

SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH** **716 218 B1**

Erfindungspatent für die Schweiz und Liechtenstein

Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(51) Int. Cl.: **H04W** **12/06** (2021.01)
G06F **21/32** (2013.01)
G07C **9/37** (2020.01)
G06Q **20/40** (2012.01)

(12) **PATENTSCHRIFT**

(21) Anmeldenummer: 000679/2019

(22) Anmeldedatum: 24.05.2019

(43) Anmeldung veröffentlicht: 30.11.2020

(24) Patent erteilt: 15.02.2024

(45) Patentschrift veröffentlicht: 15.02.2024

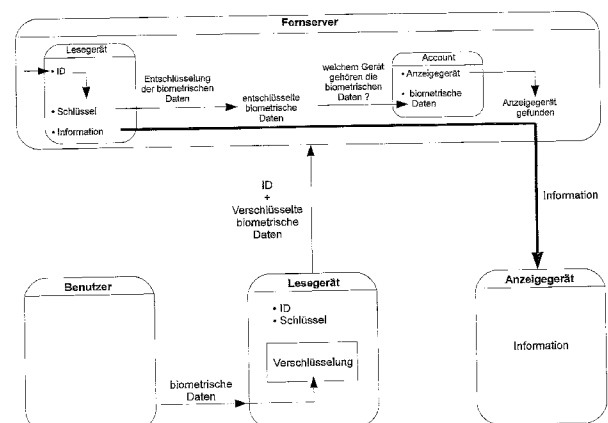
(73) Inhaber:
Digitum AG, Gerbergässlein 1
4450 Sissach (CH)

(72) Erfinder:
Dani Kalt, 4450 Sissach (CH)

(74) Vertreter:
euromaier AG, Berglihöh 3
8725 Ernetschwil (CH)

(54) **System und Verfahren zur Autorisierung von Transaktionen.**

(57) Die Erfindung betrifft ein System und ein Verfahren zur Autorisierung von Transaktionen, womit Informationen dem Benutzer aufgrund seiner biometrischen Daten über sein eigenes Gerät, d.h. ein Gerät, das im Besitz des Benutzers ist und dem Benutzer nicht vom System zur Verfügung gestellt wurde, kommuniziert werden können. Das erfindungsgemässe System besteht aus mindestens einem Lesegerät für biometrische Daten, einem Fernserver und mindestens einem Anzeigegerät.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein System zur Autorisierung von Transaktionen gemäss Oberbegriff des Patentanspruchs 1.

[0002] Biometrische Daten werden schon längst zur Identifikation und Authentifizierung eines Benutzers gebraucht. Dadurch kann ein berechtigter Benutzer Zugang zu Waren, Dienstleistungen oder Räumlichkeiten erlangen. Ein bekanntes Beispiel ist die Öffnung einer Tür oder die Entsperrung von elektronischen Geräten wie Smartphones und Laptops aufgrund der Erkennung eines Fingerabdrucks. Dafür werden vorgängig die biometrischen Daten des Benutzers ermittelt, lokal auf dem Datenspeicher des Geräts hinterlegt und mit bestimmten Zugangsberechtigungen versehen. Bei jeder Zugangsaufforderung werden die vom Antragsteller erfassten biometrischen Daten mit den bereits gespeicherten Daten verglichen, um den Zugang entsprechend zu gestatten oder zu verweigern.

[0003] Neulich werden Systeme bekannt gemacht, wobei die biometrischen Daten des Benutzers nach Ermittlung durch den biometrischen Sensor nicht lokal auf dem Datenspeicher des Geräts selbst, sondern auf einem Fernserver hinterlegt werden (siehe z.B. EP 0762261, WO 9857247, US 2013/0333015 und US 2015/0363398). Für die Identifikation eines Benutzers werden dann seine biometrischen Daten von einem Gerät mit biometrischem Sensor erfasst und dem Fernserver zum Vergleich mit den bereits gespeicherten Daten weitergeleitet. Nach dem Vergleich meldet dann der Server dem Gerät, ob der Benutzer identifiziert werden konnte und ob er die benötigte Zugangsberechtigung besitzt. Dies hat den Vorteil, dass auch ein Gerät, das von einem Benutzer zuvor noch nie benutzt wurde, diesen mithilfe des Fernservers trotzdem erkennen kann. In der Patentschrift EP 1783650 ist beispielsweise vorgesehen, dass ein Benutzer seine biometrische Daten in einem ersten Schritt auf einem Fernserver hinterlegt und mit seinem persönlichen Account verknüpft. Dann kann er z.B. ein Hotelzimmer auf dem Internet buchen und die Reservation mit seinen Fingerabdrücken verknüpfen. Schliesslich kann der Benutzer vor der Hotel- oder Zimmertür auftreten, seine Fingerabdrücke von einem Fingerabdrucksensor ablesen lassen, wobei der ermittelte Fingerabdruck dem Fernserver zur Identifikation übermittelt wird, und bei erfolgreicher Identifizierung Zugang zum Hotel oder zum Zimmer erhalten.

