



(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2011 115 827.1**
 (22) Anmeldetag: **13.10.2011**
 (43) Offenlegungstag: **18.04.2013**

(51) Int Cl.: **H04L 9/32 (2011.01)**

(71) Anmelder:
Deutsche Telekom AG, 53113, Bonn, DE

Melanie, 46569, Hünxe, DE; Petschinka, Thomas, 90482, Nürnberg, DE; Quirnbach, Matthias, 44801, Bochum, DE; Trinkel, Marian, 52372, Kreuzau, DE; Tilp, Johann, 85296, Rohrbach, DE; Hahn, Roland, 04328, Leipzig, DE; Düsterhöft, Friedhelm, 47249, Duisburg, DE

(74) Vertreter:
COHAUSZ HANNIG BORKOWSKI WIRGOTT, 40237, Düsseldorf, DE

(72) Erfinder:
Büscher, Dominik, 56244, Helferskirchen, DE; Biet, Liane, 56412, Welschneudorf, DE; Birmes, Wolfgang, 40479, Düsseldorf, DE; Lindemann,

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 2007 / 0 041 620 A1
US 2010 / 0 071 041 A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

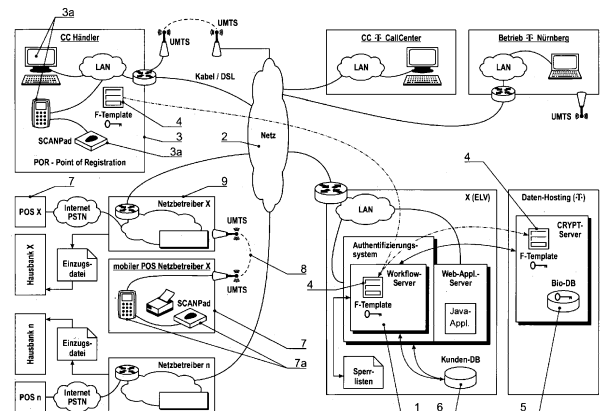
Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Der Inhalt dieser Schrift weicht von den am Anmeldetag eingereichten Unterlagen ab.

(54) Bezeichnung: **System und Verfahren zur Freischaltung eines Dienstes**

(57) Zusammenfassung: Die Erfindung betrifft ein System und ein Verfahren zur Freischaltung eines Dienstes für einen Benutzer bei dem mit einem Dienstterminal (7a), insbesondere dem einem Dienstanbieter zugeordneten Dienstterminal (7a) eine biometrische Kennung (4) des Benutzers, insbesondere ein Fingerscan, erfasst wird und bei einem Vorhandensein der biometrischen Kennung (4) in einer Kennungsdatenbank (5) der Benutzer zur Benutzung des Dienstes zugelassen wird, bei dem die biometrische Kennung (4) zusammen mit wenigstens einer Zusatzkennung in einem oder mehreren Kommunikationsschritten an einen, insbesondere zentralen Server (1) übermittelt wird, wobei der insbesondere zentrale Server (1) in einem, insbesondere dienstunabhängigen Kommunikationsnetzwerk betrieben wird und von dem Dienstterminal (7a) zur Übermittlung angewählt wird, der insbesondere zentrale Server (1) durch Zugriff auf eine biometrische Kennungen (4) enthaltende Kennungsdatenbank (5) und Vergleich mit den dort gespeicherten Kennungen überprüft, ob die erhaltene biometrische Kennung (4) in der Kennungsdatenbank (5) vorhanden ist und zu einer vorhandenen biometrischen Kennung (4) wenigstens einen der Kennung (4) zugeordneten Benutzeridentifikator aus der Kennungsdatenbank (5) ausliest, wobei die Kennungsdatenbank (5) zumindest logisch in Speicherbereiche unterteilt ist, die jeweils einer in der Kennungsdatenbank (5) vorkommenden Zusatzkennung zugeordnet sind und in denen vorkommende biometrische Kennungen (4) jeweils derselben Zusatzkennung gespeichert sind und die Überprüfung auf das Vorhandensein einer übermittelten biometrischen Kennung (4) in der Kennungsdatenbank (5) innerhalb desjenigen Speicherbereichs erfolgt, welcher der wenigstens einen übermittelten Zusatzkennung zugeordnet ist und der insbesondere zen-

trale Server (1) an das Dienstterminal (7a) bei Vorhandensein der biometrischen Kennung (4) in der Kennungsdatenbank (5) an das Dienstterminal (7a) eine Freigabemitteilung kommuniziert zur Zulassung des Benutzers für den angefragten Dienst, insbesondere ansonsten eine Sperrmitteilung kommuniziert.



Beschreibung

[0001] Die Erfindung betrifft ein System sowie auch ein Verfahren zur Freischaltung eines Dienstes für einen Benutzer, bei dem mit einem Dienstterminal, insbesondere einem Dienstterminal, das einem Dienstanbieter zugeordnet ist, eine biometrische Kennung des Benutzers, insbesondere ein Fingerscan, erfasst wird und bei einem Vorhandensein der biometrischen Kennung in einer Kennungsdatenbank der Benutzer zur Benutzung des Dienstes zugelassen wird, insbesondere anderenfalls, wenn die biometrische Kennung in einer Kennungsdatenbank nicht aufgefunden wird, von der Benutzung des Dienstes ausgeschlossen wird.

[0002] Verfahren und Systeme dieser Art sind im Stand der Technik bekannt und werden beispielsweise eingesetzt, um einen bargeldlosen Bezahlvorgang an Supermarktkassen durchzuführen.

[0003] Hierfür kann es vorgesehen sein, an Supermarktkassen ein Dienstterminal einzusetzen, mit dem der Fingerabdruck eines Benutzers, hier eines Kunden des Supermarktes, der Waren im Supermarkt kaufen möchte, erfasst wird, woraufhin sodann durch Vergleich überprüft wird, ob die den Fingerabdruck repräsentierende biometrische Kennung dieses Benutzers in einer Kennungsdatenbank vorhanden ist, die der Supermarkt unterhält und in die sich ein Benutzer bei einer Registrierung für einen solchen Bezahlvorgang mit seiner biometrischen Kennung eingetragen hat.

[0004] So kann bei erfolgreichem Auffinden der erfassten biometrischen Kennung eines Benutzers unter den gespeicherten Kennungen der Bezahlvorgang für diesen Benutzer an der Supermarktkasse frei gegeben werden, wobei weiterhin der Dienstanbieter, hier der Supermarkt, das Geld für die Bezahlung der Waren beispielsweise durch ein automatisches elektronisches Lastschriftverfahren erhält anhand der Daten des Benutzers, die im Zusammenhang mit der biometrischen Kennung gespeichert sind, wie beispielsweise Name und Kontoverbindung. Ein solches Verfahren ist nicht auf einen Bezahlvorgang an einer Supermarktkasse beschränkt, sondern kann grundsätzlich für jegliche Art von Dienst verwendet werden, für den sich ein Benutzer freischalten bzw. authentifizieren/identifizieren/verifizieren lassen muss. Dies können z. B. auch Warenausgabeautomaten sein, automatische Zugangskontrollen etc.

[0005] Eine biometrische Kennung im Sinne der Erfindung ist hier vorliegend jede datentechnische Repräsentation eines Körpermerkmals eines Benutzers, wie beispielsweise die Daten-Repräsentation des Fingerabdrucks, z. B. in der Art eines sogenannten Templates, welches durch einen vorbestimmten Algorithmus erstellt wird, der in einem Fingerscanner

implementiert ist. In gleicher Weise besteht jedoch auch die Möglichkeit, statt eines Fingerabdrucks andere biologische Körpermerkmale zu erfassen und in elektronisch verarbeitbare Daten und somit in eine biometrische Kennung im Sinne der Erfindung umzusetzen. Beispielsweise kann auch ein Iris-Abbild des Auges des Benutzers oder eine Sprachprobe oder sonstiges körperliches Merkmal zur Erfassung einer biometrischen Kennung genutzt werden.

[0006] Als nachteilig wird es bei den bislang im Stand der Technik bekannten Verfahren empfunden, dass im Wesentlichen jeder Dienstanbieter, also beispielsweise jeder Supermarkt, der das elektrische Lastschriftverfahren über Fingerabdruck anbietet, seine eigene Datenbank unterhält und somit auch jeder Benutzer dieses Verfahrens, z. B. jeder Kunde eines Dienstanbieters sich bei jedem jeweiligen Dienstanbieter separat für die Durchführung des Dienstes registrieren muss, was als lästig und aufwändig empfunden wird.

