(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
18. Januar 2001 (18.01.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/04771 A2

(51) Internationale Patentklassifikation[7]: G06F 17/00

(21) Internationales Aktenzeichen: PCT/EP00/06577

(22) Internationales Anmeldedatum:
11. Juli 2000 (11.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 32 149.3 12. Juli 1999 (12.07.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, D-81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **ALBRECHT, Norbert** [DE/DE]; Reinhardtstrasse 37, D-10117 Berlin (DE). **HINZ, Walter** [DE/DE]; Zugspitzweg 3, D-85748 Garching (DE). **WEILACHER, Hermann** [DE/DE]; Dalienweg 3, D-85241 Ampermoching (DE).

(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, D-80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, 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), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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.

(54) Title: SYSTEM FOR CARRYING OUT A TRANSACTION

(54) Bezeichnung: SYSTEM ZUR AUSFÜHRUNG EINER TRANSAKTION

(57) Abstract: The invention relates to a system for carrying out transactions using terminals that basically enable the execution of a plurality of different transactions. To this end, the terminals (10, 11) are connected to at least one node computer (40, 41) by a terminal network (30) that can be set up for carrying out a transaction. Appropriateness to execute another transaction that has not been hitherto prepared can be subsequently established at any time without requiring any special setup measures. A terminal (10, 11) requests data from a node computer (40, 41) which responds to a triggering signal characterizing the other transaction, said data providing the functionality needed to carry out the other transaction. Execution of the transaction is then effected by interaction between the terminal (10, 11) and a node computer (40, 41).

(57) Zusammenfassung: Vorgeschlagen wird ein System zur Ausführung von Transaktionen mit Endgeräten, welche grundsätzlich die Ausführung einer Vielzahl verschiedener Transaktionen erlauben. Die Endgeräte (10, 11) sind dazu über ein Endgerätenetz (30) mit mindestens einem Knotenrechner (40, 41) verbunden, über den sie zur Ausführung einer Transaktion einrichtbar sind. Die Eignung zur Ausführung einer weiteren, bis dahin nicht vorbereiteten Transaktion lässt sich dabei jederzeit ohne spezielle Einrichtungsmassnahmen nachträglich herstellen. Ein Endgerät (10, 11) fordert dazu auf ein die weitere Transaktion bezeichnendes Auslösesignal hin von einem Knotenrechner (40, 41) Daten an, welche die zur Ausführung der weiteren Transaktion benötigte Funktionalität herstellen. Die Ausführung der Transaktion erfolgt dann in Wechselwirkung zwischen einem Endgerät (10, 11) und einem Knotenrechner (40, 41).

WO 01/04771 A2

System zur Ausführung einer Transaktion

Die Erfindung geht aus von einem System nach der Gattung des Hauptanspruchs.

Ein solches ist bekannt aus der EP-B-0 305 004. Darin ist ein System zur Ausführung von Finanztransaktionen beschrieben, welches benutzerseitig Terminals vorsieht, von denen jeweils mehrere in Parallelanordnung mit einem sogenannten Konzentrator verbunden sind. Die Konzentratoren ihrerseits sind in Parallelanordnung über ein Banknetz mit einem Hintergrundbanksystem verbunden. Die Verbindungen zwischen den Systemteilen sind unabhängig voneinander gegen Ausforschen des über sie erfolgenden Datenverkehrs gesichert. Zur Sicherung der Verbindungen zwischen Terminals und Konzentratoren dienen Sicherheitsboxen, welche terminalseitig vorzugsweise in Form von Smartcards ausgeführt sind. Maßgebliches Element der Systemstruktur sind die Konzentratoren, welche die Kommunikation mit dem Hintergrundsystem durchführen und über sämtliche dazu benötigte Mittel verfügen. Die mit einem Konzentrator verbundenen Terminals sind nur zur Kommunikation mit dem jeweils vorgeschalteten Konzentrator befähigt. Der Aufbau der Terminals kann dadurch einfach gehalten werden.

Eine Schwierigkeit bei Vielteilnehmer-Systemen wie dem vorgenannten ist die Einrichtung neuer oder die Änderung bestehender Systemmerkmale. Die damit verbundene Problematik wird vor allem offensichtlich, wenn eine vorzunehmende Systemänderung, etwa die Einführung eines neuen Softwaresicherheitsmerkmals, mindestens zwei Systemteilnehmer betrifft und diese technisch nicht identisch sind. Für jeden Teilnehmertyp ist die Systemanpassung dann in der Regel typindividuell vorzunehmen. Ist die Funktionalität eines Endgerätes dabei nicht nachträglich änderbar, ist ein kompletter Austausch des Endgerätes erforderlich.

Aus der DE-A1-38 15 071 ist es desweiteren bekannt, ein Kommunikationssendgerät in Gestalt eines Bildschirmtextterminals oder eines Fernsehempfangsgerätes durch Nachladen von Programmpaketen an eine gegebene Nutzungssituation am Einsatzort anzupassen. Das Gerät verfügt über eine Mikroprozessoreinheit, eine Speichereinrichtung, eine Schnittstelle zu einer externen Programmquelle sowie über mehrere unter Steuerung der Mikroprozessoreinheit steuerbare Baugruppen. Aktivierung und Steuerung der Baugruppen erfolgen mit Hilfe von Applikationsprogrammpaketen, welche von der externen Programmquelle vor erstmaliger Nutzung des Gerätes in die Speichereinrichtung übertragen werden. Das vorgeschlagene Konzept gestattet die Fertigung technisch einheitlicher Geräte, die durch Laden von jeweils entsprechenden Applikationsprogrammpaketen vor Ort auf den Einsatzort abgestimmt werden.

Das in DE-A-38 15 071 beschriebene Konzept bietet den größten Nutzen, wenn die Kommunikationsgeräte herstellerseitig zur Ausführung aller überhaupt möglichen Funktionen vorbereitet sind und über alle dazu notwendigen Baugruppen sowie eine entsprechend groß ausgelegte Speichereinrichtung verfügen. Kommunikationsgeräte dieser Art lassen sich zwar durch Massenfertigung vergleichsweise günstig herstellen, sind aber für viele Anwendungen überdimensioniert. Die alltägliche Nutzung der Geräte setzt im übrigen voraus, daß das jeweilige Gerät bei der Einrichtung durch Laden eines entsprechenden Applikationsprogrammpaketes zur Ausführung der gewünschten Funktion vorbereitet wurde. Es können, anders ausgedrückt, nur Funktionalitäten genutzt werden, die in einem gesonderten Einrichtschritt zuvor eingerichtet wurden. Jede neue Funktionalität oder jede Änderung einer bestehenden muß in einem gesonderten Bedienungsschritt eingerichtet werden.

Der Erfindung liegt die Aufgabe zugrunde, ein flexibles Transaktionssystem mit möglichst einfach aufgebauten Endgeräten anzugeben, das die Einführung neuer Systemmerkmale oder die Änderung bestehender vereinfacht.

Diese Aufgabe wird gelöst durch ein System mit den Merkmalen des Hauptanspruchs. Zur Lösung der Aufgabe führen desweiteren ein Endgerät gemäß unabhängigem Anspruch 9 sowie ein Verfahren gemäß dem unabhängigen Anspruch 19.

Für das erfindungsgemäße System ist bezeichnend, daß die Funktionalität eines Endgerätes nicht durch seine technische Gestaltung bzw. Einrichtung dauerhaft festgelegt wird sondern variabel ist und erst durch Software bestimmt wird, welche es von einem vorgeschalteten Knotenrechner erhält. Hinsichtlich der technischen Ausgestaltung der Endgerätes besteht nur die Vorgabe, daß sie in der Lage sind, von den Knotenrechnern zugeführte Software übernehmen und ausführen zu können. Im Rahmen dieser Vorgabe können die Endgeräte frei und insbesondere unabhängig von ihrer späteren Funktionalität ausgeführt sein. Vorteilhaft können dabei Endgeräte für ganz unterschiedliche Transaktionen technisch einheitlich ausgeführt sein. Durch Verlagerung wesentlicher Teile der möglichen Funktionalitäten in die Knotenrechner ist eine einfache Ausführung der Endgeräte möglich. In vorteilhafter Weise kann dadurch auch die Schnittstelle Terminal-Knotenrechner unabhängig von der Funktionalität des Endgerätes, damit unabhängig von der Art des Endgerätes und damit einheitlich für alle Terminalarten definiert werden. Die in einem festen Rahmen freie Gestaltbarkeit der Endgerätes in Verbindung mit einer einheitlichen Gestaltung der Schnittstellen Terminal-Knotenrechner erleichtert wesentlich die Einrichtung neuer Systemsoftwaremerkmale und/oder die Änderung bestehender. Eine besonders günstige Ausgestaltung sieht vor, daß Systemänderungen nahezu verzögerungsfrei

an den Endgeräten wirksam werden. Indem seine Funktionalität grundsätzlich jederzeit frei konfigurierbar ist, kann jedes Endgerät zur Ausführung mehrerer verschiedener Transaktionen verwendet werden. Auch lassen sich Terminalfunktionalitäten jederzeit neu einrichten und wird die Entwicklung von Software für neue Funktionalitäten wesentlich erleichtert, da Schnittstellen, Netz- oder Terminalbesonderheiten nicht zu beachten sind. Deutlich erleichtert werden desweiteren Service- und Wartungsroutinen.

Das vorgeschlagene Transaktionssystem eignet sich unter anderem zur Verwendung in Bank- oder Zahlungsverkehrsanwendungen, zur Ausgabe elektronischer Fahrscheine oder als Krankenversicherungskarte.

Ein erfindungsgemäßes Endgerät gemäß dem unabhängigen Anspruch 9 zeichnet sich dadurch aus, daß es den Aufbau eines Transaktionssystems gemäß Hauptanspruch ermöglicht.

Das erfindungsgemäße Verfahren gemäß unabhängigem Anspruch 19 hat den Vorteil, daß seine Durchführung auf ein System gemäß dem Hauptanspruch führt.