[0004] Diese Systeme sind lediglich auf die Identifikation eines Benutzers und die Ausführung eines vordefinierten Standardablaufs nach erfolgreicher bzw. erfolgloser Identifikation ausgerichtet. Die Interaktion zwischen dem Benutzer und dem Gerät, das Zugang zu einer Ware, Dienstleistung oder Räumlichkeit gestattet, ist also äusserst beschränkt und umfassende Systembenutzer-Schnittstelle mit z.B. Displays, Tastenfelder oder Touchscreens absolut überflüssig.

[0005] Umgekehrt gibt es zahlreiche Automaten, die spezifisch für die Interaktion mit Benutzern bestimmt und ausgerichtet sind, wie z.B. Billetautomaten an Bahnhöfen und Parkplätzen oder Wahlgeräte. Auf diesen Geräten kann der Benutzer komplexe Eingaben machen und das System kann entsprechende Daten anzeigen. Diese Geräte weisen jedoch mehrere Nachteile auf. Erstens können sie nur von einer Person gleichzeitig benutzt werden und Benutzer müssen daher oft Schlange stehen. Zweitens ist der Erwerb und der Unterhalt solcher Automaten teuer, insbesondere weil Teile der Systembenutzer-Schnittstelle sowie Touchscreens besonders empfindlich sind und wegen Schmutz oder rücksichtslosen Benutzern leicht beschädigt werden und ausfallen. Drittens ist die Authentifizierung eines Benutzers auf solchen Geräten entweder nicht möglich, zu aufwendig oder nicht sicher, beispielsweise wenn eine Anmelder-ID und -Passwort in einer Bahnhofshalle auf einem gut sichtbaren Touchscreen eingegeben werden muss. Dann besteht auch noch die Gefahr, dass der Benutzer sich nicht richtig ausloggt, und ein Dritter Zugang zum Account erlangt.

[0006] Die vorliegende Erfindung stellt sich nunmehr die Aufgabe, ein System bereitzustellen, womit Informationen dem Benutzer aufgrund seiner biometrischen Daten über sein eigenes Gerät, d.h. ein Gerät, das im Besitz des Benutzers ist und dem Benutzer nicht vom System zur Verfügung gestellt wurde, kommuniziert werden können.

[0007] Diese Aufgabe löst ein System und ein Verfahren zur Autorisierung von Transaktionen mit den Merkmalen der Patentansprüche 1 und 2. Weitere Merkmale und Ausführungsbeispiele gehen aus den abhängigen Ansprüchen hervor und deren Vorteile sind in der nachfolgenden Beschreibung erläutert.

[0008] In der Zeichnung zeigt:

Figur 1 Schematische Darstellung des ersten vorgängigen Schritts des Verfahrens: Registrierung eines Lesegeräts.

Figur 2a Schematische Darstellung des zweiten vorgängigen Schritts des Verfahrens: Erstellung eines Accounts und Verknüpfung eines Anzeigeräts

Figur 2b Schematische Darstellung des zweiten vorgängigen Schritts des Verfahrens: Verknüpfung von biometrischen Daten mit dem Account

Figur 3 Schematische Darstellung eines möglichen Ablaufs: Ermittlung von biometrischen Daten eines Benutzers über den Lesegerät, Suche des entsprechenden Account und verknüpften Anzeigeräts und Übermittlung einer Information ans Anzeigerät

Figur 4 Schematische Darstellung eines möglichen Ablaufs: Ermittlung von biometrischen Daten eines Benutzers über den Lesegerät, Suche des entsprechenden Account und verknüpften Anzeigegerät und Kommunikation zwischen dem Anzeigegerät und einem weiteren System über den Fernserver

[0009] Die Figuren stellen mögliche Ausführungsbeispiele dar, welche in der nachfolgenden Beschreibung erläutert werden.

[0010] Das erfindungsgemässe System zur Autorisierung von Transaktionen besteht aus mindestens einem Lesegerät für biometrische Daten, einem Fernserver und mindestens einem Anzeigegerät. Das vorliegende System kann ein oder mehrere Lesegeräte aufweisen, die für die Ermittlung von biometrischen Daten geeignet sind. Beispielsweise können biometrischen Daten Fingerabdrücke, eine Stimme, Gesten, eine Iris, Gesichtszüge, Blutgefässmuster, usw. sein. Lesegeräte können entweder aus einzelnen Komponenten bestehen wie z.B. Fingerabdruckleser, Mikrofone (zur Stimmerkennung) oder Kameras (zur Erkennung von Gesichtszügen, Gesten, usw.) oder Bestandteile eines grösseren Geräts sein, beispielsweise eines Smartphones. Unter „Anzeigegerät“ ist ein Gerät zu verstehen, dass einem Benutzer Informationen übermitteln kann, beispielsweise über einem Bildschirm.

[0011] In einem ersten vorgängigen Schritt muss das mindestens eine Lesegerät beim Fernserver registriert werden (Figur 1). Dabei erhält das Lesegerät eine Identifikation, beispielsweise eine ID-Nummer, und einen eindeutigen Schlüssel zur Verschlüsselung der erfassten biometrischen Daten. Weiterhin wird das Lesegerät beim Fernserver mit Informationen verknüpft, z.B. Text, Bilder, Videos, einer Tonspur, einem Link zu einer Webseite, usw.. Diese Informationen können auch ein Programm sein, das vorbestimmte Aktionen durchführt, wenn es angestossen wird. Ausserdem ist vorgesehen, dass diese Informationen zu jedem Zeitpunkt und beliebig oft aktualisiert werden können.

