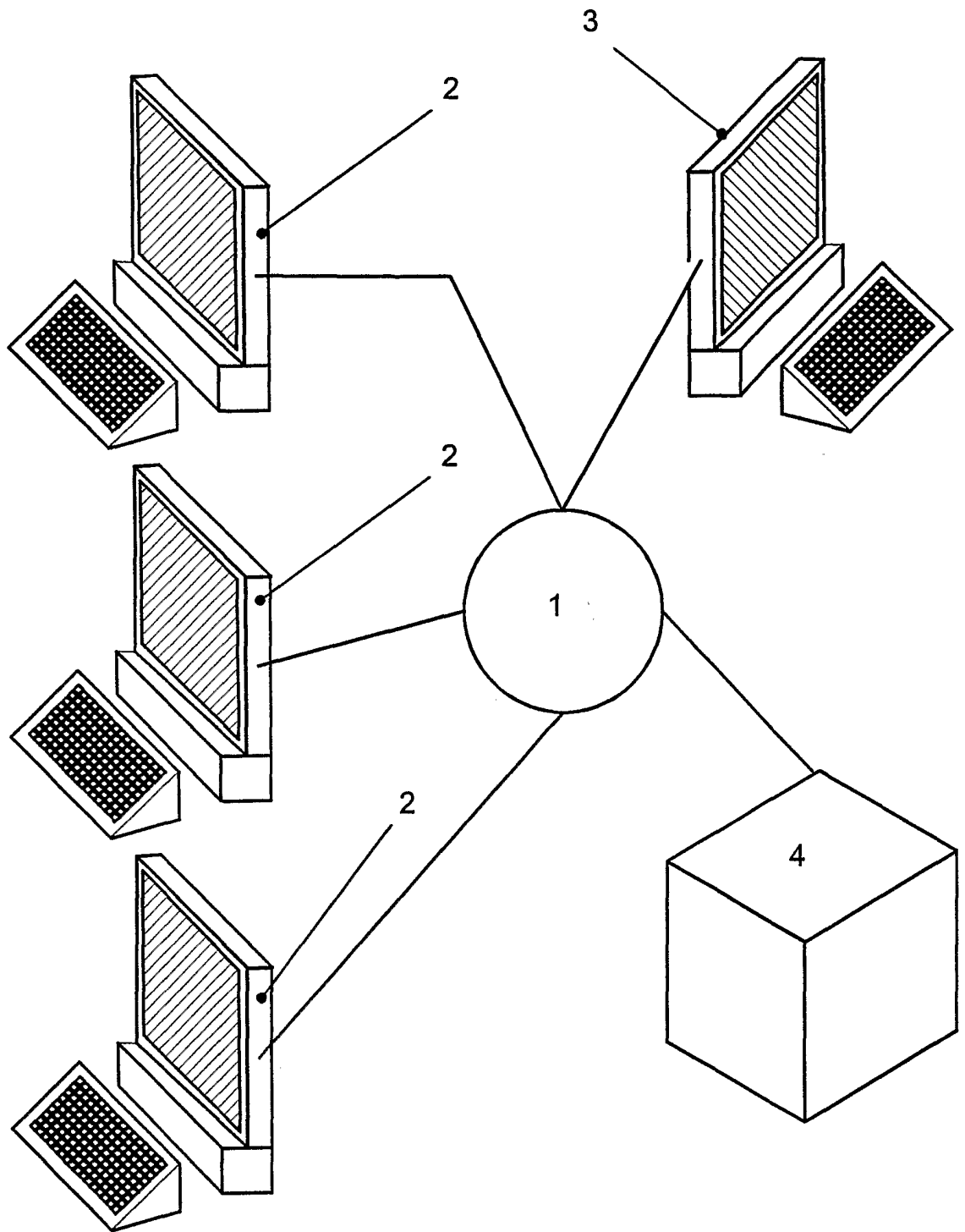


Fig. 1