Weitere zweckmäßige Ausgestaltungen und vorteilhafte Weiterbildungen des Systems gemäß Hauptanspruch, des Endgerätes gemäß unabhängigem Anspruch 9 bzw. des Verfahrens gemäß unabhängigem Anspruch 19 ergeben sich aus den jeweils rückbezogenen Unteransprüchen.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend unter Bezugnahme auf die Zeichnung näher erläutert.

Es zeigen:

	Figur 1	die Struktur eines Transaktionssystems,
	Figur 2	einen Ausschnitt aus der in Figur 1 gezeigten Struktur,
5	Figur 3	ein Flußdiagramm zur Veranschaulichung des Betriebes eines Transaktionssystems,
	Figur 4	ein Flußdiagramm einer Betriebsvariante,
	Figur 5	ein Beispiel für einen Datenaustausch zwischen einem Endgerät und einem Knotenrechner,
10	Fig. 6	einen Datenaustausch bei Verwendung eines Endgerätes zur Ausgabe eines elektronschen Fahrscheins,
	Fig. 7	einen Datenaustausch bei Verwendung eines Endgerätes zur Handhabung von Krankenversicherungskarten.

15 Figur 1 zeigt ein Endgerät 11 zur Ausführung einer Transaktion, welches über ein Endgerätenetz 30 mit einem Knotenrechner 40 verbunden ist. Der Knotenrechner 40 ist seinerseits über ein Hintergrundnetz 50 mit einer Zentraleinheit 60 verbunden. An das Endgerätenetz 30 können parallel zum Endgerät 11 weitere Endgeräte 10 angeschlossen sein, welche dieselbe
20 Grundstruktur wie das Endgerät 11 aufweisen, aber nicht baugleich mit diesem sein müssen. An das Hintergrundnetz 50 können parallel zum Knotenrechner 41 weitere Knotenrechner 40 angeschlossen sein, von denen jeweils wiederum ein Endgerätenetz 30 ausgeht, an das ein oder mehrere Endgeräte 10 angeschlossen sind. An das Hintergrundnetz 50 können weiterhin parallel
25 zur Zentraleinheit 60 weitere Zentraleinheiten 61 angeschlossen sein. Endgerätenetz 30 und Hintergrundnetz 50 können ganz oder teilweise als Fest- oder drahtlose Netze ausgeführt sein; insbesondere das Endgerätenetz 30 kann dabei über das Internet realisiert sein. Entsprechend kann die Anbindung der Endgeräte 10, 11, der Knotenrechner 40, 41 und auch der Zen-

traleinheiten 60, 61 an die jeweiligen Netze 30, 50 drahtgebunden und/oder kontaktlos erfolgen.

Die in Fig. 1 dargestellte Netzstruktur ermöglicht die Durchführung einer Vielzahl von unterschiedlichen Transaktionen, unter anderem zur Ausführung von Zahlungsfunktionen in Form von Lastschriftverfahren oder als Geldbörse, Kreditkartenfunktionen, Kundenkartenfunktionen, Applikationen eines Endgerätenutzers, Krankenversicherungsfunktionen, Service- und Wartungsfunktionen oder Diagnosefunktionen.

Fig. 2 zeigt in detaillierterer Form einen Ausschnitt aus der in Fig. 1 veranschaulichten Netzstruktur mit einem Endgerät 11, einem Knotenrechner 41 und einer Zentraleinheit 61. Ein Hauptbestandteil des Endgerätes 11 ist ein Mikroprozessor 12, welcher über einen geräteinternen Bus 16 mit einer Speichereinrichtung 20, einer Bedienvorrichtung 13, einer Bildanzeigeeinheit 14, einer Nutzerdatenschnittstelle 15, einer kontaktierenden oder kontaktlosen Schnittstelle 16 zum Endgerätenetz 30 sowie einer Sicherheitsbox 17 verbunden ist. Die Speichereinrichtung 20 gliedert sich in an sich bekannter Weise in einen flüchtigen Abschnitt 21, üblicherweise in Gestalt eines RAMs, der insbesondere als Arbeitsspeicher für den Prozessor 12 dient, sowie einen nichtflüchtigen Abschnitt 22, der wiederum in einen nur lesbaren Bereich 23, üblicherweise in Gestalt eines ROMs, sowie einen les- und beschreibbaren Bereich 24, üblicherweise in Gestalt eines EEPROMs, gegliedert ist. Im Nur-Lesebereich 23 befinden sich insbesondere Urbetriebsprogrammdaten, welche für die Herstellung einer Grundbetriebsbereitschaft des Endgerätes 11 unerläßlich sind und die nachträglich nicht mehr verändert werden dürfen, insbesondere ein Urladeprogramm zum Laden von Programmpaketen zur Festlegung der Endgerätefunktionalität. Im les- und beschreibbaren Bereich 24 finden sich vorzugsweise alle Daten, die in Verbindung mit im nur lesba-

ren Bereich 23 enthaltenen Urbetriebsprogrammdaten die Funktionalität des Endgerätes herstellen.

Die Bedienvorrichtung 13 ermöglicht einem Benutzer das Auslösen und/oder das Weiterführen einer Transaktion. Sie verfügt dazu über Betätigungsmittel, mittels derer der Benutzer Steuersignale erzeugen kann, welche über den Bus 16 dem Prozessor 12 zugeführt werden. Die Eingabe der Steuersignale wird durch Anzeigen auf der Bildanzeigeeinheit 14 unterstützt. In einer gängigen Ausführungsform ist die Bedienvorrichtung als Tastenfeld ausgeführt, welches zweckmäßig in Form von Softkeys in die Bildanzeigeeinheit 14 integriert sein kann. Zur Erhöhung der Systemsicherheit kann die Bedienvorrichtung 13 Mittel zur Identifizierung eines Benutzers aufweisen, etwa biometrische Daten auswertende Einrichtungen wie eine Fingerabdruckerkennungseinrichtung.

Die Nutzerdatenschnittstelle 15 ist vorzugsweise als Lese-/Schreibeinheit zur Kommunikation mit einem tragbaren Datenträger 80 ausgebildet, welcher für die nachfolgende Beschreibung einen Teil des Endgerätes 11 bildet. Der Datenträger 80 trägt einen Mikrocomputer 81, der seinerseits einen Mikroprozessor sowie einen Speicher aufweist, wobei letzterer grundsätzlich wie die Speichereinrichtung 20 aufgebaut sein kann. Die Kommunikation zwischen Nutzerdatenschnittstelle 15 und Mikrocomputer 81 kann kontaktbehaftet oder kontaktlos erfolgen. Der tragbare Datenträger 80 ist zweckmäßig als Chip- oder Magnetstreifenkarte ausgeführt, kann aber auch beliebige andere Erscheinungsformen haben, etwa die Gestalt einer Armbanduhr.

Die Sicherheitsbox 17 unterstützt die Systemsicherheit und beinhaltet Informationen, mittels derer über die Schnittstelle 16 an das Endgerätenetz 30 ausgegebene und von dort eingehende Informationen ver- bzw. entschlüsselt

werden, um so ein Ausforschen des über das Endgerätenetz 30 erfolgenden Datenverkehrs durch Unberechtigte zu verhindern.

Der tragbare Datenträger 80 enthält Informationen, die zur Durchführung einer Transaktion mit Hilfe des Endgerätes 11 benötigt werden. Solche Informationen können beispielsweise eine Kontonummer zur Durchführung einer Banktransaktion, ein Wertspeicherinhalt zur Durchführung eines Bezahlvorganges, der Name einer Versicherung zur Vorbereitung einer Krankenbehandlungsabrechnung oder ein Summenspeicherinhalt zur Aufzeichnung von Bonusinformationen sein. Der Mikrocomputer 81 des tragbaren Datenträgers 80 kann darüber hinaus Daten zur Herstellung einer Endgerätefunktionalität enthalten. Weiterhin kann er betriebsnotwendige Bestandteile des endgeräteseitigen Prozessors 12, der endgeräteseitigen Speichereinheit 20 oder der Sicherheitsbox 17 enthalten, so daß ein Betrieb des Endgerätes 11 nur in Einheit mit dem tragbaren Datenträger 80 möglich ist. Soweit sie als Bestandteil des Datenträgers 80 ausgeführt sind, kann endgeräteseitig entsprechend auf den Prozessor 12, die Speichereinrichtung 20 und/oder die Sicherheitsbox 17 ganz oder teilweise verzichtet werden. Auch andere Endgerätekomponenten 13, 14 können entsprechend teilweise oder ganz auf dem Datenträger 80 realisiert sein; Auswahl und Art der Verteilung sind dabei nach Zweckmäßigkeitsgesichtspunkten grundsätzlich frei gestaltbar.

Der oder die Knotenrechner 40, 41 bilden für die Endgeräte 10, 11 Server, welche die über die angeschlossenen Endgeräte 10, 11 ausgelösten Transaktionen in Wechselwirkung mit den Endgeräten 10, 11 ausführen und dabei über das Hintergrundnetz 50 Verbindungen zwischen Endgeräten 10, 11 und Zentraleinheiten 60, 61 herstellen. Zur Durchführung dieser Funktionen sind die Knotenrechner 40, 41 mit entsprechend leistungsfähigen Prozessoreinheiten 44 sowie großen Speichereinrichtungen 45 ausgestattet. Über eine kon-

taktlose oder kontaktbehaftete erste Schnittstelle 42 ist die Prozessoreinheit 44 mit dem Endgerätenetz 30 verbunden, über eine kontaktlose oder kontaktbehaftete zweite Schnittstelle 43 mit dem Hintergrundnetz 50. Zur Sicherung sowohl des Datenverkehrs zu den Endgerätes 10, 11 wie des Datenverkehrs zum Hintergrundnetz 50 hin verfügt der Knotenrechner 41 über eine Cipherbox 46. Sie verwaltet und verarbeitet Informationen zur Ver- bzw. Entschlüsselung des mit dem jeweiligen Endgerät 10, 11 bzw. der jeweiligen Zentraleinheit 60, 61 erfolgenden Datenaustausches. Ver- und Entschlüsselung basieren dabei auf an sich bekannten Mechanismen.