[0007] Darüber hinaus ist es ein weiterer Nachteil der bekannten Verfahren, dass mit zunehmender Anzahl registrierter Benutzer in einer Datenbank die Zugriffs- und Überprüfungszeiten stark zunehmen, da für die Durchführung des Dienstes bzw. die Freischaltung des Benutzers für diesen Dienst eine immer größere Anzahl hinterlegter biometrischer Kennungen verglichen werden muss mit der aktuell von einem den Dienst in Anspruch nehmenden Benutzer eingelesenen biometrischen Kennung. Dies kann zu unerwünscht hohen Wartezeiten an Dienstterminals führen, beispielsweise an solchen Dienstterminals, wie sie an Supermarktkassen für das bargeldlose Bezahlen zur Verfügung stehen. Lange Wartezeiten hingegen führen zu einer Unzufriedenheit bei den Benutzern und zu einer geringen Akzeptanz eines solchen Verfahrens.

[0008] Es ist daher die Aufgabe der Erfindung, ein System und ein Verfahren der eingangs genannten Art bereit zu stellen, welches die vorgenannten Nachteile nicht aufweist, welches somit insbesondere schnelle Überprüfungszeiten bei der Prüfung auf das Vorhandensein einer erfassten biometrischen Kennung eines Benutzers innerhalb der in einer Datenbank gespeicherten biometrischen Kennungen aller Benutzer bietet und welches in weiterer Bevorzugung auch die Möglichkeit bereitstellt, dass sich ein Benutzer nur einmalig für die Benutzung von grundsätzlich beliebigen Diensten bzw. für beliebige Dienstanbieter registrieren muss, nicht jedoch, wie bislang im Stand der Technik bei jedem Dienstanbieter oder jeden Dienst separat.

[0009] Diese Aufgabe wird erfindungsgemäß dadurch gelöst, dass bei einem Verfahren der vorbeschriebenen gattungsgemäßen Art die biometrische Kennung zusammen mit wenigstens einer Zusatz-

kennung in einem oder mehreren Kommunikationsschritten an einen z. B. zentralen Server übermittelt wird, wobei der Server in einem, insbesondere allgemein zugänglichen Kommunikationsnetzwerk betrieben wird und von dem Dienstterminal zur Übermittlung angewählt wird und der bevorzugt zentrale Server durch Zugriff auf eine biometrische Kennungen enthaltende Kennungsdatenbank und Vergleich der erhaltenen Kennung mit den dort gespeicherten Kennungen überprüft, ob die erhaltene biometrische Kennung in der Kennungsdatenbank vorhanden ist und zu einer vorhandenen biometrischen Kennung wenigstens einen der Kennung zugeordneten Benutzeridentifikator aus der Kennungsdatenbank ausliest.

[0010] Erfindungsgemäß ist dabei die Kennungsdatenbank zumindest logisch in Speicherbereiche unterteilt, die jeweils wenigstens einer in der Kennungsdatenbank vorkommenden Zusatzkennung zugeordnet sind und in denen die vorkommende biometrischen Kennungen gespeichert sind, die jeweils derselben Zusatzkennung zugeordnet sind.

[0011] Erfindungsgemäß erfolgt so die Überprüfung auf das Vorhandensein einer übermittelten biometrischen Kennung in den Kennungen der Kennungsdatenbank nur innerhalb desjenigen Speicherbereichs, welcher der wenigstens einen zusätzlich übermittelten Zusatzkennung zugeordnet ist, wobei weiterhin der bevorzugt zentrale Server an das Dienstterminal bei Vorhandensein der biometrischen Kennung in der Kennungsdatenbank, insbesondere in dem zugeordneten Speicherbereich, eine Freigabemitteilung kommuniziert zur Zulassung des Benutzers für den angefragten Dienst, insbesondere ansonsten eine Sperrmitteilung kommuniziert, d. h. den Benutzer nicht zulässt.

[0012] Der wesentliche Kerngedanke der Erfindung beruht hier darauf, für die Überprüfung, ob ein Benutzer für den angefragten Dienst – beispielsweise eine Bezahlung im Rahmen eines elektronischen Lastschriftverfahrens – zugelassen wird oder nicht, nicht die gesamte Kennungsdatenbank zu durchsuchen, sondern nur den Speicherbereich der Kennungsdatenbank, welche zumindest logisch der wenigstens einen oder ggfs. auch mehreren Zusatzkennungen zugeordnet ist. Hierdurch wird der Suchvorgang wesentlich beschleunigt.

[0013] Eine solche Zusatzkennung kann in einer Ausführungsform z. B. durch eine Kennung des Dienstterminals gegeben sein, z. B. durch eine Kennung, die das Dienstterminal im Netzwerk hat, über welches das Dienstterminal kommuniziert, z. B. mit dem bevorzugt zentralen Server. Eine solche Kennung kann z. B. die sogenannte CLI – Calling Line Identity im Telefonnetz, oder eine Netzwerkkennung/IP-Adresse oder HLR – Home Location Register im Mobilfunknetz oder eine Gerätenummer (IMEI – In-

ternational Mobile Equipment Identity) oder eine auf sonstige Art zugeordnete, z. B. im Dienstterminal gespeicherte Kennung sein.

[0014] So kann z. B. auch jeder Dienstanbieter (z. B. Supermarkt) seinen Dienstterminals eigene Kennungen zuordnen. In der Kennungsdatenbank können sich so Speicherbereiche ergeben, die durch die Kennungen der einzelnen Dienstterminals letztendlich den Dienstanbietern zugeordnet sind.

[0015] Beispielsweise kann so jeder Dienstanbieter, z. B. Supermarkt in der Kennungsdatenbank seinen eigenen Speicherbereich haben, in dem die biometrischen Kennungen der Kunden des Dienstanbieters/Supermarktes gespeichert sind. Wenn also z. B. eine Kunde bei einem Supermarkt **1** einkauft, so braucht bei der Bezahlung der Waren in der Kennungsdatenbank nur der Speicherbereich nach der biometrischen Kennung durchsucht werden, welcher dem Supermarkt **1** zugeordnet ist, nicht jedoch die Speicherbereiche anderer Supermärkte oder allgemein anderer Dienstanbieter.

[0016] In einer anderen Ausführungsform kann es auch vorgesehen sein, eine Zusatzkennung zusätzlich von einem Benutzer zu erfassen, z. B. dadurch dass dieser Benutzer eine solche Zusatzkennung am Dienstterminal oder seinem separaten Terminal eingibt bzw. durch dieses erfassen lässt.

[0017] Eine solche Zusatzkennung kann z. B. von einer einem Benutzer zugeordneten Karte, z. B. mit Chip oder Magnetstreifen oder RFID ausgelesen werden, wie z. B. Personalausweis, Kreditkarte, Bankkarte, Bonuskarte etc. Dabei dient eine solche Karte und die darauf gespeicherte Zusatzkennung im Wesentlichen nicht zur unmittelbaren Identifizierung des Benutzers, sondern zur Definition eines Speicherbereichs in der Kennungsdatenbank und zur Beschleunigung des Suchverfahrens. Z. B. kann das Dienstterminal eingerichtet sein, solche die Zusatzkennung bildenden Kartendaten mit entsprechenden Empfangsmitteln, z. B. Magnetstreifenleser, Chip- oder RFID-Leser zu erfassen.

[0018] Hier kann es auch vorgesehen sein, von solchen Karten Nummernfolgen zu erfassen, die als Zusatzkennung verwendet werden. Dabei kann es, insbesondere bei einer sehr hohen Anzahl von Nummern/Ziffern einer solchen Nummernfolge einer Karte vorgesehen sein, die als Zusatzkennung zu verwendende Nummernfolge als Teilnummernfolge aus der gesamten Nummernfolge einer Karte zu bilden, z. B. gemäß einer vorbestimmten Regel, da es – wie beim späteren Ausführungsbeispiel beschrieben wird – nicht darauf ankommt, durch die Nummernfolge selbst einen Benutzer zu individualisieren.

[0019] In einer weiteren Ausführung kann es auch vorgesehen sein, dass von dem Benutzer nicht nur eine biometrische Kennung, z. B. ein Fingerabdruck erfasst wird, sondern gleichzeitig von diesem Benutzer auch als Zusatzkennung eine (bei einer vorherigen Registrierung gewählte) Nummernfolge (PIN) erfasst wird, beispielsweise dadurch, dass der Benutzer eine solche auf einem Tastenfeld des Dienstterminals oder eines separaten Terminals eingeben muss.

[0020] Hierfür kann bevorzugt ein Dienstterminal z. B. in einer einzigen Baueinheit ein Tastenfeld und eine Erfassungseinheit für biometrische Kennungen, z. B. einen Fingerscanner umfassen, wenngleich auch eine separate Anordnung von Tastenfeld und biometrischen Erfassungseinheit möglich ist. Ein Dienstterminal kann darüber hinaus eingerichtet sein zusätzlich zur biometrischen Kennung und ggfs. einer Nummernfolge auch Bilder/Videos oder – wie zuvor genannt – Kartendaten zu erfassen.