[0012] In einem zweiten vorgängigen Schritt kann der Benutzer sich beim Fernserver anmelden, auf dem Fernserver seine biometrischen Daten oder biometrischen Daten von Dritten (z.B. von seinen Kindern, usw.) hinterlegen und diese mit einem Anzeigegerät verknüpfen (Figur 2a-b). In einer möglichen Ausführungsvariante kann der Benutzer aufgefordert werden, einen persönlichen Account auf dem Fernserver zu erstellen. Die biometrischen Daten werden dann ermittelt, z.B. mit einem Lesegerät, dem Fernserver übermittelt und mit dem Account verknüpft. Aus Sicherheits- und Datenschutzgründen ist es besonders vorteilhaft, wenn die biometrischen Daten nicht direkt als solche (z.B. als Bild) auf dem Fernserver gespeichert werden, sondern nur in abgeleiteter, „anonymisierter“ Form, womit die ursprünglichen biometrischen Daten nicht wiederhergestellt werden können. Beispielsweise könnten die Lesegeräte unmittelbar nach Ermittlung der biometrischen Daten diese irreversibel umrechnen, z.B. in einem Hashwert, der dann dem Fernserver übermittelt wird und für jeden Satz biometrischer Daten eindeutig ist. Das Anzeigegerät kann z.B. ein Mobiltelefon, ein Smartphone, ein Tablet, ein Computer, eine Smartwatch, usw. sein. Die Verbindung zwischen dem Anzeigegerät und dem persönlichen Account kann beispielsweise über ein geeignetes Computerprogramm oder eine App, die auf dem Anzeigegerät installiert ist, erfolgen. Alternativ könnte auf dem persönlichen Account auch eine Telefonnummer hinterlegt werden, wenn das Anzeigegerät eine Telefonnummer besitzt. Somit sind Anzeigegerät und biometrische Daten über den persönlichen Account auf dem Fernserver verbunden.

[0013] Nach diesen zwei vorgängigen Schritten kann der Benutzer an beliebigen Lesegeräten Aktionen auslösen (Figur 3). In einer möglichen Variante erfolgt das Auslösen alleine dadurch, dass der Benutzer seine biometrischen Daten vom Lesegerät aufnehmen lässt. Danach leitet das Lesegerät die ermittelten biometrischen Daten am Fernserver weiter. Besonders vorteilhaft ist, wenn das Lesegerät vor der Übermittlung zum Fernserver die biometrischen Daten mit seinem eindeutigen Schlüssel verschlüsselt, und dem Fernserver auch seine Identifikation zuschickt. Aufgrund der Identifikation des Lesegeräts kann der Fernserver den entsprechenden Schlüssel zur Entschlüsselung der ermittelten biometrischen Daten finden und diese entschlüsseln. Danach werden die ermittelten biometrischen Daten mit den biometrischen Daten der registrierten Accounts verglichen, bis der richtige Account und das verknüpfte Anzeigegerät gefunden werden. Die beim Lesegerät angegebenen Informationen werden dann dem Anzeigegerät geschickt und dem Benutzer angezeigt. Erfindungsgemäss ist vorgesehen, dass die Lesegeräte, mit denen die Transaktion ausgelöst wird, nicht Bestandteile des Anzeigegeräts sind.

[0014] In einer Ausführungsvariante kann das Anzeigegerät vom Benutzer auch Inputs bekommen, beispielsweise durch ein Touchscreen, ein Tastenfeld, Knöpfe, eine Maus, ein Mikrofon, eine Kamera usw., die dem Fernserver übermittelt werden. In einer Variante der Erfindung werden diese Eingaben durch den Fernserver verarbeitet und entsprechende Rückmeldungen dem Anzeigegerät zurückgeschickt. Vorteilhaft könnte der Benutzer auf seinem Konto auch persönliche Einstellungen wählen, damit der Fernserver die Eingabe gemäss dieser Einstellungen personalisiert bearbeiten kann. In anderen Varianten ist der Fernserver zusätzlich mit einem weiteren System verbunden, dem die Eingabe des Benutzers und/oder die Identifikation des Lesegeräts weitergeleitet wird. Besonders vorteilhaft ist es, wenn dieses weitere System dem Fernserver und dem Anzeigegerät auch Informationen übermitteln kann. Somit können das Anzeigegerät und das weitere System über dem Fernserver kommunizieren (Figur 4). Die Tatsache, dass der Fernserver als Vermittler zwischen dem Anzeigegerät und dem weiteren System dient, weist etliche Vorteile auf. Zum Beispiel stehen in dieser Konfiguration sowohl das Anzeigegerät sowie das weitere System immer nur mit dem Fernserver in Verbindung, was einfacher ist als jeweils eine neue Verbindung Anzeigegerät/weiteres System herzustellen. Ausserdem kann dadurch auch die Anonymität des Anzeigegeräts bzw. des Benutzers bewahrt werden, da das weitere Gerät die Kontaktdetails des Anzeigegeräts nicht

erhält. Somit kann z.B. vermieden werden, dass der Benutzer nach einer Interaktion mit einem weiteren System später noch unerwünschte Meldungen davon bekommt, wie Werbungen usw.. Wenn aber eher eine direkte Verbindung zwischen dem Anzeigegerät und das weitere System von Vorteil ist, können das Anzeigegerät und das weitere System auch ihre respektive Kontaktdetails über den Fernserver austauschen und danach eine eigene, unabhängige Verbindung miteinander herstellen. In dieser Variante dient der Fernserver also lediglich als initialer Auslöser der Transaktion.