Eine wichtige Funktion des Knotenrechners 41 bildet die Herstellung der zur Durchführung einer Transaktion benötigten Endgerätefunktionalität nach Auslösen der Transaktion an einem Endgerät 10, 11. In der Speichereinheit 45 befinden sich deshalb in der Regel eine Vielzahl von Daten zur Herstellung von auf den angeschlossenen Endgeräten 10, 11 möglichen Funktionalitäten.

Die Zentraleinheiten 60, 61 haben typischerweise die Gestalt üblicher Rechenzentren, wie sie bei Netzbetreibern, Banken, Kreditkarteninstituten, Ladezentralen, Autorisierungszentralen, Servicezentralen und dergleichen zu finden sind. Da Zentraleinheiten 60, 61 in diesem Sinne hinlänglich bekannt sind und sie für das erfindungsgemäße System nur in ihren bekannten Funktionen genutzt werden, wird auf ihren Aufbau hier nicht näher eingegangen.

Eine charakteristische Eigenschaft des in Figur 1 dargestellten Transaktionssystems ist, daß den Endgeräten 10, 11 ihre jeweilige Funktionalität nicht fest zugeordnet ist, sondern durch Software festgelegt wird, die sie von den Knotenrechnern 41 erhalten. Die Festlegung kann dabei dauerhaft oder situati-

onsabhängig wechselnd erfolgen. Vorteilhaft können wesentliche Teile einer Funktionalität in die Knotenrechner 40, 41 verlagert sein. Figur 2 veranschaulicht diese Eigenschaft anhand der Schrittfolge bei der Durchführung einer Transaktion.

Ein Benutzer löst zunächst über die Bedienvorrichtung 13 eine Transaktion aus, Schritt 100. Auf das Auslösesignal hin prüft der Endgeräteprozessor 12 , ob in der Speichereinheit 20 die Daten zur Herstellung der für die beabsichtigten Transaktion benötigten Funktionalität zur Verfügung stehen. Ist das der Fall, führt der Prozessor 12 die mit den vorhandenen Daten möglichen ersten Transaktionsschritte unmittelbar aus, Schritt 102. Beispielsweise veranlaßt der Prozessor 12 bei einer mittels einer Chipkarte 80 durchzuführenden Transaktion die dann als Leseeinheit ausgebildete Nutzerdatenschnittstelle 15 zum Auslesen der Kartendaten aus dem Speicher des Kartenmikrocomputers 81 sowie den Benutzer zur Eingabe weiterer Steuersignale über die Bedienvorrichtung 13, etwa einer Benutzeridentifizierungsinformation. Weiterhin erzeugt der Prozessor 12 eine Startsequenz, Schritt 106, die angibt, welche Transaktion ausgelöst wurde, und die eine Information enthält, die das jeweilige Endgerät 10, 11 identifiziert.

Ergibt die Prüfung in Schritt 102, daß die Daten zur Herstellung einer zur Durchführung einer Transaktion benötigten Funktionalität in der Speichereinheit 20 nicht vorhanden sind, bildet der Prozessor 12 nur die Startsequenz. Die Startsequenz, und, sofern vorhanden, die aufgrund erster ausgeführter Transaktionsschritte vorliegenden Daten verschlüsselt der Prozessor 12 mit Hilfe der in der Sicherheitsbox 17 enthaltenen Sicherungsinformationen und sendet sie über das Endgerätenetz 30 an den zugehörigen Knotenrechner 41.

Dessen Prozessoreinheit 44 empfängt die Daten über die Schnittstelle 42 und entschlüsselt sie mit Hilfe der in der Cipherbox 46 enthaltenen Entschlüsselungsinformationen. Die entschlüsselten Daten prüft die Prozessoreinheit 44 sodann darauf, ob sie nur aus einer Startsequenz bestehen oder bereits die Ergebnisdaten erster Transaktionsschritte beinhalten, Schritt 110. In ersterem Fall ermittelt die Prozessoreinheit 44 aus der Startsequenz die zur Durchführung der ausgelösten Transaktion benötigte Endgerätefunktionalität und prüft, ob die dazugehörenden Daten in der Speichereinheit 45 des Knotenrechners 41 vorhanden sind. Ist das nicht der Fall, fordert die Prozessoreinheit 44 sie über das Hintergrundnetz 50 von einer Zentraleinheit 60, 61 an. Sind die erforderlichen Daten vorhanden, stellt die Prozessoreinheit 44 sie zur Übermittlung an das Endgerät 11 bereit, Schritt 116.

Ergibt die Prüfung im Schritt 110, daß die vom Endgerät 10, 11 erhaltenen ersten Daten bereits Ergebnisse erster ausgeführter Transaktionsschritte beinhalten, bearbeitet die Prozessoreinheit 44 diese und erzeugt erste Antwortdaten. Dabei führt sie in der Regel über das Hintergrundnetz 50 einen Datenaustausch mit den Zentraleinheiten 60, 61.

Im Anschluß an die Bearbeitung der Erstdaten prüft die Prozessoreinheit 44, ob dem Endgerät 11 für die Ausführung der nächsten Transaktionsschritte weitere Daten zur Herstellung der benötigten Funktionalität zuzuführen sind, Schritt 114. Bejahendenfalls fährt sie mit der Durchführung des Schrittes 116 fort und prüft, ob die noch benötigten Daten in der Speichereinheit 45 vorhanden sind. Stellt sie dabei fest, daß benötigte Daten in der Speichereinheit 45 nicht vorhanden sind, fordert sie sie über das Hintergrundnetz 50 von der entsprechenden Zentraleinheit 60, 61 an. Die Daten, sofern solche benötigt werden, sowie die ersten Antwortdaten sendet der Knotenrechner 40, 41 sodann über das Endgerätenetz 30 an das Endgerät 11.

Handelt es sich bei den vom Knotenrechner 41 zurückgesandten Antwortdaten ausschließlich um Daten zur Herstellung einer Funktionalität, d.h. waren die erforderlichen Daten beim Auslösen der Transaktion in der Speichereinheit 20 des Endgerätes 11 nicht vorhanden, übernimmt der Endgeräteprozessor 12 die Daten in die Speichereinheit 20. Anschließend veranlaßt er die Ausführung der ersten Transaktionsschritte. Die daraus resultierenden Erstdaten sendet er zurück an den Knotenrechner 41, welcher darauf die Schrittfolge 102 fortfolgend ausführt.

Beinhalten die vom Knotenrechner 41 an ein Endgerät 11 zurückgesandten Daten weiterführende Antwortdaten, veranlaßt der Endgeräteprozessor 12 die Ausführung der nächsten Transaktionsschritte. Wurden dabei mit den weiterführenden Antwortdaten weitere Daten zur Herstellung der zur Durchführung der Transaktion benötigten Funktionaltität übermittelt, übernimmt er diese in die Speichereinheit 20 und verwendet sie unmittelbar zur Ausführung der nächsten Transaktionsschritte.

Die Daten zur Herstellung der Funktionalität zur Durchführung der Transaktion können nach Abschluß der Transaktion in der Speichereinheit erhalten bleiben. Bei der nächsten Ausführung der Transaktion führt der Endgeräteprozessor 12 dann die ersten Transaktionschritte nach dem Auslösen einer Transaktion unmittelbar durch, ohne vorher die Daten zur Herstellung der benötigten Funktionalität vom Knotenrechner 41 anzufordern. Das Endgerät 11 kann die aufgrund einer Funktionalität möglichen Transaktionen jederzeit ohne Notwendigkeit zur Anforderung von Daten von einem Knotenrechner 40, 41 erneut ausführen.

Vorgesehen sein kann andererseits, daß die Daten zur Herstellung der Funktionalität für eine Transaktion nach Abschluß der Transaktion jeweils wieder gelöscht werden. Der Endgeräteprozessor 12 lädt dann bei jeder Transaktionsausführung die zur Herstellung der benötigten Funktionalität notwendigen Daten jeweils neu. Die Speichereinrichtung 20 kann in diesem Fall neben dem Bereich 23 zur Speicherung der Urprogrammdaten nur aus einem flüchtigen Speicherbereich 21 bestehen.

Die Übertragung von zur Herstellung der Funktionalität für eine bestimmte Transaktion benötigten Daten muß nicht zwingend durch Auslösen der Transaktion selbst ausgelöst werden. Sie kann vielmehr auch unabhängig vom tatsächlichen Auslösen einer bestimmten Transaktion erfolgen. Auslöser können beliebige, definierte Ereignisse sein. Beispielsweise kann vorgesehen sein, beim erstmaligen Anschluß eines Endgerätes an ein Netz die Daten für die wichtigsten oder die am häufigsten ausgeführten Transaktionen in das Endgerät zu übertragen. In einer Variante hierzu werden Daten für die wichtigsten oder die am häufigsten ausgeführten Transaktionen geladen, wenn erstmals eine beliebige der wichtigsten oder häufigsten Transaktionen ausgelöst wird. Ein weiteres mögliches Auslöseereignis ist die regelmäßig oder auf Anforderung vorgenommene Durchführung von Service- oder Wartungsmaßnahmen an den Endgeräten. In allen Fällen kann eine einmal ausgelöste Datenübertragung zur regelmäßigen Aktualisierung von in einem Endgerät bereits eingerichteten Funktionalitäten genutzt werden; im Speicher des Endgerätes werden dabei überholte Versionen mit aktuellen überschrieben.

Fig. 4 veranschaulicht einen möglichen Ablauf einer nicht unmittelbar transaktionsgebundenen Datenübertragung vom Knotenrechner zum Endgerät.

Der Ablauf wird durch Eintritt eines vorbestimmten Ereignisses eingeleitet, Schritt 101, etwa durch Erreichen eines Servicezeitpunktes.