[0021] Es kann vorgesehen sein, dass in einem vorgelagerten Registrierungs-Schritt ein Benutzer bei einer Erfassung einer biometrischen Kennung eine von ihm gewählte Nummernfolge als erfindungsgemäße Zusatzkennung wählen muss mit einer vorbestimmten Anzahl von Stellen, insbesondere wenigstens zwei Stellen. Hierbei kann der Benutzer z. B. auch mehrere biometrische Kennungen hinterlegen, z. B. im einfachsten Fall die gescannten Abdrücke verschiedener Finger.

[0022] So hat das erfindungsgemäße Verfahren durch die Bereitstellung einer biometrischen Kennung sowie auch die Bereitstellung einer Zusatzkennung, z. B. durch Eingabe einer Nummernfolge oder Einlesen einer solchen Nummernfolge von einer Karte bei der Inanspruchnahme eines Dienstes zum einen eine höhere Sicherheit als die bislang im Stand der Technik bekannten Verfahren, die lediglich ausschließlich auf eine biometrische Kennung abstellen, wie beispielsweise einen Fingerabdruckscan, da bei dem erfindungsgemäß hier verwendeten Verfahren zusätzlich die Zusatzkennung zur Suche verwendet wird, insbesondere eine von einem Benutzer individuell gewählte Nummernfolge abgefragt wird, insbesondere die lediglich hinsichtlich der Stellenanzahl der Nummer durch das Verfahren bzw. das System vorbestimmt wird.

[0023] Beispielsweise kann es vorgesehen sein, eine vierstellige oder fünfstellige Nummernfolge bei der Registrierung auszuwählen, die sodann für die zukünftige Inanspruchnahme eines Dienstes am Dienstterminal zusätzlich zur biometrischen Kennung einzugeben ist. Die Auswahl kann dadurch erfolgen, dass ein Benutzer sich eine beliebige Nummernfolge ausdenkt oder aber auch, dass der Benutzer eine seiner Karten wählt und davon eine Nummernfolge oder

Teilnummernfolge gelesen und dem Benutzer zugeordnet wird.

[0024] Neben dieser zusätzlichen Sicherheit ist der ganz wesentliche Erfindungsgedanke jedoch darauf ausgerichtet, dass durch die Verwendung der zusätzlichen Zusatzkennung und besonders der Nummernfolge ein ganz wesentlicher Geschwindigkeitsvorteil erzielt wird bei der Abfrage der Kennungsdatenbank, welche gespeicherte Kennungen und Zusatzkennungen insbesondere Nummernfolgen umfasst, um zu überprüfen, ob die Kennung, die der Benutzer an dem Dienstterminal z. B. als Fingerscan abgegeben hat, in der Kennungsdatenbank vorhanden ist.

[0025] Dieser erhebliche Geschwindigkeitsvorteil beruht bei der Verwendung einer Nummernfolge als Zusatzkennung auf der Überlegung, dass bei der zusätzlichen Verwendung einer Nummernfolge mit einer vorbestimmten Anzahl von Ziffern bzw. Stellen, in einem hier verwendeten Beispiel von lediglich vier Ziffern, sich eine Wahrscheinlichkeit ergibt, dass unter der Menge aller registrierter Benutzer sich mehrere Benutzer finden, die zufällig dieselbe Nummernfolge in Ergänzung zu ihrer eindeutigen, individuellen biometrischen Kennung auswählen.

[0026] Mit Bezug auf das genannte Beispiel einer vierstelligen Nummernfolge ergeben sich insgesamt mögliche Zahlen von 0000–9999, d. h. insgesamt 10.000 verschiedene Zahlen, die durch die alle Benutzer als zusätzliche individuelle Nummernfolge ausgewählt werden können. Nimmt man zur Vereinfachung an, dass jede der 10.000 insgesamt zur Verfügung stehenden vierstelligen Nummernfolgen mit gleicher Wahrscheinlichkeit von den Benutzern gewählt werden, so kann in diesem Beispiel weiterhin vereinfacht angenommen werden, dass bei einer Anzahl von einer Million teilnehmenden und registrierten Benutzern jede der 10.000 Nummernfolgen im statistischen Durchschnitt 100mal ausgewählt wurde, tatsächlich wird die Auswahlwahrscheinlichkeit jedoch von dieser vereinfachten Annahme abweichen.

[0027] Durch die zumindest logische Organisation der Kennungsdatenbank in den Nummernfolgen zugeordnete Speicherbereiche kann so gemäß der Erfindung bewirkt werden, dass es eine von der Stellenzahl der Nummernfolge abhängige Anzahl von Speicherbereichen gibt, im vorliegenden Fall nämlich 10.000 Speicherbereiche, in denen jeweils 100 biometrische Kennungen gespeichert sind. Beispielsweise kann also jede mögliche Nummernfolge wenigstens einem, insbesondere genau einem Speicherbereich zugeordnet sein.

[0028] Mit Bezug auf das beschriebene Beispiel wird somit deutlich, dass bei einer Abfrage der Kennungsdatenbank zur Überprüfung, ob ein Benutzer für den angefragten Dienst freizuschalten oder abzulehnen

ist, in Abhängigkeit der von dem Benutzer eingegebenen Nummernfolge lediglich in der Kennungsdatenbank derjenige Speicherbereich auf das Vorhandensein der biometrischen Kennung überprüft werden muss, welcher dieser von dem Benutzer eingegebenen Nummernfolge zugeordnet ist und somit wiederum mit Bezug auf das genannte Beispiel bei einer Million Benutzern lediglich 100 biometrische Kennungen mit der aktuell von dem Benutzer zur Verfügung gestellten Kennung zu vergleichen sind, nicht hingegen sämtliche Kennungen der insgesamt eine Million gespeicherten Benutzer.

[0029] Das erfindungsgemäße Verfahren zur Durchführung des Vergleichs bietet demnach einen erheblichen Geschwindigkeitsvorteil, der sich ausschließlich durch die zusätzlich verwendete Nummernfolge ergibt.

[0030] Das erfindungsgemäße Verfahren bietet demnach besonders dann Vorteile, wenn eine besonders hohe Anzahl von Benutzern für die Durchführung des Verfahrens registriert sind und hilft somit Wartezeiten bei der Freischaltung oder Ablehnung eines Benutzers hinsichtlich des angefragten Dienstes zu vermeiden, was beispielsweise an Supermarktkassen zu Stoßzeiten ein wesentliches Kriterium ist.

[0031] Der erfindungsgemäße Vorteil ergibt sich insbesondere dann, wenn es vorgesehen ist, die Überprüfung einer an einem Dienstterminal erfassten biometrischen Kennung auf das Vorhandensein innerhalb der Kennungsdatenbank nicht nur für einen bestimmten Dienst, wie z. B. das elektronische Lastschriftverfahren von einer Girokontoverbindung einzusetzen, sondern erfindungsgemäß für eine Vielzahl verschiedener Dienste, z. B. im einfachsten Fall unterschiedlicher Bezahlverfahren, wie z. B. einerseits Lastschrifteinzug vom Girokonto sowie andererseits auch Kreditkartenzahlung von einer Kreditkartennummer etc.

[0032] So kann nämlich das erfindungsgemäße Verfahren aufgrund der dienstübergreifenden Anwendung eine deutlich höhere Nutzeranzahl aufweisen bzw. verarbeiten als im Stand der Technik bekannte Verfahren, die beispielsweise nur für einen Dienstanbieter oder nur für einen ganz bestimmten Dienst durchgeführt werden und insofern die Kennungsdatenbanken bei diesen bekannten Verfahren hinsichtlich der Anzahl der Benutzer starke Beschränkung aufweisen.

[0033] So zeichnet sich das erfindungsgemäße Verfahren in bevorzugter Ausführung gerade dadurch aus, dass der zentrale Server in einem dienstunabhängigen Kommunikationsnetzwerk betrieben wird, was bedeutet, dass dieser Server innerhalb des Kommunikationsnetzwerkes von außen durch grundsätzlich beliebige Dritte, insbesondere am Server an-

gemeldete Dritte, in Anspruch genommen werden kann, also keine proprietäre Beschränkung hat, so dass verschiedene Dienstanbieter, wie beispielsweise unterschiedliche Supermarktketten, den zentralen Server sowie die damit in Verbindung stehende Kennungsdatenbank für wenigstens einen, gegebenenfalls auch mehrere Dienste, insbesondere unterschiedliche Arten von Bezahldiensten, in Anspruch nehmen können.

[0034] So wird die Notwendigkeit, entsprechende Rechner- und Datenbankressourcen bei jedem Dienstanbieter separat für diesen vorzuhalten, zentralisiert und gemäß der Erfindung in ein Netzwerk ausgelagert, auf welches von außen zugegriffen werden kann über an das Netzwerk direkt oder über andere Netzwerke angeschlossene Dienstterminals. Beispielsweise kann es sich bei dem Netzwerk um das Internet handeln, in welchem der zentrale Server eingebunden ist.