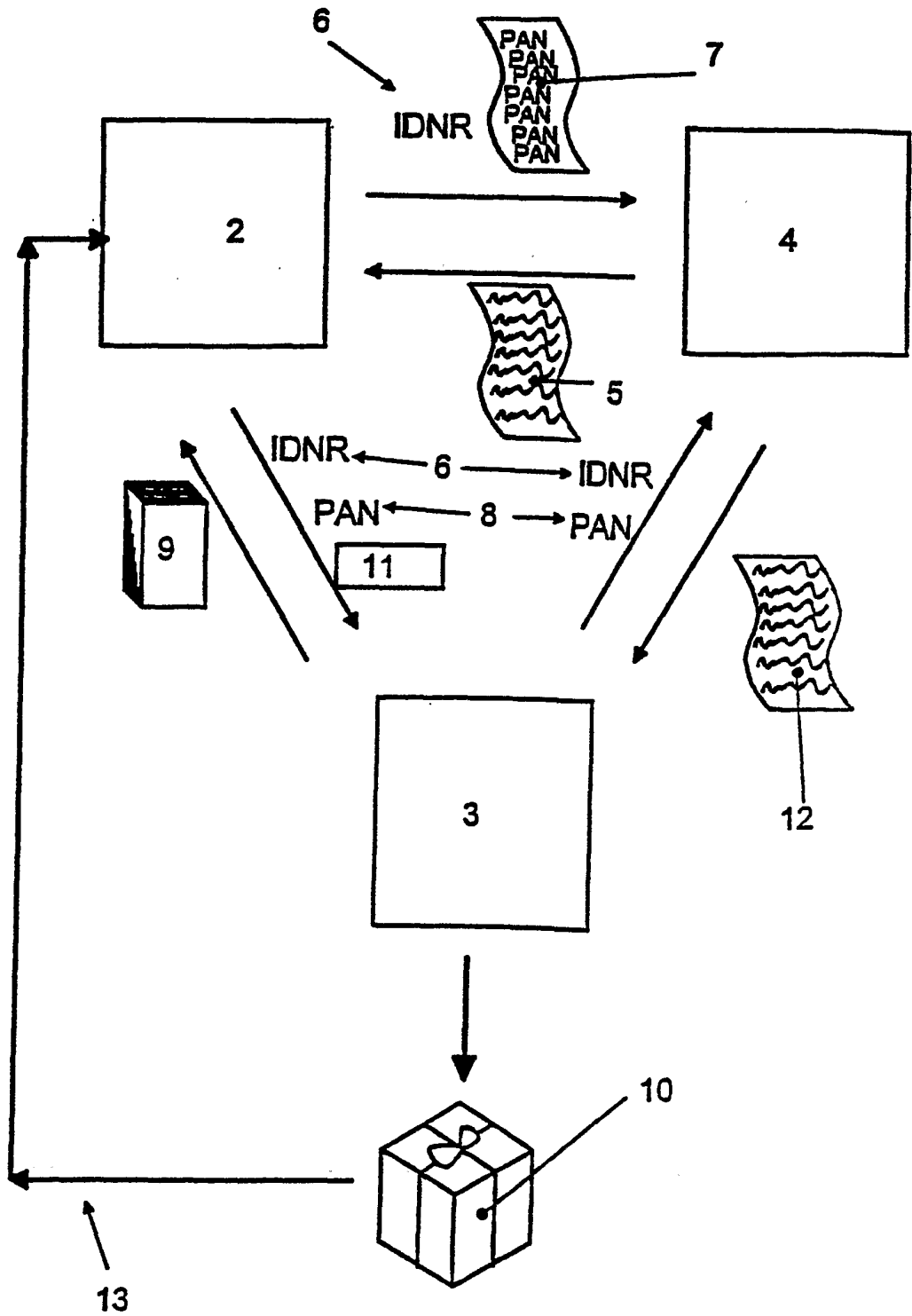


Fig. 2

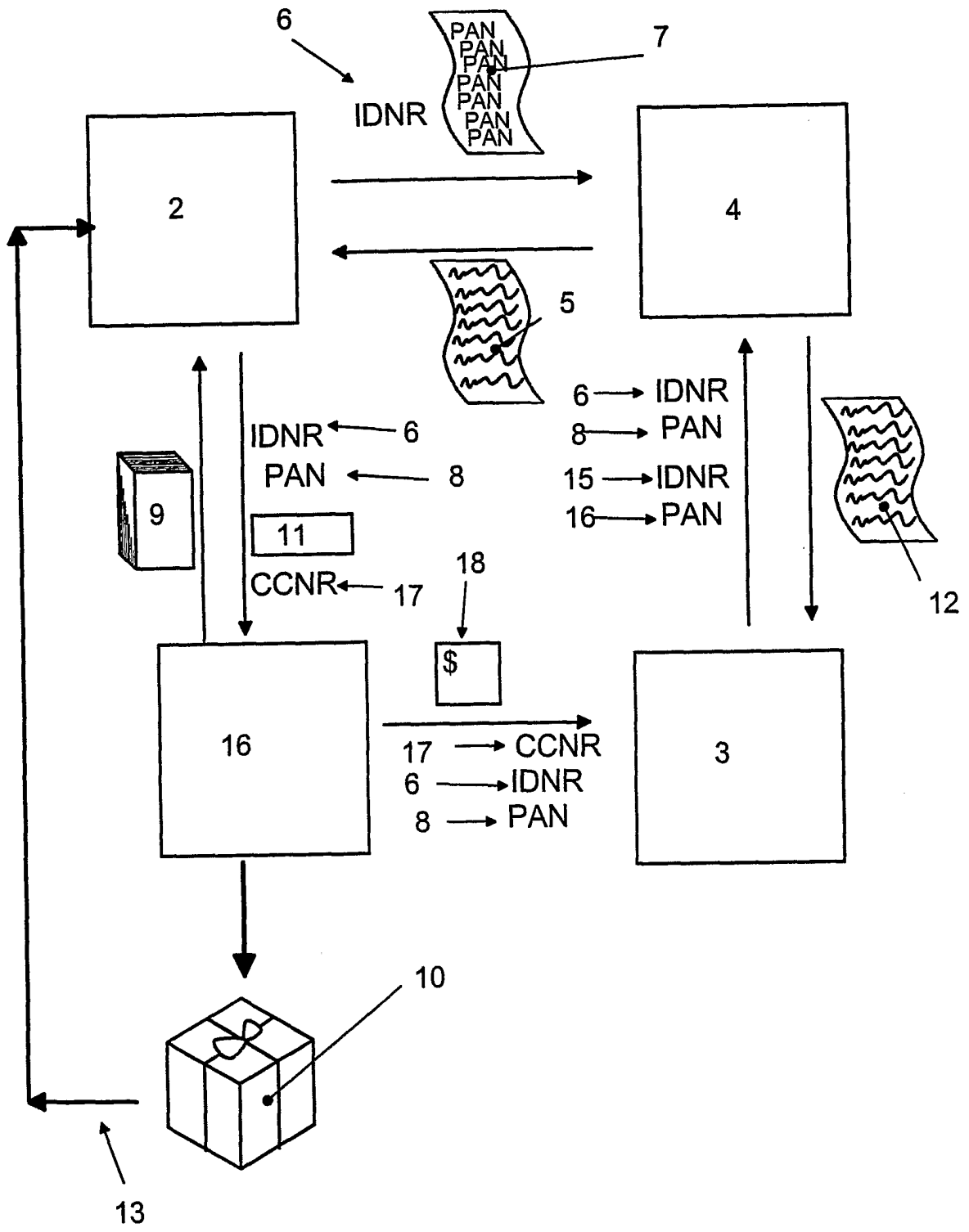