Das Endgerät 11 bildet darauf wieder eine Startsequenz, Schritt 106, die angibt, welche Transaktion ausgelöst wurde, und die eine Information enthält, die das jeweilige Endgerät 11 identifiziert.und sendet sie an den zugehörigen Knotenrechner.

Der Knotenrechner 41 prüft, ob die Startsequenz unmittelbar eindeutig zu übertragende Daten festlegt, Schritt 111.

Ist das nicht der Fall, erzeugt der Knotenrechner eine Anfrage zur Feststellung der dem Endgerät zu übertragenden Daten und sendet diese an das Endgerät, Schritt 113.

Das Endgerät führt die Anfrage aus und benennt dem Knotenrechner in einer entsprechenden Rückmeldung die gewünschten Daten, Schritt 115.

Der Knotenrechner 41 prüft darauf, ob die benötigten Daten in der Speichereinheit 45 vorhanden sind. Stellt er dabei fest, daß benötigte Daten in seiner Speichereinheit 45 nicht vorhanden sind, fordert er sie über das Hintergrundnetz 50 von der entsprechenden Zentraleinheit 61 an. Die Daten sendet er sodann über das Endgerätenetz 30 an das Endgerät 1, Schritt 119.

Folgen die Informationen über die zu übertragenden Daten direkt aus der Startsequenz bei deren Prüfung in Schritt 111, führt der Knotenrechner unmittelbar Schritt 119 aus.

Vorgesehen sein kann ferner, die Endgeräte bereits im Neuzustand mit einer Auswahl von Funktionalitäten auszurüsten. Die Auswahl kann zweckmäßig die wichtigsten oder die am häufigsten benutzten Funktionalitäten umfassen. Sofern insbesondere die Speicherkapazität das zuläßt, können auch alle möglichen Funktionalitäten auf einem Endgerät eingerichtet sein.

Figur 5 veranschaulicht einen möglichen Datenaustausch zwischen einem Knotenrechner 41 und einem als Zahlungsverkehrterminal eingesetzten Endgerät 11. Bei dem dargestellten Datenaustausch sind wesentliche Teile der Funktionalität im Knotenrechner 41 realisiert. Es sei angenommen, daß die Daten zur Herstellung der Funktionalität "Zahlungsverkehr" bereits in der Speichereinheit 20 des Endgerätes 11 vorhanden sind und daß die mittels des Endgerätes 11 ausführbaren Transaktionen die Verwendung einer Chipkarte 80 voraussetzen. Bei der Transaktion handele es sich um einen Zahlungsvorgang, der die Umbuchung eines Geldbetrages von einem zu der Chipkarte 80 korrespondierenden Konto bei einer ersten Bank mit der Zentraleinheit 61 auf ein Konto bei einer zweiten Bank mit der Zentraleinheit 61 nach sich ziehe. Bei dem Endgerät 11 handele es sich um um ein bei einem Händler installiertes Terminal, zu dem im zugeordneten Knotenrechner 41 eine virtuelle Händlerkarte, d.h. ein in Programmform realisierter Datenträger nach Art einer Chipkarte angelegt sei.

Das Auslösen der Zahlungstransaktion erfolgt durch Einbringen der Chipkarte 80 in die als Leseeinrichtung ausgeführte Nutzerdatenschnittstelle 15. Erkennt das Endgerät 11, daß eine Transaktion durchgeführt werden soll, erfolgt zweckmäßig zunächst in bekannter Weise eine Prüfung der Berechtigung des Benutzers zur Verwendung der Karte 80, etwa durch Prüfen einer PIN. Fällt diese Prüfung positiv aus, liest das Endgerät 11 aus dem Speicher 83 der Chipkarte allgemeine Kartendaten aus, etwa eine Kartennummer

und/oder eine Bankverbindung. Ermöglicht die Karte mehrere verschiedene Transaktionen, ist sie etwa wahlweise als Geldbörse oder als Debit- oder Kreditkarte betreibbar, veranlaßt das Endgerät 11 den Benutzer durch Anzeige auf der Bildanzeigevorrichtung 14 zur Auswahl einer Transaktion, d.h. zur Auswahl einer Zahlungsart. Darauf veranlaßt es den Benutzer durch Anzeige auf der Bildanzeigevorrichtung 14 zur Eingabe eines Betrages, der umgebucht werden soll. Desweiteren stellt das Endgerät 11 Daten zur Terminalidentifikation sowie eine Datumsinformation bereit. Aus allgemeinen Kartendaten, Betrag, Terminalinformationsdaten sowie Datumsinformation bildet das Endgerät eine Startsequenz, Schritt 200, welche es an den Knotenrechner 41 sendet. Das Senden der Startsequenz und der gesamte nachfolgende Datenaustausch zwischen Endgerät 11 und Knotenrechner 41 erfolgen verschlüsselt, wobei für die Verschlüsselung an sich bekannte Verfahren eingesetzt werden. Ein erster Schlüssel ist zweckmäßig dem Endgerät 11 zugeordnet und wird im Rahmen der Startsequenz oder gegebenenfalls in einem vorgeschalteten Schritt aufgrund der Endgeräteidentifikation gebildet. Er dient nachfolgend als übergreifender Transportschlüssel, mit dem der gesamte Datenaustausch zwischen Endgerät 11 und Knotenrechner 41 abgesichert wird. Ein weiterer Schlüssel ist zweckmäßig der Chipkarte 80 zugeordnet und wird zur Bildung von Datensicherungscodes genutzt, um insbesondere die Unversehrtheit von Daten prüfen zu können.

Der Knotenrechner 41 ermittelt die zu der in der Startsequenz bezeichneten Bankverbindung korrespondierende Zentraleinheit 61, bei der das zu der Karte 80 gehörende Konto angelegt ist, Schritt 202. Mit der ermittelten Zentraleinheit 61 beginnt er einen Datenaustausch. Darin wird beispielsweise zunächt geprüft, ob der beabsichtigte Zahlungvorgang überhaupt zugelassen ist. Ist die beabsichtigte Transaktion danach grundsätzlich möglich, übermittelt der Knotenrechner 41 dem Endgerät 11 Daten, welche das End-

gerät 11 zur Ausführung der beabsichtigten Transaktion einrichten und insbesondere Befehle umfassen, welche die Nutzerdatenschnittstelle 15 zur Ausführung von weiteren Zugriffen auf die Chipkarte 80 veranlassen, Schritt 204. Daneben enthalten die Daten Befehle, welche das Endgerät 11 veranlassen, mitzuteilen, wer der Empfänger bzw. der Geber einer Zahlung sein soll.

Die erhaltenen Daten und Chipkartenbefehle führt das Endgerät 11 aus, Schritt 206. Ist die Chipkarte 80 zur Ausführung einer Abbuchung vorbereitet, übersendet das Endgerät 11 dem Knotenrechner 41 nach Verschlüsselung eine Rückmeldung, Schritt 208, welche im zugrundegelegten Beispiel eine Information beinhaltet, daß von der Karte eine Zahlung auf die dem Endgerät zugehörige virtuelle Händlerkarte erfolgen soll.

Der Knotenrechner 41 bestimmt aus der Rückmeldung, wem ein von der Karte 80 oder dem zugehörigen Konto ab- bzw. aufzubuchender Betrag gutgeschrieben bzw.belastet werden soll, im angenommenen Beispiel der virtuellen Händlerkarte. Anhand der in der Startsequenz zugesandten Terminalinformationsdaten liest der Knotenrechner 41 daher den Speicher der virtuellen Händlerkarte aus, und ermittelt die der Händlerkarte zugehörige Zentraleinheit 60. Mit dieser eröffnet er sodann einen Datenaustausch, Schritt 210, um die virtuelle Händlerkarte zum Aufbuchen einzurichten.

Sind Chipkarte 80 und Händlerkarte vorbereitet, sendet der Knotenrechner 41 dem Endgerät 11 Buchungsbefehle, die endgeräteseitig die Eintragung der Abbuchung im Speicher der Chipkarte 80 bewirken, Schritt 218. Parallel dazu vermerkt er im Speicher der virtuellen Händlerkarte die entsprechende Aufbuchung und veranlaßt in einem Datenaustausch über das Hintergrundnetz 50 die Ausführung der Buchung zwischen den beteiligten Zentraleinheiten 60, 61.

Das Endgerät 11 nimmt die Eintragung der Abbuchung auf der Chipkarte vor, Schritt 220, und quittiert den Abschluß der Transaktion durch Rücksendung einer bestätigenden Rückmeldung an den Knotenrechner 41, Schritt 222.

Ist der buchungtechnische Teil der Transaktion beendet, erzeugt der Knotenrechner 41 Steuerdaten, welche das Endgerät 11 zur Darstellung einer Beleganzeige über die ausgeführte Transaktion, d.h. über den ausgeführten Buchungsvorgang auf der Bildanzeigevorrichtung 14 veranlassen, Schritt 224. Ist dem Endgerät 11 eine Belegausgabe zugeordnet, etwa in Gestalt eines Druckers, erzeugt der Knotenrechner 41 zweckmäßig auch Steuerdaten zum Ausdruck eines Beleges. Die Steuerdaten sendet er an das Endgerät 11, das sie ohne weitere Verarbeitung zur Ausführung bringt, Schritt 226.

Fig. 6 veranschaulicht als weitere mögliche Nutzung des in Fig. 2 dargestellten Transaktionssystems eine Variante, in der das Endgerät 11 zur Ausgabe elektronischer Fahrscheine genutzt wird. Es wird angenommen, daß der elektronische Fahrschein die Gestalt eines Datensatzes hat, welcher in den Speicher einer Chipkarte 80 eingebracht wird. Das Endgerät 11 besitzt entsprechend eine Nutzerdatenschnittstelle 15 in Gestalt einer Chipkartenkontaktiereinheit.