[0015] In einer möglichen Variante hinterlegt der Benutzer Zahlungsinformationen auf dem Fernserver. Hier sind nicht nur die Details einer Kreditkarte zu verstehen, sondern auch direkte Anbindungen an Bankkonten oder Kontos bei anderen Finanzinstituten (PayPal, Paymit, usw.). Alternativ ist auch vorgesehen, dass Benutzer Kontokorrente auf dem Fernserver besitzen können. Die Transaktion, die der Benutzer an einem Lesegerät auslöst, kann also eine Zahlungstransaktion sein, die mit den erfassten Zahlungsinformationen ausgeführt wird. Eventuell kann vor der Ausführung der Zahlungstransaktion der Benutzer auch noch um Bestätigung über seinem Anzeigegerät gebeten werden.

[0016] In vorteilhaften Ausführungsvarianten der Erfindung ist auch vorgesehen, dass das vorliegende System nicht nur zur Autorisierung einer Transaktion durch Vorweisen der biometrischen Daten des Antragstellers geeignet ist, sondern auch zur Identifizierung des Benutzers. In einer möglichen Variante könnte der Fernserver also die Identität des Benutzers dem weiteren System übermitteln, damit das weitere System dem Anzeigegerät personalisierte Informationen oder Dienstleistungen anbieten kann.

[0017] Im Folgenden werden einige Beispiele zur Anwendung des erfindungsgemässen Systems gegeben.

[0018] Beispiel 1: In Museen sind neben den Kunstwerken oft Schautafeln angeordnet, die die wichtigsten Informationen im Zusammenhang mit dem Kunstwerk zusammenfassen. Diese können aus Platzmangel jedoch nur eine kurze Beschreibung aufweisen, und in einer Beschränkten Anzahl Sprachen. Neuerdings werden in manchen Museen neben wichtigen Kunstwerken Touchscreens eingebaut, die dem Besucher mehr Informationen zur Verfügung stellen können. Da die Anzahl solcher Geräte jedoch beschränkt ist, und da sie nur eine Person aufs Mal benutzen kann, sind diese zusätzlichen Informationen eigentlich nicht für alle zugänglich. Mit dem vorliegenden System könnte das Museum neben dem Kunstwerk ein Lesegerät für biometrische Daten einbauen, und dieses Gerät auf dem Fernserver mit den zusätzlichen Daten im Zusammenhang mit dem Kunstwerk verknüpfen. Dann könnte jeder registrierte Benutzer vom Lesegerät seine biometrischen Daten ablesen lassen, und sofort sämtliche Informationen auf seinem verknüpften Smartphone oder Tablet usw. erhalten. Vorteilhaft könnte der Benutzer auf seinem Konto auch beispielsweise seine Muttersprache einstellen, damit er sämtliche Informationen gleich in der richtigen Sprache bekommt.

[0019] Beispiel 2: Bei Partys läuft meistens eine Playlist, die der Gastgeber für seine Gäste zusammengestellt hat. Es kommt aber öfters vor, dass Gäste auch an der Erstellung der Playlist teilnehmen möchten, z.B mit Songs, die sie aber nur auf ihrem eigenen Smartphone haben. Erfindungsgemäss könnte beim Gastgeber ein Lesegerät für biometrische Daten installiert werden, wobei sich registrierte Benutzer anmelden könnten und auf ihrem Smartphone Zugang zur Playlist erhalten, beispielsweise um die Reihenfolge der Songs zu ändern oder neue Musik hinzuzufügen. Auch bei Nachtclubs könnte mit dem erfindungsgemässen System die Playlist allgemein bestimmt werden. Nach dem Auslösen mit ihren biometrischen Daten könnten die Benutzer mit ihren Smartphone Zugang zu einer Plattform erhalten, auf deren sie für Songs, die Ihnen vom DJ vorgeschlagen sind, wählen können. Dann könnte z.B. die nächste Musik immer diejenige sein, die am populärsten ist. Die Notwendigkeit der vorgängigen Anmeldung mit der Ermittlung der biometrischen Daten hat den Vorteil, dass nur die Leute, die tatsächlich anwesend sind, die Musik bestimmen können.

[0020] Beispiel 3: In Vereinen gibt es in regelmässigen Zeitabständen Wahlen, wobei ein neues Präsidium gewählt wird. Dies erfolgt meistens durch eine geheime Abstimmung mit Stimmzetteln oder durch eine offene Abstimmung mit Handhebung. Über eine bestimmte Anzahl Wähler wird die Auszählung der Stimmen jedoch ziemlich aufwendig. Mit dem vorliegenden System könnten die registrierten Wähler ihre Anwesenheit durch das Einscannen ihrer biometrischen Daten am Lesegerät bestätigen, und dann z.B. auf ihren Smartphones den gewünschten Kandidaten geheim wählen. Da jeder ein Smartphone hat und alle Teilnehmer gleichzeitig wählen können, können Wahlen für mehrere Hunderte Personen innerhalb von Minuten einfach, sicher und präzise durchgeführt werden.