[0035] Es kann in diesem Zusammenhang weiterhin vorgesehen sein, dass an dem zentralen Server softwareseitig eine standardisierte Schnittstelle implementiert ist, die verwendet werden kann von den einzelnen Dienstanbietern (z. B. den Besitzern der Dienstterminals) um über diese Schnittstelle, z. B. in einem normierten Datenformat die für die Überprüfung notwendigen Daten vom einem Dienstterminal an den zentralen Server zur Verfügung zu stellen. So kann unabhängig von der Art des durchzuführenden Dienstes beispielsweise Bezahlung per elektronischer Lastschrift oder Bezahlung per Kreditkarte oder das Einlösen von Bonuspunkten etc. oder auch unabhängig vom Dienstanbieter immer auf den zentralen Server zugegriffen werden, um den aktuell den Dienst anfragenden Benutzer zu überprüfen.

[0036] Durch diese Zentralisierung der Überprüfungsinstanz in ein Kommunikationsnetzwerk mit der Möglichkeit, dass unterschiedliche Dienstanbieter, insbesondere hinsichtlich wenigstens eines Dienstes, diesen Server nutzen können, ergibt sich eine grundsätzliche Vereinfachung und Ressourceneinsparung, bei den jeweiligen Dienstanbietern, jedoch eine Häufung von biometrischen Kennungen und Benutzerdaten im zentralen Netzwerkbereich, so dass besonders in dieser erfindungsgemäßen Ausgestaltung das eingangs beschriebene erfindungsgemäße Verfahren zur Überprüfung der biometrischen Kennungen auf das Vorhandensein in der Kennungsdatenbank besondere Relevanz entfaltet, da der durch die Erfindung erzielte Geschwindigkeitsvorteil mit zunehmender Nutzeranzahl gewichtiger wird.

[0037] Neben der zuvor beschriebenen, zumindest logischen Unterteilung der Kennungsdatenbank in verschiedene Speicherbereiche, die jeweils individuell vorkommenden Nummernfolgen zugeordnet sind, kann es in einer Weiterbildung auch zusätzlich vorge-

sehen sein, die Kennungsdatenbank auch physikalisch in verschiedene Speicherbereiche zu unterteilen, die eine entsprechende Zuordnung zu den Nummernfolgen, insbesondere zu jeder möglichen Nummernfolge aufweisen.

[0038] Besonders auch hierdurch kann realisiert werden, dass bei einer Vielzahl von Anfragen zum Vergleich übermittelter biometrischer Kennungen auf das Vorhandensein einer Kennungsdatenbank diese vielen Anfragen physikalisch in Abhängigkeit der gleichzeitig übermittelten Nummernfolgen auf unterschiedliche Hardwarebereiche der Kennungsdatenbank aufgesplittet werden können und so die Parallelbearbeitung der Anfragen erleichtert wird.

[0039] Hierfür kann es beispielsweise auch vorgesehen sein, dass der zentrale Server intern mehrere Rechereinheiten aufweist, die jeweils einer Nummernfolge oder einer Gruppe bzw. einer Menge von mehreren Nummernfolgen zugeordnet sind, um so die erhaltenen Anfragen auf Überprüfung, ob die übermittelte Kennung in der Datenbank vorhanden ist, parallel und unabhängig voneinander vornehmen zu können.

[0040] In einer Weiterbildung der Erfindung kann es vorgesehen sein, dass der zentrale Server aus einer zur Kennungsdatenbank physikalisch getrennten Benutzerdatenbank dem Benutzeridentifikator zugeordnete Benutzerdaten ausliest und mit den Benutzerdaten einen Datensatz erstellt mit zur Durchführung des angefragten Dienstes benötigten Daten. Hierzu hat der Server den Benutzeridentifikator zuvor aus der Kennungsdatenbank erhalten aufgrund der Zuordnung des Benutzeridentifikator zur gespeicherten biometrischen Kennung.

[0041] Diese zusammengestellten Daten können sodann in einer Ausführungsvariante beispielsweise einem Dienstserver (z. B. durch Kommunikation über ein Netzwerk) zur Verfügung gestellt werden, der den angefragten Dienst entweder selbst durchführt oder zumindest die Durchführung veranlasst.

[0042] Ein solcher Dienstserver kann dem Dienstanbieter zugeordnet sein, bevorzugt jedoch auch unabhängig von dem Dienstanbieter im Netzwerk des zentralen Servers angeordnet sein, so dass die Durchführung des angefragten Dienstes, ebenso wie die Überprüfung der Zulassung eines Benutzers, vom Dienstanbieter ausgelagert ist und somit auch die Durchführung des Dienstes keinerlei Ressourcen des Dienstanbieters benötigt.

[0043] Beispielsweise kann es in einer Ausführung vorgesehen sein, solche Daten in einen Datensatz zusammenzustellen, die für die Durchführung eines elektronischen Lastschriftverfahrens benötigt werden, wie beispielsweise die Kontonummer und Bank-

leitzahl der belasteten Bank sowie derjenigen Bank, zu deren Gunsten die Gutschrift erfolgen soll.

[0044] Den Dienstanbieter identifizierende oder von diesem benötigte Daten (z. B. dessen Bankverbindung) können durch einen Parameter gegeben oder durch diesen identifiziert sein, der von Dienstterminal ebenso an den zentralen Server gesendet wird, entweder in demselben Schritt der Datenübermittlung von Nummernfolge und biometrischer Kennung oder auch in einem getrennten Übermittlungsschritt. Ebenso können in gleicher Weise weitere Dienstparameter übermittelt werden, wie ein zu zahlender Betrag oder sonstige Parameter, die zur Durchführung des Dienstes benötigt werden, insbesondere die von Dienstanbieter abhängen oder von diesem vorgegeben werden.

[0045] Es kann beispielsweise vorgesehen sein, die zu erstellenden Daten in den Datensatz ohne weitere, den Kunden identifizierende Daten zu integrieren, so dass aus Datenschutzgründen eine Anonymität des Dienstbenutzers sowohl beim Dienstanbieter, also beispielsweise an der Supermarktkasse gewährt ist, ebenso wie bei dem den Dienst durchführenden oder zumindest veranlassenden Dienstserver.

[0046] Die physikalische Trennung von Kennungsdatenbank und den darin gespeicherten biometrischen Kennungen sowie den Nummernfolgen und den in der Benutzerdatenbank gespeicherten Benutzerdaten, wie Namen, Adressen, Kontoverbindungen etc. gewährleistet somit voll umfänglich bei der Durchführung des erfindungsgemäßen Verfahrens die Datenschutzinteressen des jeweils teilnehmenden Benutzers, da dessen Identität zwar grundsätzlich im System, insbesondere im zentralen Server vorliegt, jedoch weder für die Freischaltung noch für die Durchführung des Dienstes an die jeweiligen Instanzen (Dienstanbieter, dienstdurchführenden bzw. -veranlassenden Dienstserver) übermittelt werden.

[0047] In einer weiteren vorteilhaften Ausführung der Erfindung kann es vorgesehen sein, dass die Anzahl der Stellen/Ziffern einer von einem Benutzer bei einer Registrierung auszuwählenden Nummernfolge in Abhängigkeit von der Anzahl der bereits in der Kennungsdatenbank und/oder Benutzerdatenbank gespeicherten Daten vorgeschrieben wird, insbesondere durch den zentralen Server oder einen separaten Registrierungsserver.

[0048] So kann mit Bezug auf eingangs genanntes Beispiel es ausreichend sein bei einer geringen Anzahl von Benutzern Nummernfolgen mit einer ebenso geringen Anzahl von Stellen einzusetzen, um einen Geschwindigkeitsvorteil zu erzielen.

[0049] Beispielsweise kann zunächst mit Eröffnung einer Kennungsdatenbank und/oder Benutzerdaten-

bank eine geringe Anzahl von Stellen vorgeschrieben werden, wie beispielsweise zwei oder drei Stellen bei der Nummernfolge, wohingegen das System bei der Registrierung späterer Benutzer, beispielsweise wenn eine bestimmte Benutzeranzahl überschritten ist, die geforderte Anzahl von Stellen erhöht, z. B. von drei auf vier Stellen oder von vier auf fünf Stellen, um den eingangs beschriebenen Geschwindigkeitsvorteil bei der Überprüfung der biometrischen Kennungen zu realisieren und somit für jeden, zumindest logischen, gegebenenfalls auch physikalischen Speicherbereich der Kennungsdatenbank die Anzahl der darin hinterlegten biometrischen Kennungen zu beschränken, insbesondere auf ein vorbeschriebenes Maß.

[0050] So kann beispielsweise das Verfahren auch vorsehen, insbesondere in zeitlichen Abschnitten zu überprüfen, mit welcher Anzahl von biometrischen Kennungen jeder zumindest logische Speicherbereich der Kennungsdatenbank belastet ist, um sodann bei einem Überschreiten einer Grenzanahl die Anzahl von Stellen der auszuwählenden Nummernfolgen im Registrierungsprozess weiterer Benutzer zu ändern, insbesondere zu erhöhen.