Das Auslösen einer Fahrscheinausgabetransaktion erfolgt, indem der Kunde dem Endgerät 11 die Chipkarte 80 präsentiert und/oder z.B. über die Bedienvorrichtung 13 mitteilt, daß er die Transaktion „elektronischer Fahrschein" ausführen will, Schritt 300, um einen elektronischen Fahrschein zu erwerben. Erkennt das Endgerät 11 hierauf, daß eine Fahrscheinausgabetransaktion durchgeführt werden soll, kann zunächst eine Prüfung der Be-

rechtigung des Kunden zur Verwendung der Chipkarte 80 für die vorgesehene Transaktion vorgesehen sein, etwa in bekannter Weise durch Prüfen einer PIN.

Steht fest, daß die Transaktion „elektronischer Fahrschein" ausgeführt werden soll und daß der Kunde zur Durchführung der Transaktion berechtigt ist, ermittelt das Endgerät 11 die Kartennummer der Chipkarte 80 und prüft, ob es zur weiteren Ausführung einer Transaktion „elektronischer Fahrschein" eingerichtet ist, Schritt 302. Ist das nicht der Fall, stellt es ferner fest, ob ausreichend Freispeicherraum zur Einrichtung der Funktionalität verfügbar ist.

Nachfolgend erzeugt das Endgerät 11 eine Startsequenz 306, welche die Kartennummer sowie eine Endgeräteidentifikation beinhaltet. Ist die zur Durchführung der Transaktion „elektronischer Fahrschein" benötigte Funktionalität in der Speichereinheit 20 des Endgerätes 11 nicht vorhanden, beinhaltet die Startsequenz 306 weiterhin eine Information, welche anzeigt, daß das Endgerät 11 die, im folgenden Applikation genannten Daten zur Einrichtung der Funktionalität benötigt.

Die Startsequenz 306 wird mittels eines dem Endgerät 11 zugeordneten, übergreifenden Transportschlüssels verschlüsselt, welcher unter Verwendung der Endgeräteidentifikation im Rahmen der Startsequenz oder in einem vorgeschalteten, gesonderten Datenaustausch nach einem üblichen Verfahren generiert wird. Mit dem Transportschlüssel wird der gesamte nachfolgende Datenaustausch zwischen Endgerät 11 und Knotenrechner 41 abgesichert. Erzeugung und Nutzung des Schlüssels beruhen dabei in an sich bekannter Weise darauf, daß die Kommunikationsteilnehmer unabhängig voneinander jeweils ein Geheimnis kennen, das nicht über das Endgerä-

tenetz 30 zwischen Endgerät 11 und Knotenrechner 41 ausgetauscht werden kann. Das Geheimnis ist auf der einen Seite im Endgerät 11, vorzugsweise in der Sicherheitsbox 17, fest abgelegt und wird auf der anderen Seite im Knotenrechner 41 oder über das Hintergrundnetz 50 durch die Zentraleinheiten 60, 61 verwaltet. Ist ein zur Generierung eines Schlüssels notwendiges Geheimnis in einem Knotenrechner 41 nicht verfügbar, beschafft dieser es sich von der verwaltenden Zentraleinheit 60, 61.

Die verschlüsselte Startsequenz 306 übersendet das Endgerät 11 an den zugeordneten Knotenrechner 41. Dessen Prozessoreinheit 44 prüft nach Erhalt - und Entschlüsselung - der Startsequenz 306, ob die Applikation „elektronischer Fahrschein" in der Speichereinheit 45 des Knotenrechners 41 vorhanden ist, Schritt 308. Ist das nicht der Fall ermittelt der Knotenrechner 41, etwa mit Hilfe der Endgeräteinformation, eine Zentraleinheit 60, 61, welche über die die Applikation resalisierenden Daten verfügt und fordert über das Hintergrundnetz 50 von ihr die Daten an. Liegen Applikationsdaten bereit, Schritt 310, übermittelt der Knotenrechner 41 sie an das Endgerät 11.

Dessen Prozessor 12 übernimmt die Applikationsdaten in die Speichereinheit 20 und führt die eingerichtete Funktionalität aus, Schritt 312. Das Endgerät 11 fordert den Kunden hierbei über die Bildanzeigevorrichtung 14 auf, einen Fahrschein auszuwählen. Die Auswahl erfolgt benutzergeführt im Dialog. Der Kunde macht dabei mittels der Bedienvorrichtung 13 jeweils gemäß einer Aufforderung durch die Bildanzeigevorrichtung 14 Angaben, die zur Ermittlung des benötigten Fahrscheines erforderlich sind, etwa Start- und Zielort, Fahrzeitpunkt, Anzahl der Personen, Reiseklasse usw., Schritt 314. Sind in das Endgerät 11 alle zur Ermittlung eines Fahrscheines notwendigen Angaben eingegeben worden, übermittelt das Endgerät 11 die Auswahldaten an den Knotenrechner 41.

Aus den vom Endgerät 11 erhaltenen Angaben zur Fahrscheinauswahl ermittelt der Knotenrechner 41 einen den elektronischen Fahrschein repräsentierenden Datensatz, Schritt 316. Zweckmäßig ist der Knotenrechner 41 dabei dazu eingerichtet, einfache und besonders häufig angeforderte Fahrscheinermittlungen, etwa die Ermittlung eines Fahrscheines des lokalen Verkehrsbetriebes, unmittelbar durch die Prozessoreinheit 44 des Knotenrechners 41 vorzunehmen. In vielen Fällen bedingt die Ermittlung eines Fahrscheines allerdings komplexe Programmabläufe, die üblicherweise die Einschaltung einer Zentraleinheit 60, 61 über das Hintergrundnetz 50 erfordern. Der resultierende Fahrscheindatensatz beinhaltet neben den für die Ermittlung verwendeten Informationen ggf. die möglichen Fahrscheinalternativen sowie insbesondere den oder die Fahrpreise.

Sodann generiert der Knotenrechner 41 aus der Kartennummer sowie einem Geheimnis, das auch in der Chipkarte 80 fest abgelegt ist, einen chipkartenspezifischen Schlüssel, welcher nachfolgend zur Bildung eines Datensicherungscodes dient, Schritt 318.

Hat der Knotenrechner 41 einen chipkartenspezifischen Schlüssel erzeugt, bildet er damit zu dem resultierenden Fahrscheindatensatz einen Datensicherungscode, etwa einen MAC (Message Authentication Code) und verschlüsselt den resultierenden, aus Fahrscheindatensatz und Datensicherungscode bestehenden Fahrscheindatenblock mit Hilfe des Transportschlüssels, Schritt 320. Den resultierenden verschlüsseltem Fahrscheindatenblock übermittelt der Knotenrechner 41 an das Endgerät 11.

Den angekommenen Fahrscheindatenblock entschlüsselt das Endgerät 11 mit Hilfe des Transportschlüssels, den es, z. B. in der Sicherheitsbox 17, auf

gleiche Weise wie der Knotenrechner 41 generiert. Dabei führt das Endgerät 11 zugleich eine Vorprüfung der Unversehrtheit des Fahrscheindatensatzes durch, indem es z.B. prüft, ob der entschlüsselte Fahrscheindatensatz an definierten Posititonen bestimmte Werte aufweist. Den entschlüsselten Fahrscheindatensatz leitet das Endgerät 11 an die Chipkarte 80 weiter, welche durch Überprüfung des Datensicherungscodes mittels des auf der Chipkarte 80 vorhandenen chipkartenspezifischen Schlüssels seine Unversehrtheit kontrolliert.

Erweist sich der Fahrscheindatensatz danach als unversehrt, fordert das Endgerät 11 den Kunden durch entsprechende Darstellung auf der Bildanzeigeeinheit 14 dazu auf, den elektronischen Fahrschein auf Richtigkeit zu prüfen und den Kauf zu bestätigen, Schritt 322. Beinhaltet der Fahrscheindatensatz mehrere mögliche elektronische Fahrscheinalternativen, fordert das Endgerät 11 den Kunden dabei auf, eine Auswahl aus den angebotenen Alternativen zu treffen. In einfachen, alternativlosen Fällen, beispielsweise bei Kauf eines Fahrscheins für einen lokalen Verkehrsbetrieb, sind Auswahl und Kaufbestätigung durch den Kunden nicht erforderlich.

Ist der an das Endgerät 11 übersandte elektronische Fahrschein danach durch den Kunden akzeptiert, wird der bestätigte, den ausgewählten Fahrschein ausmachende Teil des Fahrscheindatensatzes zunächst in der Speichereinrichtung 20 des Endgerätes 11 zwischengespeichert, Schritt 324. Desweiteren veranlaßt das Endgerät 11 die Bezahlung des elektronischen Fahrscheins, Schritt 326. Der Bezahlvorgang kann durch Barzahlung oder etwa, wie in Zusammenhang mit Fig. 5 beschrieben, durch Einziehung von auf der Chipkarte 80 gespeicherten elektronischen Geld erfolgen.

Ist der Bezahlvorgang abgeschlossen, erzeugt der Knotenrechner 41 ein Quittungssignal, Schritt 328, welches er an den Knotenrechner 41 übermittelt.

Nach Erhalt des Quittungssignales erzeugt der Knotenrechner 41 einen Steuerbefehl, welcher den Prozessor 12 des Endgerätes 11 veranlaßt, den in der Speichereinrichtung 20 abgelegten Fahrscheindatensatz auf die Chipkarte 80 zu übertragen.

Das Endgerät 11 nimmt die Übertragung des elektronischen Fahrscheines auf die Chipkarte vor, Schritt 330, und quittiert den Abschluß der Transaktion durch Rücksendung einer bestätigenden Rückmeldung an den Knotenrechner 41, Schritt 332. An den Eingang dieser Rückmeldung im Knotenrechner 41 kann sich beispielsweise die Ausgabe eines Beleges, etwa durch einen dem Endgerät 11 zugeschalteten Drucker anschließen.