[0021] Beispiel 4: Das vorliegende System kann auch als Zahlungssystem benutzt werden. Ein registrierter Benutzer könnte Zahlungsinformationen auf dem Server hinterlegen, und in einem Geschäft bei der Zahlung einfach seine biometrischen Daten ablesen lassen, um die Zahlung zu autorisieren. Eventuell könnte der Benutzer zuerst auch eine Meldung auf seinem Smartphone erhalten und um Bestätigung der Transaktion gebeten werden. In einer anderen Situation könnte z.B. ein Elternteil die biometrischen Daten von einem ihrer Kinder mit seinem Account verknüpfen, damit das Kind mit dem Geld seiner Eltern etwas kaufen kann, beispielsweise einen Wecken in der Bäckerei.

Patentansprüche

1. System zur Autorisierung von Transaktionen bestehend aus mehreren Lesegeräten für biometrische Daten, einem Fernserver, und mindestens einem Anzeigegerät, wobei die Lesegeräte beim Fernserver registriert sind und jedes Lesegerät vom Fernserver eine Identifikation und einen eindeutigen Schlüssel für die Verschlüsselung von biometrischen Daten besitzt,

jedes Lesegerät beim Fernserver mit Informationen verknüpft ist,
wobei der Fernserver derart konfiguriert ist, dass:

- ein Benutzer sich darauf anmelden kann und mit einem der Lesegeräte seine biometrischen Daten oder einen aus biometrischen Daten erzeugten eindeutigen Hashwert auf dem Fernserver hinterlegen kann, und
- der Benutzer das Anzeigegerät auf dem Fernserver mit seinen biometrischen Daten oder mit dem Hashwert verknüpfen kann,

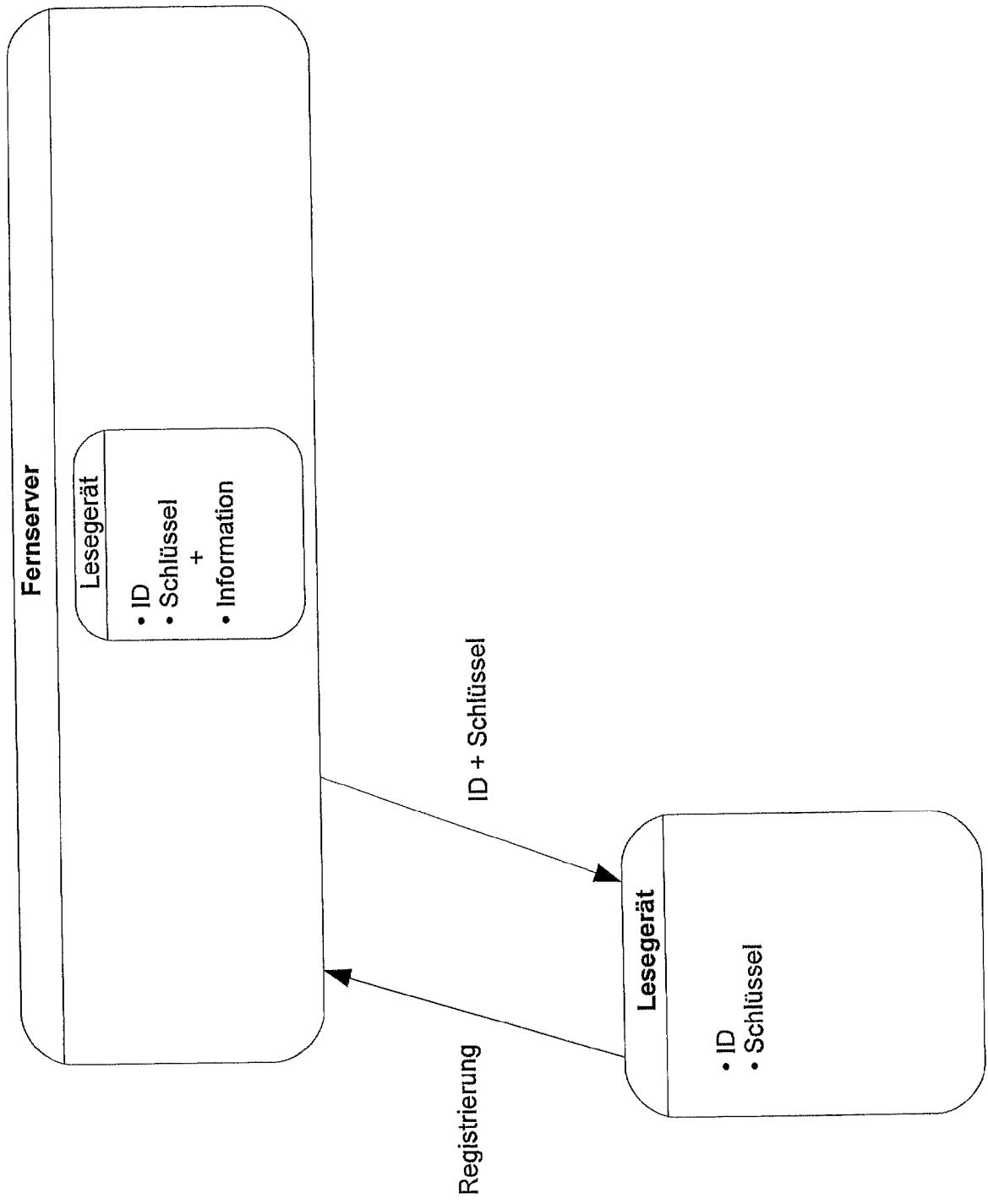
wobei die weiteren Lesegeräte eine Transaktion auslösen können, indem sie die biometrischen Daten des Benutzers aufnehmen und die verschlüsselten biometrischen Daten zusammen mit deren Identifikation an den Fernserver übermitteln,