[0051] Um zu vermeiden, dass bei einer nachträglichen Erhöhung der bei einer Registrierung zu verwendenden Stellenanzahl der Nummernfolgen die bereits registrierten Benutzer aufgefordert werden müssen, eine neue Nummernfolge mit höherer Stellenanzahl zu wählen, kann es im Rahmen einer möglichen Weiterbildung der Erfindung vorgesehen sein, bei einer solchen Erhöhung der Stellenanzahl der Nummernfolgen die bereits vergebenen und in der Kennungsdatenbank gespeicherten Nummernfolgen um vorbestimmte Nummern, insbesondere Nullen, an führenden oder nachfolgenden Stellen zu ergänzen.

[0052] Hat beispielsweise ein früher Benutzer bei seiner Registrierung eine lediglich dreistellige Nummernfolge auswählen müssen, wie beispielsweise die Nummer 357, so kann dieser Nutzer auch für das weitere spätere Verfahren diese Nummernfolge weiterhin verwenden, wobei jedoch intern, z. B. im zentralen Server diese Nummernfolge auf die nun vorgeschriebene erhöhte Stellenanzahl automatisch ergänzt wird um eine vorgeschriebene Nummer/Ziffer, z. B. eine Null, in dem Sinne, dass statt der eingegebenen Nummernfolge 357 intern die Nummernfolge 0357 verarbeitet wird, wodurch automatisch auch sicher gestellt wird, dass zumindest logisch, gegebenenfalls auch physikalisch die biometrischen Kennungen, die zu Nummernfolgen mit geringerer Stellenanzahl gespeichert wurden, automatisch in die logische, gegebenenfalls auch physikalischen Speicherbereiche integriert werden, von denjenigen Nummernfolgen mit nachträglich festgelegter höherer Stellenanzahl. Bezogen auf das beschrie-

bene Beispiel kann so erzielt werden, dass die biometrischen Kennungen zu der ursprünglichen Nummernfolge 357 nun automatisch integriert werden in den logischen, gegebenenfalls auch physikalischen Speicherbereich all derjenigen biometrischen Kennungen, die zu der Nummernfolge 0357 gespeichert sind.

[0053] In einer weiterhin bevorzugten Ausführungsform kann es vorgesehen sein, dass in einem Dienstterminal eines Dienstansbieters, beispielsweise eines Supermarktes, einer von mehreren auswählbaren Diensten auswählbar ist und ausgewählt wird und das Dienstterminal zusammen mit der biometrischen Kennung und der Nummernfolge zusätzlich eine dem ausgewählten Dienst zugeordnete Dienstkennung, ggfs. auch weitere Dienstparameter an den zentralen Server übermittelt, wobei der zentrale Server nach Erhalt des Benutzeridentifikators aus der Kennungsdatenbank im Anschluß aus der Benutzerdatenbank solche Benutzerdaten ausliest, die gleichzeitig dem Benutzeridentifikator und der Dienstkennung zugeordnet sind.

[0054] In einem konkreten Beispiel kann dies bedeuten, dass an einer Supermarktkasse dem Kunden sowohl die Bezahlung durch Lastschriftzug von seinem Girokonto angeboten wird als auch beispielsweise die Bezahlung mit Kreditkarte, wobei der Kunde in keinem der beiden verschiedenen Fällen seine entsprechenden Karten an der Supermarktkasse vorlegen muss, sondern lediglich die Dienstart auswählt und sodann die Freischaltung mit seiner biometrischen Kennung, also beispielsweise einem Fingerabdruckscan sowie der Angabe der Nummernfolge durchführt.

[0055] Es wird durch Übermittlung einer Dienstkennung an den zentralen Server sodann sicher gestellt, dass nach Überprüfung des Vorhandenseins der biometrischen Kennung in der Kennungsdatenbank anhand dem aus dieser Datenbank ausgelesenen Benutzeridentifikator zusammen mit der Dienstkennung nun aus der Benutzerdatenbank genau diejenigen Benutzerdaten ausgelesen werden, die für den angefragten bestimmten Dienst benötigt werden, also beispielsweise entweder die Kontonummer und Bankleitzahl der das Girokonto führenden Hausbank bei einer elektronischen Lastschrift oder aber auch alternativ bei dem anderen gewählten Dienst die Kreditkartennummer. Es besteht daher die Möglichkeit, innerhalb der Benutzerdatenbank mehrere Benutzerdaten zu hinterlegen, die jeweils einer Dienstkennung zugeordnet sind und die für den mit der Dienstkennung verbundenen spezifischen Dienst die benötigten Daten darstellen.

[0056] Es besteht daher auch die Möglichkeit, für jeden Benutzer nachträglich, insbesondere nach einer einmaligen Registrierung, bei welcher insbeson-

dere zu zumindest zu einem Dienst von dem Benutzer eine biometrische Kennung, eine Nummernfolge und Benutzerdaten erfasst werden, über einen Server, insbesondere den zentralen Server, mittels eines Webinterfaces, das dem Benutzer zur Verfügung gestellt wird, weitere Benutzerdaten, insbesondere zu bestimmten, bevorzugt vorgegebenen Diensterkennungen zu ergänzen oder zu ändern, insbesondere nachdem ein Benutzer sich selbst für diese Ergänzung oder Änderung mit einem eigenen, dem Benutzer zugeordneten Dienstterminal der erfindungsgemäßen Art unter Nutzung des erfindungsgemäßen Verfahrens freigeschaltet hat.

[0057] Es kann demnach vorgesehen sein, dass ein (z. B. jeder) Benutzer für eine Heimanwendung, insbesondere zur Pflege seiner eigenen Daten, ein eigenes Dienstterminal mit einer Erfassungsvorrichtung für die Nummernfolge und eine biometrische Kennung, somit insbesondere einen Fingerscanner zur Verfügung gestellt bekommt und sich so mittels des erfindungsgemäßen Verfahrens für die Verwaltung seiner eigenen Daten freischaltet.

[0058] Beispielsweise ist ein Benutzer so in die Lage versetzt, nachdem er einmalig an einer dafür autorisierten Stelle mit Benutzerdaten, wie Name und einer biometrischen Kennung registriert wurde, Daten nachzupflegen, nämlich z. B. eine Kontoverbindung für elektronische Lastschriften oder eine Kreditkartennummer für eine Kreditkartenabbuchung oder sonstige Kennungen für andere Dienste, beispielsweise auch für das Einlösen von Punkten von Rabattkarten etc.

[0059] Das erfindungsgemäße Verfahren hat demnach den besonderen Vorteil, dass ein Kunde bei einem Dienstanbieter, z. B. einer Supermarktkette an der Kasse auswählen kann, ob er die Bezahlung der Waren durch Lastschrifteinzug von seinem Girokonto, Belastung seiner Kreditkarte über die Kreditkartennummer oder eventuell auch die Bezahlung der Waren über Rabattpunkte vornimmt, ohne dass der Kunde hierfür die dienstspezifischen Kennungen bzw. Zugangsdaten vorhalten muss, sondern den Dienst am Dienstterminal lediglich auswählt und sodann durch das erfindungsgemäße Verfahren hierfür bei positiver Prüfung seiner biometrischen Kennung und der Nummernfolge freigeschaltet wird, wohingegen im Hintergrund und völlig unabhängig von dem Dienstanbieter vom zentralen Server der zur Durchführung des Dienstes benötigte Datensatz erstellt wird, in welchem die dem ausgewählten Dienst anhand der Dienstkennung zugeordneten Benutzerdaten integriert werden.

[0060] Kurz zusammengefasst kann demnach ein Benutzer, sofern er einmalig registriert ist und gegebenenfalls mehrere Dienste mit den dafür benötigten Daten in der Benutzerdatenbank hinterlegt hat,

im Einzelfall jeweils entscheiden, auf welche Art und Weise er z. B. eine Bezahlung oder eine sonstige Inanspruchnahme eines jeglichen Dienstes wünscht und hierfür immer zwecks Identifizierung seiner Person und Autorisierung seiner Person zur Durchführung des Dienstes seine biometrische Kennung, insbesondere seinen Fingerabdruck verwenden kann.

[0061] Dieses Verfahren ist insoweit auch als besonders vorteilhaft einzustufen, da ein Benutzer, der für das erfindungsgemäße Verfahren und insbesondere für verschiedene Dienstarten registriert ist, seine ansonsten üblicherweise mitzuführenden Karten, wie ec-Girokarte, gegebenenfalls mehrere verschiedene Kreditkarten sowie sonstigen Karten, wie z. B. Bonuskarten, nicht mit sich führen muss, um diese zum Einsatz zu bringen.

[0062] Vielmehr reicht in jedem Fall die Freischaltung des Benutzers anhand seiner biometrischen Kennung, insbesondere seines Fingerabdrucks aus, um den entsprechend gewünschten Dienst nach Auswahl durch den Benutzer am Dienstterminal durchführen zu lassen.