Fig. 7 veranschaulicht als weitere mögliche Nutzung des in Fig. 2 dargestellten Transaktionssystems eine Variante, in der ein Endgerät in einem Krankenversicherungskartensystem eingesetzt ist. Es wird angenommen, daß die Krankenversicherungskarte wiederum die Gestalt einer Chipkarte 80 aufweist und die Funktionalität zur Handhabung von Krankenversicherungskarten in der Speichereinheit 20 des Endgerätes 11 bereits vorhanden ist. Das Endgerät 11 befindet sich beispielsweise in einer Arztpraxis, einem Krankenhaus oder einer Institution zur Abrechnung medizinischer Leistungen, etwa einer Krankenversicherung. Dem medizinischen Personal sind dabei in Bezug auf die Krankenversicherungskarte 80 andere Zugriffsrechte eingeräumt als den Angehörigen der Krankenversicherung.

Eine Transaktion unter Verwendung einer, nachfolgend einfach als Karte bezeichneten Krankenversicherungskarte 80 wird eingeleitet, indem die Karte 80 der Nutzerdatenschnittstelle 15 des Endgerätes 11 präsentiert wird, Schritt 400. Das Endgerät 11 betätigt darauf über die Bildanzeigeeinheit 14, daß eine Transaktion unter Verwendung einer Krankenversicherungskarte angefordert wurde und fordert - im Normalbetrieb - den Bediener auf anzugeben, ob er auf die Karte 80 nur lesend oder schreibend und lesend zugreifen möchte, Schritt 402. Weiter fordert es den Bediener auf, Schritt 404, anzugeben, auf welche auf der Karte 80 abgelegten Daten er zugreifen möchte. Die in der Speichereinrichtung der Karte 80 gehaltenen Daten sind zweckmäßig nach ihrer sachlichen Natur, z.B. abrechnungstechnisch oder medizinisch gegliedert, wobei diese Gliederung weiter z.B. nach Art des medizinischen Fachgebietes feinunterteilt ist. Die Gliederungsbereiche sind einzeln oder in Gruppen durch gebietsbezogene Zugriffsschlüssel gegen Lese- und Schreibzugriffe geschützt. Die Zugriffsschlüssel leiten sich vorzugsweise aus dem kartenspezifischen Schlüssel sowie einer den Bediener, etwa einen Arzt, oder den Gliederungsbereich, etwa ein medizinisches Fachgebiet, charakterisierenden Information ab.

Steht fest, welche Art Zugriff auf welchen Bereich der Karte 80 der Bediener wünscht, fordert das Endgerät 11 den Bediener über die Bildanzeigeeinheit 14 auf, sich zu identifizieren, Schritt 406. Dies kann beispielsweise mittels der Bedienvorrichtung 13 durch Eingabe eines Codes zur Identifizierung eines Arztes, eines Krankenhauses oder einer Krankenversicherung erfolgen. Desweiteren ermittelt das Endgerät 11 die Kartennummer der Karte 80.

Aus den Angaben über gewünschte Zugriffsart, Kartenbereich, auf den zugegriffen werden soll, Identifikationscode, Nummer der präsentierten Karte 80 sowie aus der Endgeräteidentifikation bildet das Endgerät 11 eine Startse-

quenz, Schritt 408, welche sie an den zugeordneten Knotenrechner 41 übermittelt. Die Übermittlung erfolgt verschlüsselt unter Verwendung eines Transportschlüssels, welcher unter Verwendung der Endgeräteidentifikation gegebenenfalls in einem vorgeschalteten Datenaustauschschritt generiert und mit dem der gesamte nachfolgende Datenaustausch zwischen Endgerät 11 und Knotenrechner 41 abgesichert wird.

Nach Eingang der Startsequenz 408 im Knotenrechner 41 bildet dieser mit Hilfe der Kartennummer sowie eines der Karte 80 zugeordneten Geheimnisses einen kartenspezifischen Schlüssel. Ist das Geheimnis dabei nicht im Knotenrechner 41 selbst verfügbar, ermittelt er es über das Hintergrundnetz 50 von der verwaltendendem Zentraleinheit 60, 61.

Sodann prüft der Knotenrechner 41, ob sich die zur Bewertung der Startsequenz 408 notwendigen Informationen im Speicher 45 befinden. Ist das nicht der Fall, ermittelt er eine zur Bewertung der Startsequenz geeignete Zentraleinheit 60 und leitet mit dieser über das Hintergrundnetz 15 einen Datenaustausch ein, Schritt 412. Im Rahmen des folgenden Datenaustausches prüft der Knotenrechner 41 unter Verwendung des mit der Startsequenz 408 übetragenen Bedieneridentifikationscodes, ob der vom Bediener gewünschte Zugriff auf die Karte 80 zulässig ist. Ist das der Fall, werden im Knotenrechner 41 Einrichtungsdaten bereitgestellt, welche das Endgerät 11 befähigen, den gewünschten Zugriff auf die Karte 80 durchzuführen, Schritt 414. Vorzugsweise beinhalten die Einrichtungsdaten hierfür einen oder mehrere jeweils einzelnen Bereichen der Karte 80 zugeordnete Zugriffsschlüssel.

Zu den Einrichtungsdaten bildet der Knotenrechner 41 sodann mittels des kartenspezifischen Schlüssels einen Datensicherungscode, Schritt 416. Der aus Einrichtungsdaten und Datensicherungscode bestehende Datensatz wird

anschließend mit dem Transportschlüssel verschlüsselt und an das Endgerät 11 übersandt.

Jenes entschlüsselt den eingegangenen Datensatz mit Hilfe des Transportschlüssels und führt dabei zugleich eine Vorprüfung des Datensatzes auf Unversehrtheit durch, z.B. durch Prüfen des Vorhandenseins bestimmter Datenwerte an definierten Positionen des Datensatzes. Fällt die Vorprüfung positiv aus, übermittelt das Endgerät 11 die Einrichtungsdaten an die Karte 80. Diese kontrolliert die Einrichtungsdaten mit Hilfe des kartenspezifischen Schlüssels durch Prüfen der Richtigkeit des Datensicherungscode auf Unversehrtheit. Wird die Unversehrheit der Einrichtungsdaten festgestellt, kann anschließend über das Endgerät 11 der gemäß den Einrichtungsdaten mögliche Zugriff auf die Karte 80 durchgeführt werden.

Neben den im Normalbetrieb durchführbaren Zugriffen ist im Endgerät 11 zweckmäßig noch eine Zugriffsart für Notfälle eingerichtet. Ausgelöst wird eine Notfalltransaktion wie eine Transaktion im Normalbetrieb, jedoch identifiziert sich der Bediener im Schritt 406 nicht durch eine personenindividuelle Identifikation, sondern durch eine Notfallidentifikation.

Erkennt der Knotenrechner 41 bzw. eine Zentraleinheit 60, 61, nach Erzeugung eines Schlüssels zur Bildung eines Datensicherungscodes sowie eines Transportschlüssels, bei der Bewertung der Startsquenz 408 eine Notfallidentifikation, stellt er im Knotenrechner 41 anhand der Kartennummer einen Satz von Zugriffsschlüsseln bereit, welcher zumindest einen Lesezugriff auf alle auf der Krankenversicherungskarte 80 befindlichen medizinischen Daten ermöglicht. Zur Beschleunigung der Transaktionsausführung kann vorgesehen sein, daß auf eine zusätzliche Prüfung der Berechtigung des Bedieners verzichtet wird. Den Zugriffsschlüsseldatensatz versieht der Knotenrechner

mit einem Datensicherungscode, Schritt 416, verschlüsselt beide mit dem Transportschlüssel und übermittelt den resultierenden Datensatz an das Endgerät 11.

Dieses entschlüsselt den eingegangenen Datensatz wieder mit dem Transportschlüssel und leitet ihn der Karte 80 zur Prüfung auf Unversehrtheit mittels des kartenspezifischen Schlüssels weiter. Wird Unversehrtheit des übermittelten Schlüsseldatensatzes festgestellt, erlaubt das Endgerät 11 den Lesezugriff auf sämtliche auf der Karte 80 vorhandenen medizinischen Daten.

Unter Beibehaltung des grundlegenden Konzeptes, in einem Transaktionssystem die Funktionalität der nutzerseitigen Endgeräte durch vorgeschaltete Knotenrechner zu bestimmen, lassen sich das vorgeschlagene System, die zu seiner Realisierung eingesetzten Komponenten sowie das Betriebsverfahren in weitem Rahmen variieren. Dies gilt etwa für die physikalische Struktur der Endgeräte 10, 11. Deren Komponenten können zusammengefaßt sein, indem Speichereinheit 20, Prozessor 12, Kryptobox 17 und Bedienvorrichtung 13 beispielsweise eine Einheit bilden. An ein Endgerätenetz 30 können mehrere Knotenrechner 40, 41 angeschlossen sein, welche zur Ausführung unterschiedlicher Transaktionen dienen. Die möglichen Nutzungen des Systems sind selbstverständlich nicht auf die beschriebenen Ausführungsbeispiele beschränkt. Neben der Art der Transaktionen kann dabei insbesondere auch die Verteilung der Funktionalität auf Endgeräte und Knotenrechner variiert werden. Dabei kann sich die in den Endgeräte zugeordnete Funktionalität einerseits auf das Durchreichen von Daten an einen Datenträger beschränken, andererseits kann eine weitgehende Datenverarbeitung unmittelbar durch ein Endgerät eingerichtet werden. Ohne Beeinträchtigung des grundlegenden Gesamtkonzeptes läßt sich ferner das Verschlüsselungskon-

zept mit Transportschlüssel und datenträgerbezogenem Schlüssel in einem weiten Rahmen variieren, wobei eine Verschlüsselung auf der einen Seite gänzlich entfallen, auf der anderen Seite zusätzliche Verschlüsselungen vorgesehen sein können.