wobei der Fernserver die folgenden Verfahrensschritte ausführen kann:

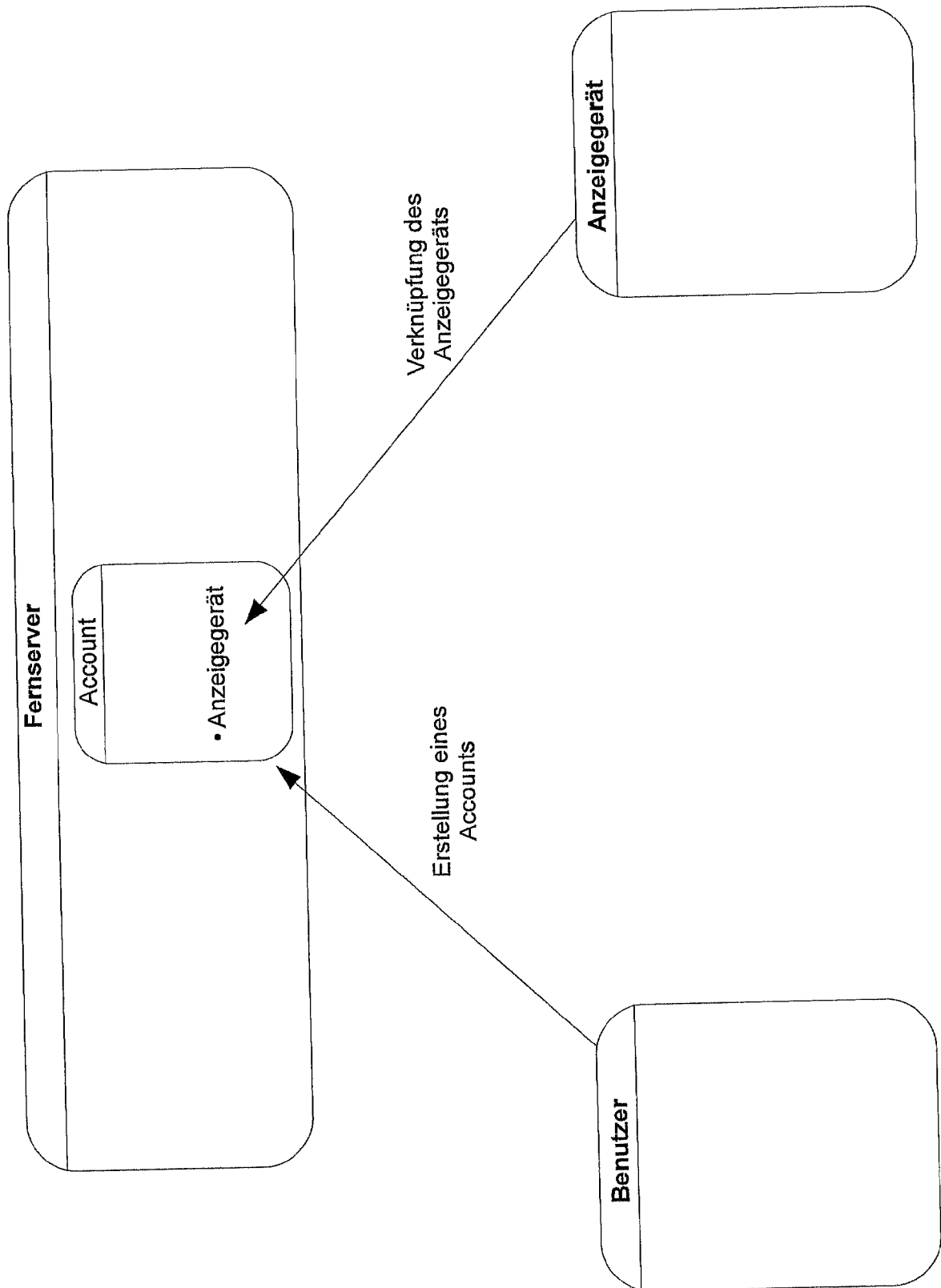
- Bereitstellung der verknüpften Information anhand der Identifikation eines der Lesegeräte;
 - Ermittlung des mit den biometrischen Daten verknüpften Anzeigegeräts;
 - Übermittlung der bereitgestellten Informationen an das verknüpfte Anzeigegerät,
- und wobei das Anzeigegerät die Informationen dem Benutzer anzeigen kann.