[0063] Beispielsweise um Missbrauch zu reduzieren, kann es vorgesehen sein, dass jedes Dienstterminal, das am erfindungsgemäßen Verfahren teilnehmen soll, am zentralen Server mit einer das Dienstterminal identifizierenden Kennung anzumelden ist.

[0064] So kann sicher gestellt werden, dass nur angemeldete Dienstterminals am erfindungsgemäßen Verfahren teilnehmen können, wodurch auch Sicherheitsstandards eingehalten werden können, beispielsweise dadurch, dass nur bestimmte, sicherheitszertifizierte Dienstterminals für eine Anmeldung am zentralen Server zugelassen werden.

[0065] Beispielsweise kann es vorgesehen sein, dass nur solche Dienstterminals in den freien Verkauf gelangen, die eine solche Zulassung, gegebenenfalls eine bereits vorgenommene Anmeldung am zentralen Server aufweisen, so dass ein Kunde im freien Handel ein solches Dienstterminal erwerben kann, um dieses selbst zur Durchführung von Diensten an das Netzwerk anzuschließen, in welches der vorgenannte zentrale Server eingebunden ist, wodurch dem Kunden nicht nur bei speziellen Dienstanbietern, wie Supermärkten, sondern auch bei sich selbst als Dienstanbieter die Durchführung eines oder mehrerer Dienste, z. B. zum Bezahlen verwenden kann.

[0066] Es besteht so beispielsweise die Möglichkeit, über Webseiten, die Onlineshopping bereitstellen, anhand des Dienstterminals Bezahlvorgänge durchzuführen. Hierfür kann es auch vorgesehen sein, dass ein Dienstterminal, welches in das Netzwerk eingebunden ist, zeitweise für die Durchführung eines Dienstes einem Dienstanbieter zugeordnet wird,

beispielsweise einem Onlineshop im Internet, um so zugunsten dieses Diensteanbieters einen Dienst durchzuführen, obwohl das Dienstterminal räumlich zum Zeitpunkt der Durchführung des Dienstes nicht mit dem Dienstanbieter in Verbindung steht.

[0067] Hierfür kann es beispielsweise im Rahmen des Verfahrens vorgesehen sein, dass der Dienstanbieter z. B. ein Onlineshop an den Benutzer, der zuhause mit einem Dienstterminal an seinem Computer sitzt, eine den Dienstanbieter identifizierende Kennung übersendet und das Dienstterminal zusammen mit der Nummernfolge und der biometrischen Kennung des Benutzers die zuvor erhaltene Dienstanbieterkennung an den zentralen Server kommuniziert, um so sicher zu stellen, dass der Dienst zugunsten des so identifizierten Diensteanbieters durchgeführt wird, beispielsweise also eine Bezahlung zugunsten des vorgenannten Onlineshops stattfindet, obwohl der Benutzer aktuell zuhause an seinem Heimcomputer sitzt.

[0068] Ein Ausführungsbeispiel der Erfindung wird anhand der nachfolgend beschriebenen Figur näher erläutert.

[0069] Die [Fig. 1](#) zeigt einen zentralen Server **1** in einem Kommunikationsnetzwerk, z. B. eines Telekommunikationsunternehmens, auf den über ein Netz **2**, z. B. das Internet zugegriffen werden kann.

[0070] Es ist in dem erfindungsgemäßen Verfahren bzw. System in einem vorgelagerten Schritt vorgesehen, dass in einem Registrierungsort **3** ein Benutzer, der an dem erfindungsgemäßen Verfahren teilnehmen möchte, die Registrierung seiner Person durch Angabe persönlicher Daten, wie Name, Adresse, ggfs. Kontoverbindungen etc. sowie Erfassung einer biometrischen Kennung, z. B. eines Fingerscans, sowie weiterhin der Erfassung einer Nummernfolge registriert wird. Dies erfolgt an einem dienstterminal **3a** des Registrierungsortes **3**.

[0071] Ein solcher Registrierungsort kann beispielsweise bei einem Händler, z. B. einem Supermarkt eingerichtet sein, der selbst an dem erfindungsgemäßen Verfahren zur Durchführung von Bezahlvorgängen seiner Waren teilnimmt. Insbesondere kann es hier vorgesehen sein, einen Registrierungsort mit dafür vorgesehenen Geräten, wie beispielsweise Eingabeinheiten für die Nummernfolgen und Fingerscanner separat anzuordnen zu denjenigen Dienstterminals, mit denen für einen späteren Bezahlvorgang das erfindungsgemäße Verfahren durchgeführt wird.

[0072] Erfindungsgemäß ist es vorgesehen, die erfassten Registrierungs-Daten an den zentralen Server **1** zu übermitteln, der sodann die biometrische Kennung **4** zusammen mit der Nummernfolge in eine Kennungsdatenbank **5** einschreibt und dort spei-

chert, wobei diese Daten von den kundenbezogenen Daten, wie z. B. Name und Kontonummer separiert sind/wurden.

[0073] Diese kundenbezogenen Daten werden in einer räumlich getrennten weiteren Benutzerdatenbank **6** gespeichert. Um eine Zuordnung zwischen biometrischer Kennung und Kundendaten zu erhalten, ist es hier vorgesehen, einen Benutzeridentifikator zu erstellen und sowohl der biometrischen Kennung zuzuordnen, die in die Kennungsdatenbank **5** eingeschrieben wird als auch den Benutzerdaten, die in die Benutzerdatenbank **6** eingeschrieben werden. Im einfachsten Fall kann es sich bei einem solchen Benutzeridentifikator um eine fortlaufende Nummer handeln.

[0074] Bei einer späteren gewünschten Inanspruchnahme eines beliebigen Dienstes, z. B. eines Bezahlvorganges mittels elektronischem Lastschriftzugang, kann es an einem Verkaufspunkt **7** vorgesehen sein, dass ein Kunde, beispielsweise an einer Supermarktkasse zur Bezahlung seiner Waren, seine bei der Registrierung gewählte Nummernfolge angibt, ebenso wie seine biometrische Kennung, z. B. in Form eines gescannten Fingerabdrucks. Dies erfolgt an einem Dienstterminal **7a** des Verkaufspunktes, welches auch durch die Kasse selbst gebildet werden kann.

[0075] Über ein oder mehrere Netzwerke **8, 9, 2** etc. können diese erfassten Daten gegebenenfalls mit weiteren Dienstparametern, wie z. B. einem zu bezahlenden Betrag, den Dienstanbieter identifizierenden Daten etc. über die eingesetzten Netzwerkverbindungen an den zentralen Server **1** kommuniziert werden, der aus den Daten die biometrische Kennung und die Nummernfolge verwendet, um über Vergleich der in der Kennungsdatenbank gespeicherten Daten zu ermitteln, ob die übermittelten Kennungsdaten in der Kennungsdatenbank vorhanden sind und somit bei Vorhandensein der anfragende Benutzer für den Dienst freizuschalten ist.

[0076] Beim Vorhandensein der biometrischen Kennung innerhalb der Kennungsdatenbank kann über den zentralen Server eine Freigabemitteilung zurückkommuniziert werden über die eingesetzten Netzwerkverbindungen zum Dienstanbieter, um diesem zu signalisieren, dass die Waren ausgehändigt werden können und der Dienstanbieter seine Bezahlung erhalten wird. Dabei werden bevorzugt dem Dienstanbieter jedoch keinerlei persönliche Daten zurückgemeldet, sondern lediglich die abstrakte Freigabe für den aktuellen Benutzer.

[0077] Es ist weiterhin vorgesehen, dass von dem zentralen Server anhand des aus der Kennungsdatenbank erhaltenen und der aufgefundenen biometrischen Kennung zugeordneten Benutzeridentifikators

aus der Benutzerdatenbank **6** die für die Durchführung des Dienstes benötigten Daten, wie beispielsweise eine Kontoverbindung, ausgelesen wird.

[0078] Durch den zentralen Server wird sodann ein Datensatz erstellt, beispielsweise eine Einzugsdatei für eine elektronische Lastschrift erstellt oder aber ein schon bestehender Datensatz um die Daten des letzten Kunden ergänzt. Es kann sodann dieser Datensatz in einer möglichen Ausführung an einen vom Dienstanbieter unabhängigen dienstausführenden oder -veranlassenden Server übergeben werden oder unmittelbar an den Dienstanbieter selbst, damit durch eine dieser Stellen das automatische Lastschriftverfahren zugunsten des Dienstanbieters durchgeführt wird.

[0079] Wie sich der [Fig. 1](#) entnehmen lässt, kann über eine Vielzahl unterschiedlicher oder gleicher Netzwerke eine an sich unbegrenzte Anzahl von Dienst Anbietern mit jeweiligen Dienstterminals an dem erfindungsgemäßen Verfahren teilnehmen, ohne eigene Infrastruktur, wie Datenbanken hinsichtlich biometrischer Kennungen und Benutzerdaten vorhalten zu müssen, da dies zentral erfolgt.