Fig. 3

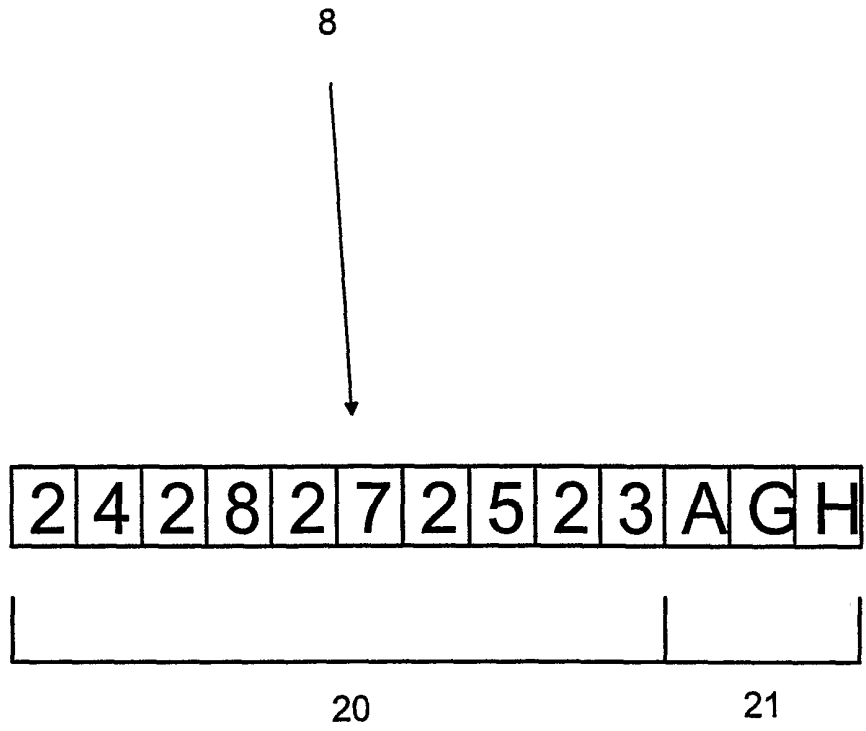


Fig. 4