2. Verfahren zur Autorisierung von Transaktionen mit dem System gemäss Anspruch 1 und mit den folgenden Verfahrensschritten
 - (a) biometrische Daten eines bei einem Fernserver registrierten Benutzers werden mit einem Lesegerät erfasst
 - (b) die biometrischen Daten werden mit einem bei der Registrierung des Lesegeräts beim Fernserver festgelegten Schlüssel verschlüsselt
 - (c) die verschlüsselten biometrischen Daten werden vom Lesegerät an den Fernserver übermittelt
 - (d) der Fernserver stellt die mit dem Lesegerät verknüpften Informationen bereit
 - (e) der Fernserver übermittelt die bereitgestellten Informationen an ein Anzeigegerät, welches mit den biometrischen Daten des registrierten Benutzers verknüpft ist
 - (f) die Informationen werden auf dem Anzeigegerät zur Autorisierung angezeigt.
3. Verfahren gemäss Anspruch 2, dadurch gekennzeichnet, dass
 - (g) eine vom Benutzer aufgrund der angezeigten Information auf dem Anzeigegeräte gemachte Eingabe an den Fernserver übermittelt wird.
4. Verfahren gemäss Anspruch 3, dadurch gekennzeichnet, dass
 - (h) die Eingabe vom Fernserver an ein externes System übermittelt wird.
5. Verfahren gemäss Anspruch 2, dadurch gekennzeichnet, dass
 - (i) der Fernserver eine Identifikation des Lesegeräts und/oder eine vorgängig zwischen dem Fernserver und einem externen System ausgetauschten Identität des Benutzers dem externen System übermittelt.
6. Verfahren gemäss Anspruch 4 oder 5, dadurch gekennzeichnet, dass
 - (j) das externe System dem Fernserver Informationen übermittelt, welche an das Anzeigegerät weitergeleitet werden.
7. Verfahren gemäss Anspruch 3, dadurch gekennzeichnet, dass
 - (k) der Fernserver aufgrund der vom Anzeigegerät erhaltenen Eingabe eine Zahlungstransaktion durchführt oder abbricht.
8. Verfahren gemäss Anspruch 7, dadurch gekennzeichnet, dass
 - (l) die Zahlungstransaktion erst nach der Authentifizierung des Benutzers anhand der biometrischen Daten durch den Fernserver ausgelöst wird.