Patentansprüche

1. System zur Ausführung von Transaktionen mit

- einer Mehrzahl von Endgeräten, welche zur Ausführung einer Vielzahl verschiedener Transaktionen geeignet sind, sowie
- einem Knotenrechner, der über ein Endgerätenetz mit den Endgeräten verbunden ist,
- wobei die Eignung eines Endgerätes zur Ausführung einer Transaktion über einen Knotenrechner herstellbar ist, indem dieser dem Endgerät Daten übermittelt, welche dort die zur Ausführung der Transaktion benötigte Funktionalität einrichten,

dadurch **gekennzeichnet,** daß

zumindest ein Endgerät (10, 11) dazu ausgebildet ist, während seiner üblichen Nutzung die Einrichtung zur Ausführung einer weiteren Transaktion zu veranlassen, indem es auf ein im Zusammenhang mit der Ausführung einer Transaktion erzeugtes Auslösesignal hin von einem Knotenrechner (40, 41) Daten anfordert, welche die zur Ausführung der weiteren Transaktion benötigte Funktionalität herstellen.

2. System nach Anspruch 1, dadurch **gekennzeichnet,** daß die Ausführung wenigstens einer Transaktion in Wechselwirkung zwischen einem Endgerät (10, 11) und einem Knotenrechner (41) erfolgt.

3. System nach Anspruch 1, dadurch **gekennzeichnet,** daß das Endgerät (10, 11) die Übermittlung der Daten zur Einrichtung der Funktionalität zur Ausführung der Transaktion veranlaßt.

4. System nach Anspruch 3, dadurch **gekennzeichnet,** daß das Endgerät (10, 11) eine Datenübermittlung auf den Eintritt eines vorbestimmten Ereignisses im Endgerät (10, 11) hin veranlaßt.

5. System nach Anspruch 3, dadurch **gekennzeichnet,** daß das Endgerät (10, 11) eine Datenübermittlung auf das Auslösen der bestimmten Transaktion im Endgerät (10, 11) hin veranlaßt.

6. System nach Anspruch 1, dadurch **gekennzeichnet,** daß der Knotenrechner (40, 41) über ein Hintergrundnetz (50) mit mindestens einer Zentraleinheit (60, 61) verbunden und diese in eine Transaktion einbeziehbar ist.

7. System nach Anspruch 3, dadurch **gekennzeichnet,** daß der Knotenrechner (40, 41) Daten von der Zentraleinheit (60, 61) abrufen kann.

8. System nach Anspruch 1, dadurch **gekennzeichnet,** daß der Knotenrechner (40, 41) eine Cipherbox (17) besitzt, welche Informationen zur Ver- bzw. Entschlüsselung des mit dem Endgerät (10, 11) erfolgenden Datenverkehrs verarbeitet.

9. Endgerät zur Ausführung einer Transaktion mit

- einer Prozessoreinheit (12),
- einer damit verbundenen Speicherinrichtung (20) zur Aufnahme von Daten, welche die Funktionalität der Prozessoreinheit (12) einrichten,
- Mitteln (13, 14, 15) zum Auslösen einer Transaktion, sowie
- einer Schnittstelle (18) zur Verbindung mit einem Knotenrechner (41) über ein Endgerätenetz (30),

dadurch **gekennzeichnet,** daß die Prozessoreinheit (12) im Zuge der üblichen Nutzung des Endgerätes (10, 11) auf ein im Zusammenhang mit der

Ausführung einer Transaktion erzeugtes Auslösesignal hin die Einrichtung des Endgerätes (10, 11) zur Ausführung einer weiteren Transaktion veranlaßt, indem es von einem Knotenrechner (40, 41) Daten anfordert, welche die zur Ausführung der Transaktion benötigte Funktionalität herstellen.

10. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß es die Daten zur Einrichtung einer Funktionalität auf den Eintritt eines vorbestimmten Ereignisses hin vom Knotenrechner (41) anfordert.

11. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß das vorbestimmte Ereignis das Auslösen einer Transaktion ist, deren Ausführung eine Funktionalität erfordert, die nur unvollständig oder gar nicht in der Speichereinheit (20) vorhanden ist.

12. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß es eine Sicherheitsbox (17) aufweist, welche Informationen zur Ver- bzw. Entschlüsselung des mit dem Knotenrechner (40, 41) erfolgenden Datenverkehrs enthält..

13. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß die Mittel zum Auslösen einer Transaktion eine Tastatur (13) und eine Display (14) umfassen.

14. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß es eine Vorrichtung (15) zum Lesen von tragbaren Datenträgern (80) aufweist.

15. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß es dem Knotenrechner (40, 41) zur Anforderung von Daten zur Einrichtung einer neuen Funktionalität eine Startsequenz (106) sendet, die eine Information zur Identifikation des Endgerätes (10, 11) beinhaltet.

16. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß die Speichereinrichtung (20) und/oder die Prozessoreinheit (12) zumindest teilweise auf einem tragbaren Datenräger (80) ausgebildet sind.

17. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß die Startsequenz (106) eine Information über die Art der ausgelösten Transaktion beinhaltet.

18. Endgerät nach Anspruch 9, dadurch **gekennzeichnet,** daß es nach dem Auslösen einer Transaktion alle dazu in der Speichereinrichtung (20) bereits in Form von Daten vorhandenen und ausführbaren Programmbefehle ausführt und ggf. resultierende Zwischenergebnisse der Startsequenz (106) beifügt.

19. Verfahren zur Ausführung einer Transaktion unter Verwendung eines Endgerätes, das über ein Endgerätenetz mit einem in die Transaktionsausführung eingebunden Knotenrechner verbunden ist,
mit folgenden Schritten:

- Auslösen einer Transaktion mittels des Endgerätes (10, 11),
- Übertragen einer die Transaktion bezeichnenden Startsequenz 106) vom Endgerät (10, 11) an den Knotenrechner (40, 41),
- Rückübertragen von Daten, welche im Endgerät (10, 11) die zur Ausführung der Transaktion benötigte Funktionalität herstellen, vom Knotenrechner (40, 41) an das Endgerät (10, 11).

20. Verfahren nach Anspruch 19, dadurch **gekennzeichnet,** daß das Endgerät (10, 11) nach Auslösen einer Transaktion prüft, inwieweit die bereits in der Speichereinrichtung (20) vorhanden Daten eine Ausführung der Trans-

aktion ermöglichen und die Transaktion, soweit möglich, unmittelbar ausführt (104).

21. Verfahren zum Betrieb eines zur Ausführung einer Transaktion geeigneten Endgerätes, das über ein Endgerätenetz mit einem in die Transaktionsausführung eingebunden Knotenrechner verbunden ist, wobei zur Ausführung einer Transaktion wenigstens eine Funktionalität benötigt wird, mit folgenden Schritten:

- Überwachen des Endgerätes (10, 11) auf Eintritt eines vorbestimmten Ereignisses,
- bei Eintritt eines vorbestimmten Ereignisses Übertragen einer eine Transaktion bezeichnenden Startsequenz (106) vom Endgerät (10, 11) an den Knotenrechner (40, 41),
- Rückübertragen von Daten, welche im Endgerät (10,11) mindestens eine zur Ausführung der Transaktion benötigte Funktionalität herstellen, vom Knotenrechner (40, 41) an das Endgerät (10,11).

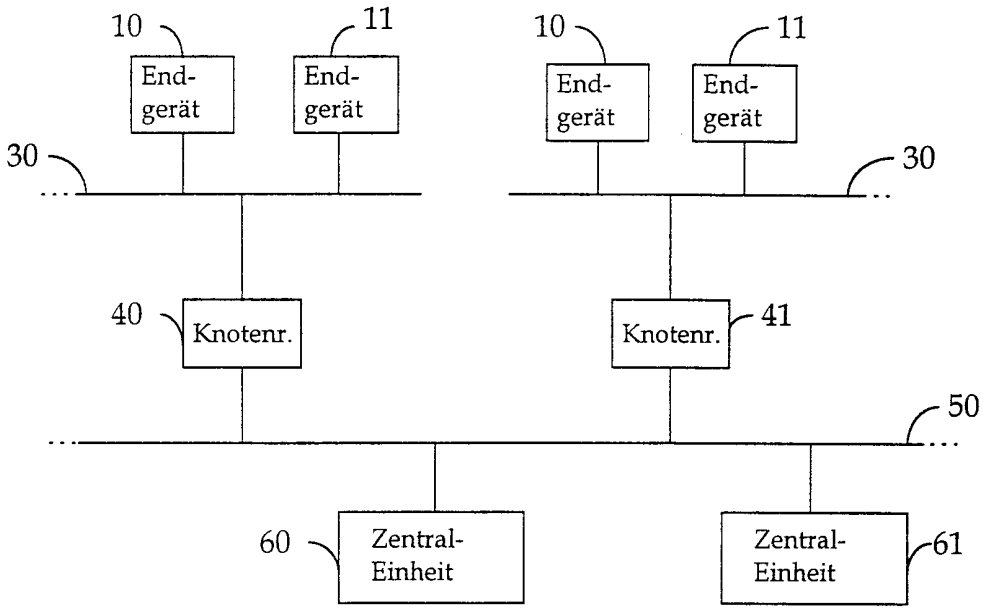
10
End-gerät
11
End-gerät
10
End-gerät
11
End-gerät
30
30
40
Knotenr.
Knotenr.
41
50
60
Zentral-Einheit
Zentral-Einheit
61