[0080] Um hier aufgrund der gegebenenfalls sehr hohen Anzahl von Benutzerdaten und biometrischer Kennungen einen schnellen Zugriff auf die Kennungsdatenbank zu erhalten, ist es wie eingangs im allgemeinen Teil der Erfindung beschrieben, vorgesehen, die Kennungsdatenbank **5** zumindest logisch, gegebenenfalls auch physikalisch in verschiedene Speicherbereiche zu unterteilen, die jeweils einer vorkommenden Nummernfolge zugeordnet sind und in denen jeweils die zu einer Nummernfolge zugeordneten biometrischen Kennungen unterschiedlicher Benutzer gespeichert sind, um so bei einem Vergleich bzw. der Überprüfung auf das Vorhandensein einer übermittelten biometrischen Kennung innerhalb der Kennungsdatenbank **6** zunächst anhand der ebenso übermittelten Nummernfolge einem der zumindest logisch, gegebenenfalls auch physikalisch vorhandenen Speicherbereiche auszuwählen und sodann nur innerhalb dieses Speicherbereichs die übermittelte biometrische Kennung mit den dort gespeicherten biometrischen Kennungen zu vergleichen.

Patentansprüche

1. Verfahren zur Freischaltung eines Dienstes für einen Benutzer bei dem mit einem Dienstterminal (**7a**), insbesondere dem einem Dienstanbieter zugeordneten Dienstterminal (**7a**) eine biometrische Kennung (**4**) des Benutzers, insbesondere ein Finger-Scan, erfasst wird und bei einem Vorhandensein der biometrischen Kennung (**4**) in einer Kennungsdatenbank (**5**) der Benutzer zur Benutzung des Dienstes zugelassen wird, **dadurch gekennzeichnet**, dass

a) die biometrische Kennung (**4**) zusammen mit wenigstens einer Zusatzkennung in einem oder mehreren Kommunikationsschritten an einen, insbesondere zentralen Server (**1**) übermittelt wird, wobei

b) der insbesondere zentrale Server (**1**) in einem, insbesondere dienstunabhängigen Kommunikationsnetzwerk betrieben wird und von dem Dienstterminal (**7a**) zur Übermittlung angewählt wird

c) der insbesondere zentrale Server (**1**) durch Zugriff auf eine biometrische Kennungen (**4**) enthaltende Kennungsdatenbank (**5**) und Vergleich mit den dort gespeicherten Kennungen überprüft, ob die erhaltene biometrische Kennung (**4**) in der Kennungsdatenbank (**5**) vorhanden ist und zu einer vorhandenen biometrischen Kennung (**4**) wenigstens einen der Kennung (**4**) zugeordneten Benutzeridentifikator aus der Kennungsdatenbank (**5**) ausliest

d) wobei die Kennungsdatenbank (**5**) zumindest logisch in Speicherbereiche unterteilt ist, die jeweils einer in der Kennungsdatenbank (**5**) vorkommenden Zusatzkennung zugeordnet sind und in denen vorkommende biometrische Kennungen (**4**) jeweils derselben Zusatzkennung gespeichert sind und die Überprüfung auf das Vorhandensein einer übermittelten biometrischen Kennung (**4**) in der Kennungsdatenbank (**5**) innerhalb desjenigen Speicherbereichs erfolgt, welcher der wenigstens einen übermittelten Zusatzkennung zugeordnet ist,

e) der insbesondere zentrale Server (**1**) an das Dienstterminal (**7a**) bei Vorhandensein der biometrischen Kennung (**4**) in der Kennungsdatenbank (**5**) an das Dienstterminal (**7a**) eine Freigabemitteilung kommuniziert zur Zulassung des Benutzers für den angefragten Dienst, insbesondere ansonsten eine Sperrmitteilung kommuniziert.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die wenigstens eine Zusatzkennung gebildet wird durch

a) Eine Kennung, die dem Dienstterminal (**7a**) oder einem Dienstanbieter zugeordnet ist, insbesondere eine Kennung im Netzwerk, insbesondere eine CLI, HLR, VLR, IMEI und/oder

b) Eine wenigstens zweistellige Nummernfolge, die dem Benutzer zugeordnet ist und vom Benutzer durch Eingabe am Dienstterminal (**7a**) oder einem separaten Nummernterminal erfasst wird und/oder

c) Eine Kennung, insbesondere wenigstens zweistellige Nummernfolge oder Teilnummernfolge einer dem Benutzer zugeordneten Karte, insbesondere Ausweiskarte, Kreditkarte, Bankkarte etc., die von der Karte gelesen wird, insbesondere durch das Dienstterminal (**7a**).

3. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass der Server (**1**) aus einer zur Kennungsdatenbank (**5**) getrennten Benutzerdatenbank (**6**) dem Benutzeridentifikator zugeordnete Benutzerdaten ausliest und mit den Benutzerdaten einen Datensatz erstellt mit zur Durchfüh-

zung des angefragten Dienstes benötigten Daten, insbesondere für einen vom Dienstanbieter getrennt angeordneten/betriebenen dienstdurchführenden oder dienstveranlassenden Dienstserver.

4. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die Anzahl der Stellen einer von einem Benutzer bei einer Registrierung auszuwählenden Nummernfolge oder der von einer Karte stammenden Nummernfolge in Abhängigkeit von der Anzahl der bereits in der Kennungsdatenbank (5) und/oder Benutzerdatenbank (6) gespeicherten Daten vorgeschrieben wird, insbesondere mit zunehmender Anzahl von Daten erhöht wird.

5. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei Erhöhung der Stellenanzahl der Nummernfolgen die bereits vergebenen und in der Kennungsdatenbank (5) gespeicherten Nummernfolgen um vorbestimmte Nummern, insbesondere Nullen, an führender oder nachfolgenden Stellen ergänzt werden.

6. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass an einem Dienstterminal (7a) einer von mehreren auswählbaren Diensten ausgewählt wird und das Dienstterminal (7a) zusammen mit der biometrischen Kennung (4) und der Zusatzkennung zusätzlich eine dem ausgewählten Dienst zugeordnete Dienstkennung an den insbesondere zentralen Server (1) übermittelt, wobei der Server (1) aus der Benutzerdatenbank (6) dem Benutzeridentifikator und der Dienstkennung zugeordnete Benutzerdaten ausliest.

7. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass nach einer einmaligen Registrierung eines Benutzers, bei welcher zu zumindest einem Dienst von dem Benutzer eine biometrische Kennung (4), eine Zusatzkennung, insbesondere Nummernfolge, und Benutzerdaten erfasst werden, über einen Server (1), insbesondere den zentralen Server ein Webinterface zur Verfügung gestellt wird, mittels dem ein Benutzer selbst, insbesondere nach Freischaltung an einem dem Benutzer zugeordneten Dienstterminal, seine Benutzerdaten ergänzt und/oder geändert insbesondere hinsichtlich weiterer Dienstkennungen und diesen zugeordneten Benutzerdaten.

8. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass jedes Dienstterminal (7a) am insbesondere zentralen Server (1) mit einer das Dienstterminal (7a) identifizierenden Kennung angemeldet wird.

9. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass das Dienstterminal (7a) alle an den insbesondere zentralen Server (1) zu übermittelnde Daten, in einen gemeinsamen

Datencontainer integriert und diesen an den zentralen Server (1) übermittelt, der die Integrierten Daten aus dem Datencontainer extrahiert.

10. System zur Freischaltung eines Dienstes für einen Benutzer umfassend wenigstens ein Dienstterminal (7a), insbesondere einem Dienstanbieter zugeordnetes Dienstterminal (7a), mit dem eine biometrische Kennung (4) des Benutzers, insbesondere ein Fingerscan, erfassbar ist und eine Kennungsdatenbank (5), wobei das System eingerichtet ist bei einem Vorhandensein der biometrischen Kennung (4) in der Kennungsdatenbank (5) den Benutzer zur Benutzung des Dienstes zuzulassen, dadurch gekennzeichnet, dass es eingerichtet ist,

a) die biometrische Kennung (4) zusammen mit wenigstens einer Zusatzkennung in einem oder mehreren Kommunikationsschritten an einen, insbesondere zentralen Server (1) zu übermitteln und

b) den insbesondere zentralen Server (1) in einem, insbesondere dienstunabhängigen Kommunikationsnetzwerk von dem Dienstterminal (7a) zur Übermittlung anzuwählen und

c) der insbesondere zentrale Server (1) eingerichtet ist, durch Zugriff auf eine biometrische Kennungen (4) enthaltende Kennungsdatenbank (5) und Vergleich mit den dort gespeicherten Kennungen zu überprüfen, ob die erhaltene biometrische Kennung (4) in der Kennungsdatenbank (5) vorhanden ist und zu einer vorhandenen biometrischen Kennung (4) wenigstens einen der Kennung zugeordneten Benutzeridentifikator aus der Kennungsdatenbank (5) auszulesen

d) wobei die Kennungsdatenbank (5) zumindest logisch in Speicherbereiche unterteilt ist, die jeweils einer in der Kennungsdatenbank (5) vorkommenden Zusatzkennung zugeordnet sind und in denen vorkommende biometrische Kennungen jeweils derselben Zusatzkennung gespeichert sind und die Überprüfung auf das Vorhandensein einer übermittelten biometrischen Kennung (4) in der Kennungsdatenbank (5) innerhalb desjenigen Speicherbereichs erfolgt, welcher der wenigstens einen übermittelten Zusatzkennung zugeordnet ist.