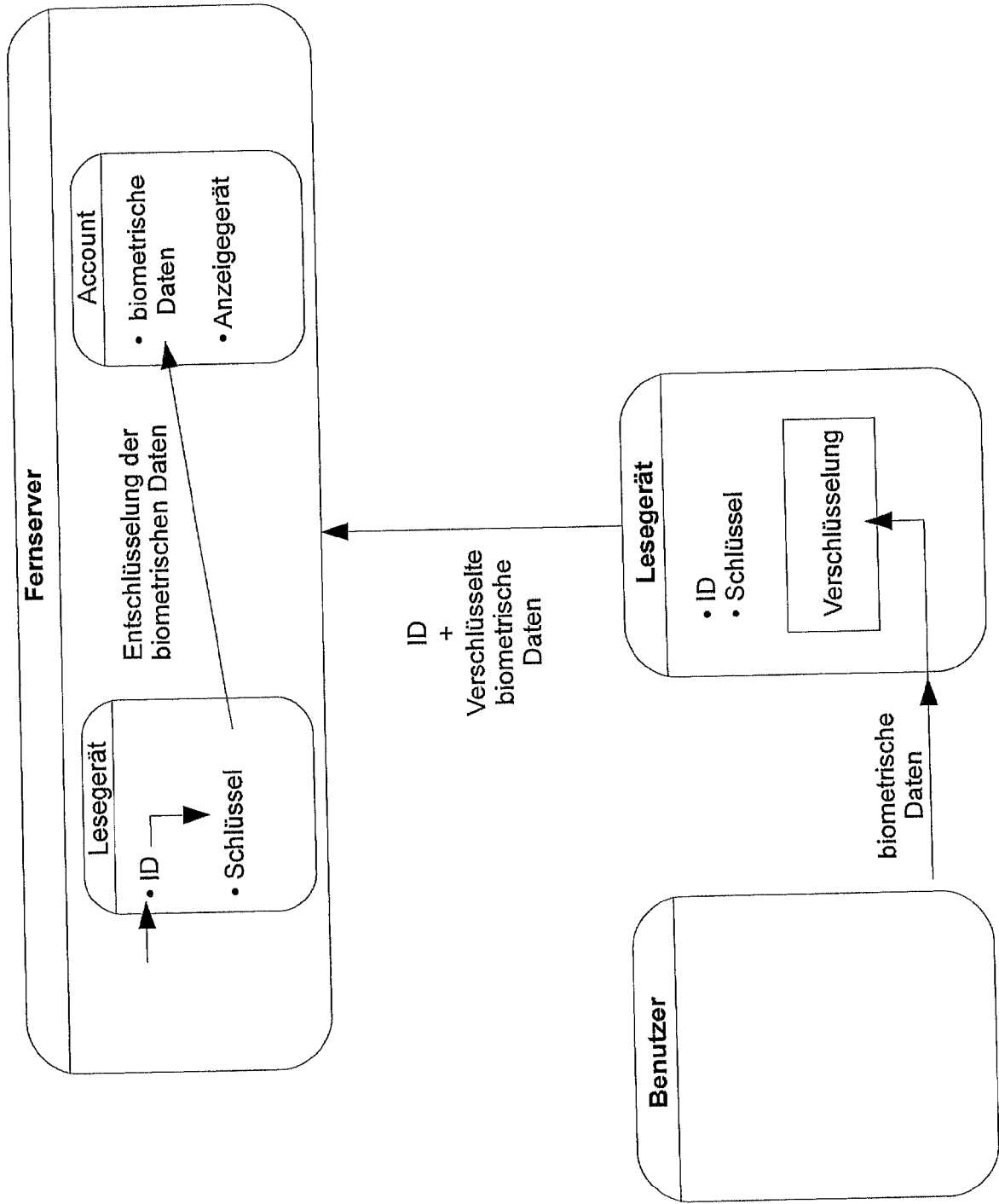
Figur 1



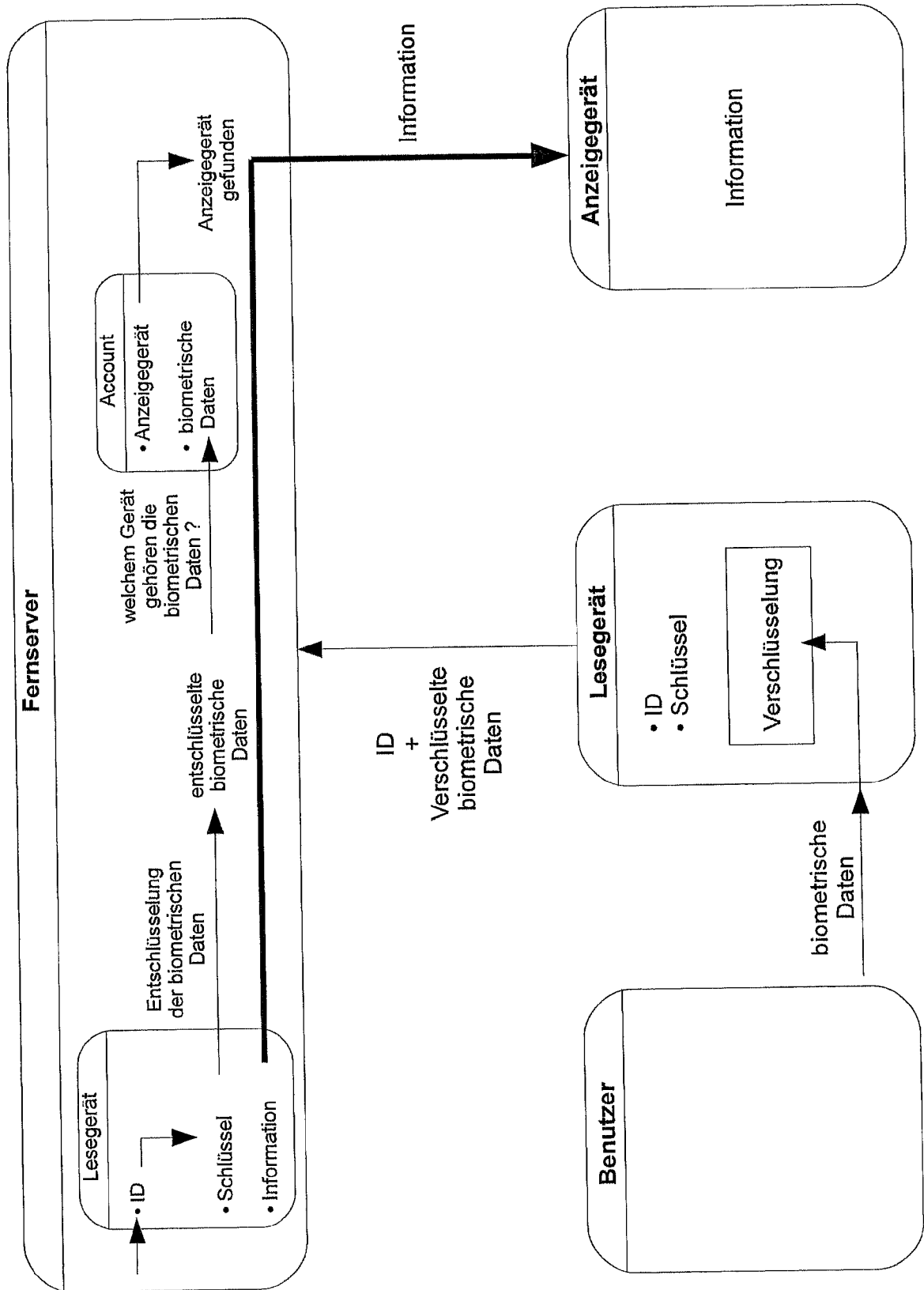
Figur 2a



Figur 2b



Figur 3



Figur 4