e) der insbesondere zentrale Server (1) weiterhin eingerichtet ist, an das Dienstterminal (7a) bei Vorhandensein der biometrischen Kennung (4) in der Kennungsdatenbank (5) an das Dienstterminal (7a) eine Freigabemitteilung zu kommunizieren zur Zulassung des Benutzers für den angefragten Dienst, insbesondere ansonsten eine Sperrmitteilung zu kommunizieren.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

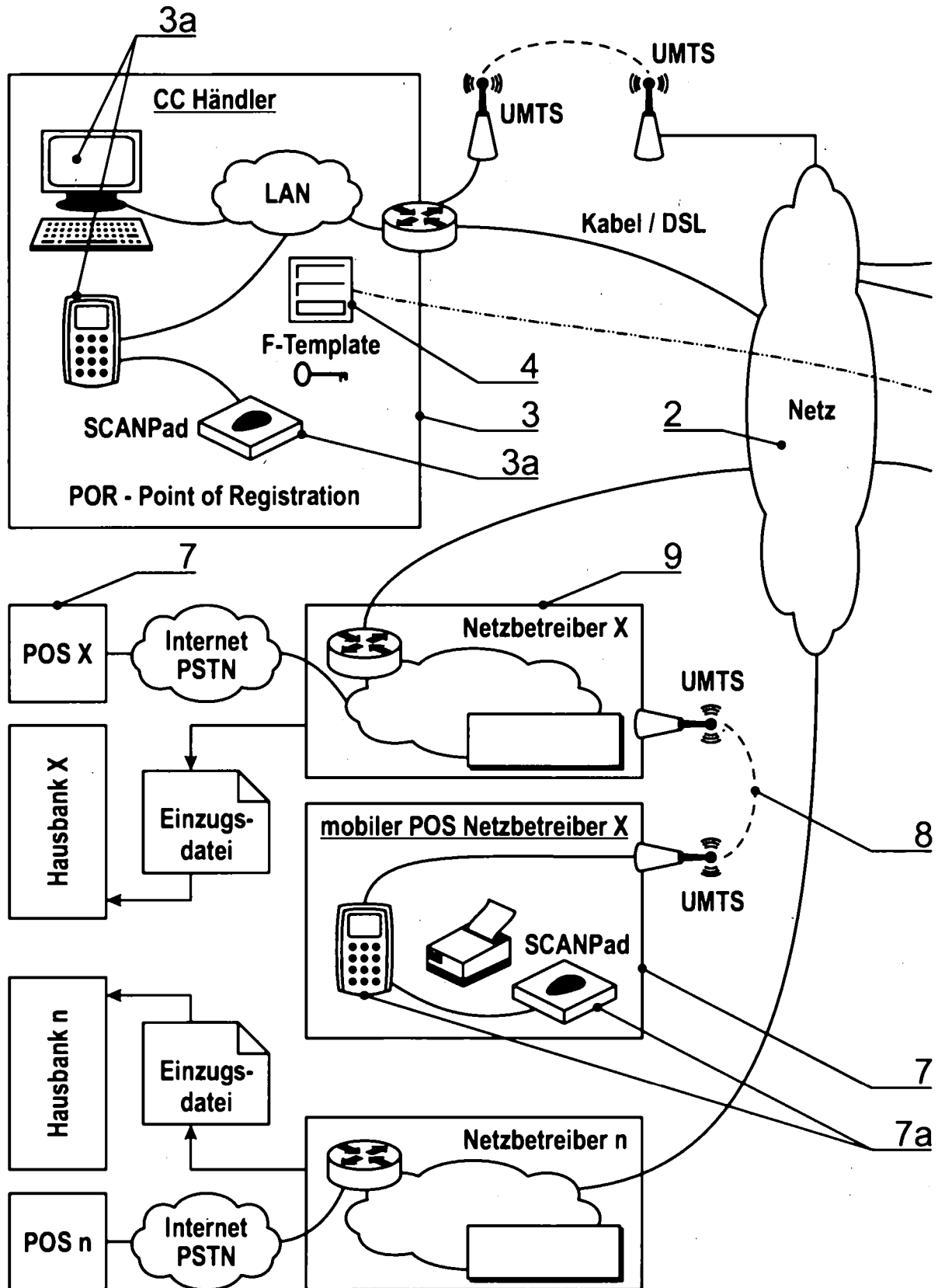


Fig. 1 - Teil 1/2

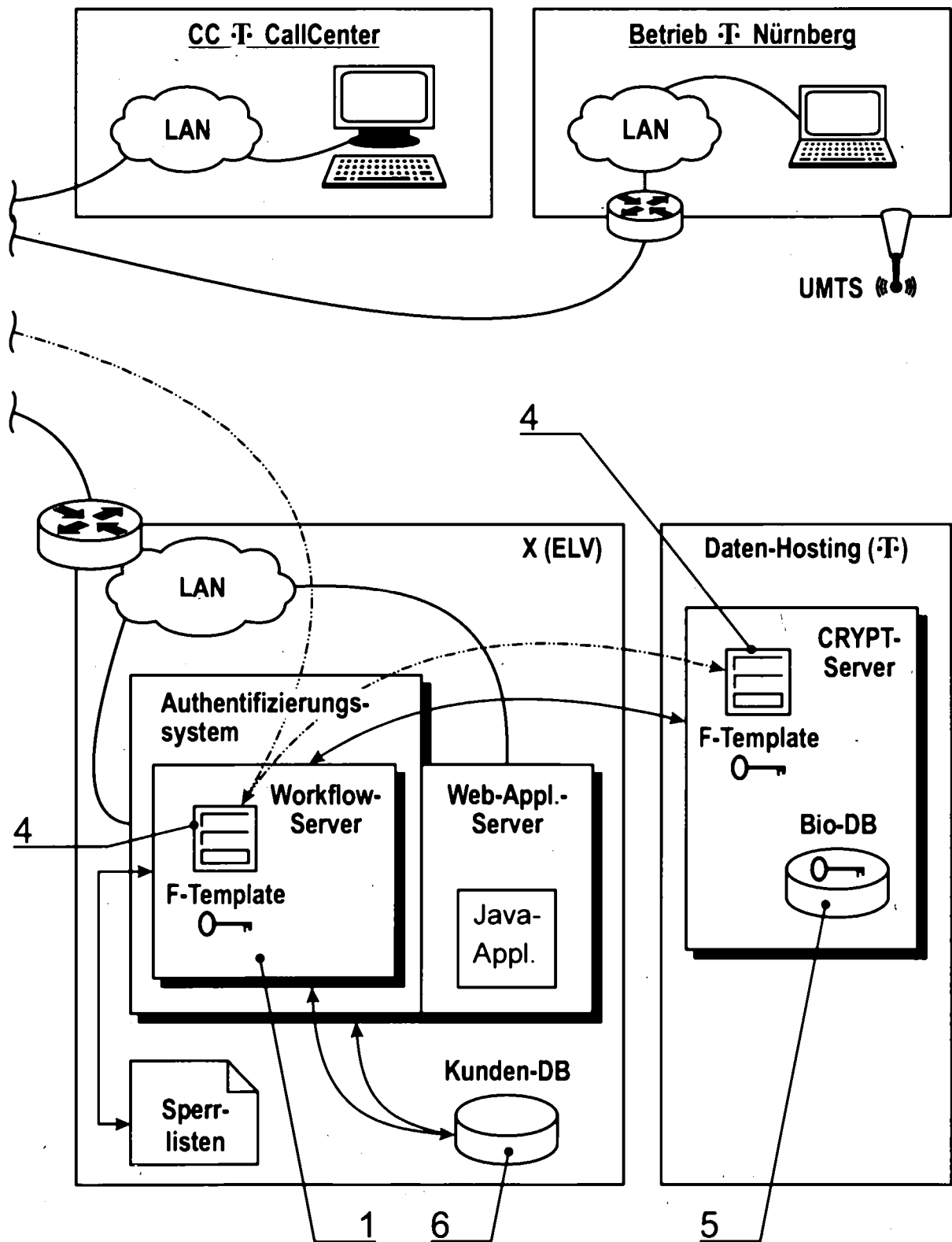


Fig. 1 - Teil 2/2