Fig. 1

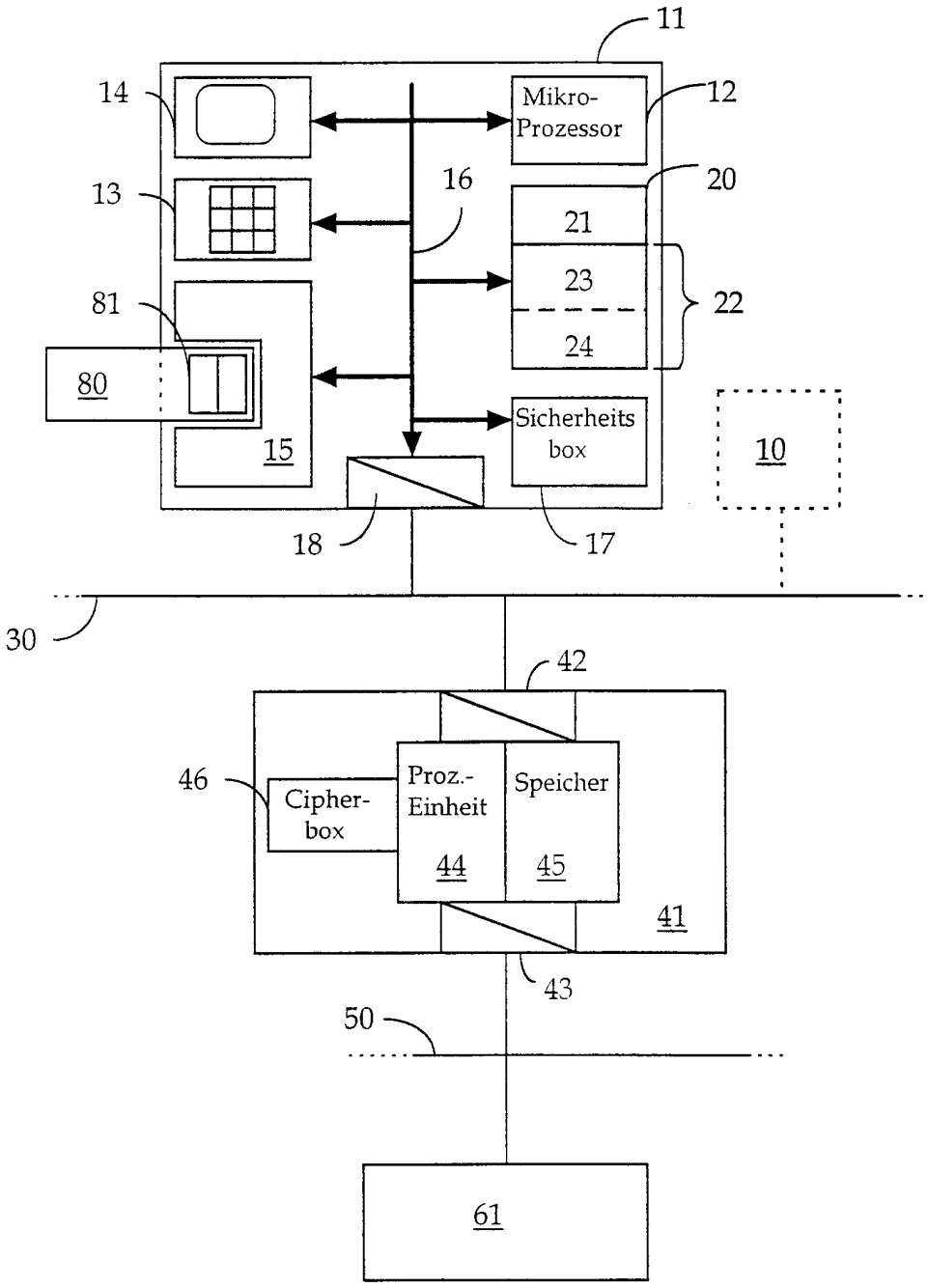
11
14
Mikro-
Prozessor
12
16
20
13
21
23
22
24
81
80
15
Sicherheits
box
10
18
17
30
42
46
Cipher-
box
Proz.-
Einheit
Speicher
44
45
41
43
50
61

Fig. 2

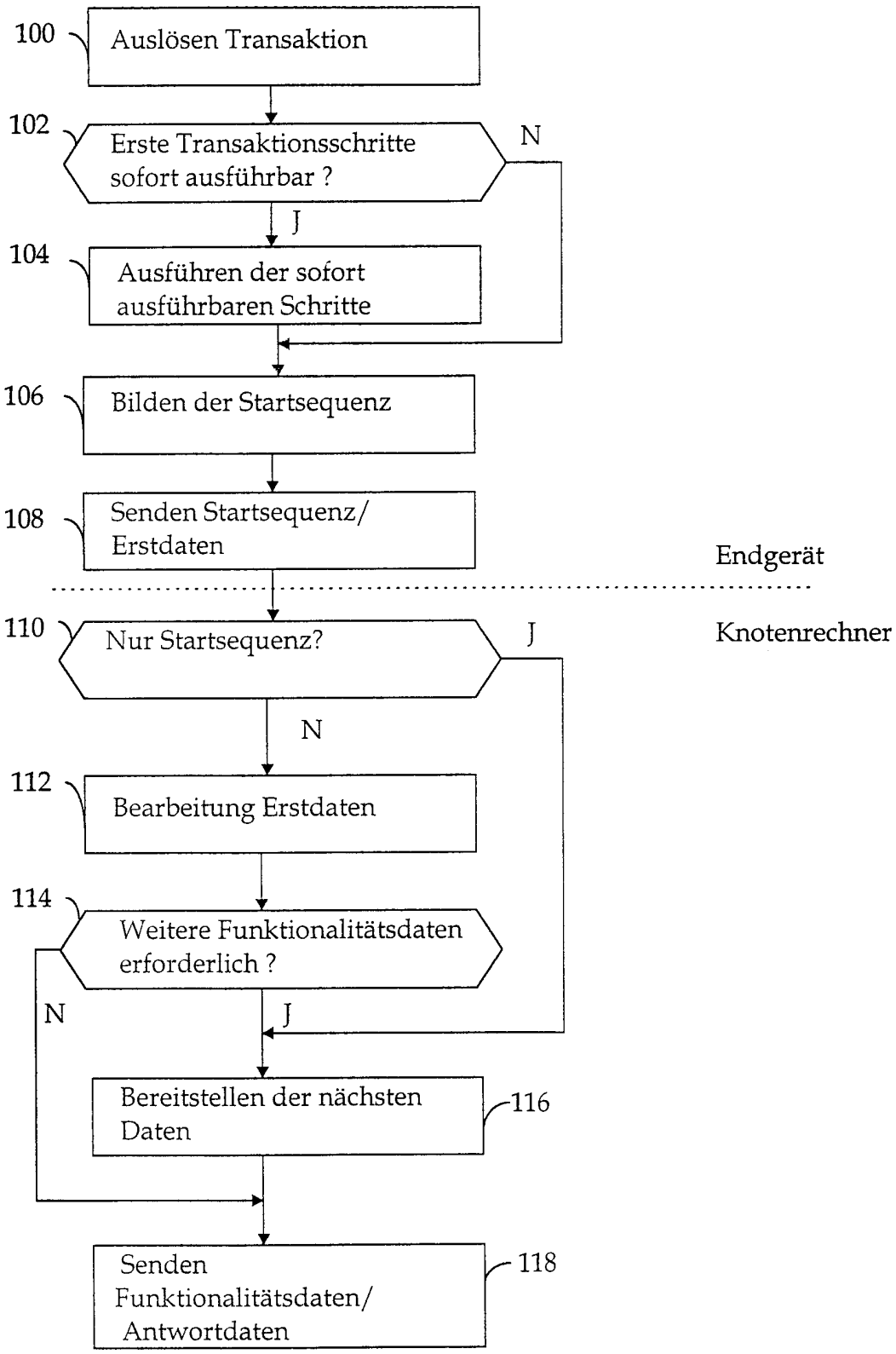
100
Auslösen Transaktion
102
Erste Transaktionsschritte sofort ausführbar ?
N
J
104
Ausführen der sofort ausführbaren Schritte
106
Bilden der Startsequenz
108
Senden Startsequenz/ Erstdaten
Endgerät
Knotenrechner
110
Nur Startsequenz?
J
N
112
Bearbeitung Erstdaten
114
Weitere Funktionalitätsdaten erforderlich ?
N
J
Bereitstellen der nächsten Daten
116
Senden Funktionalitätsdaten/ Antwortdaten
118

Fig. 3

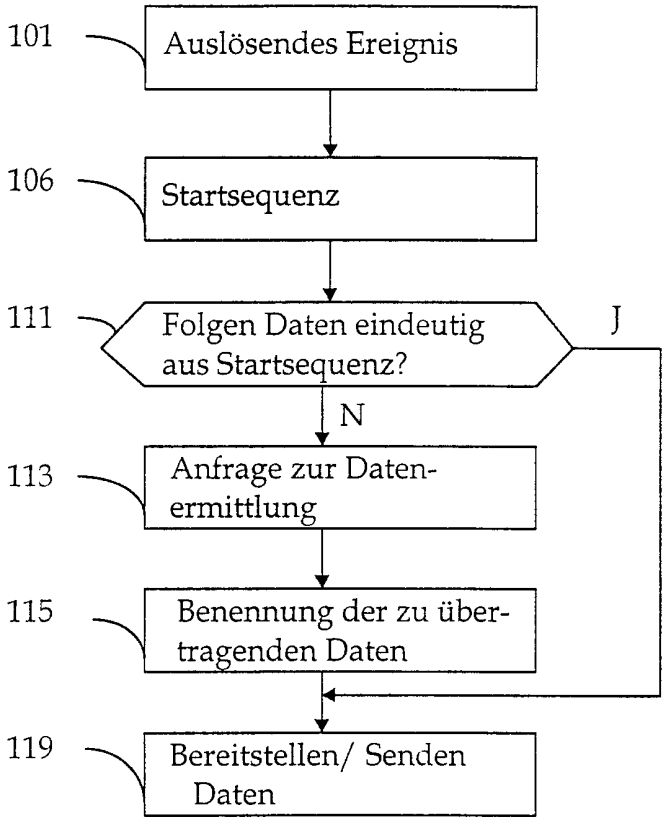
101
Auslösendes Ereignis
106
Startsequenz
111
Folgen Daten eindeutig aus Startsequenz?
J
N
113
Anfrage zur Daten-ermittlung
115
Benennung der zu über-tragenden Daten
119
Bereitstellen/ Senden Daten

Fig. 4

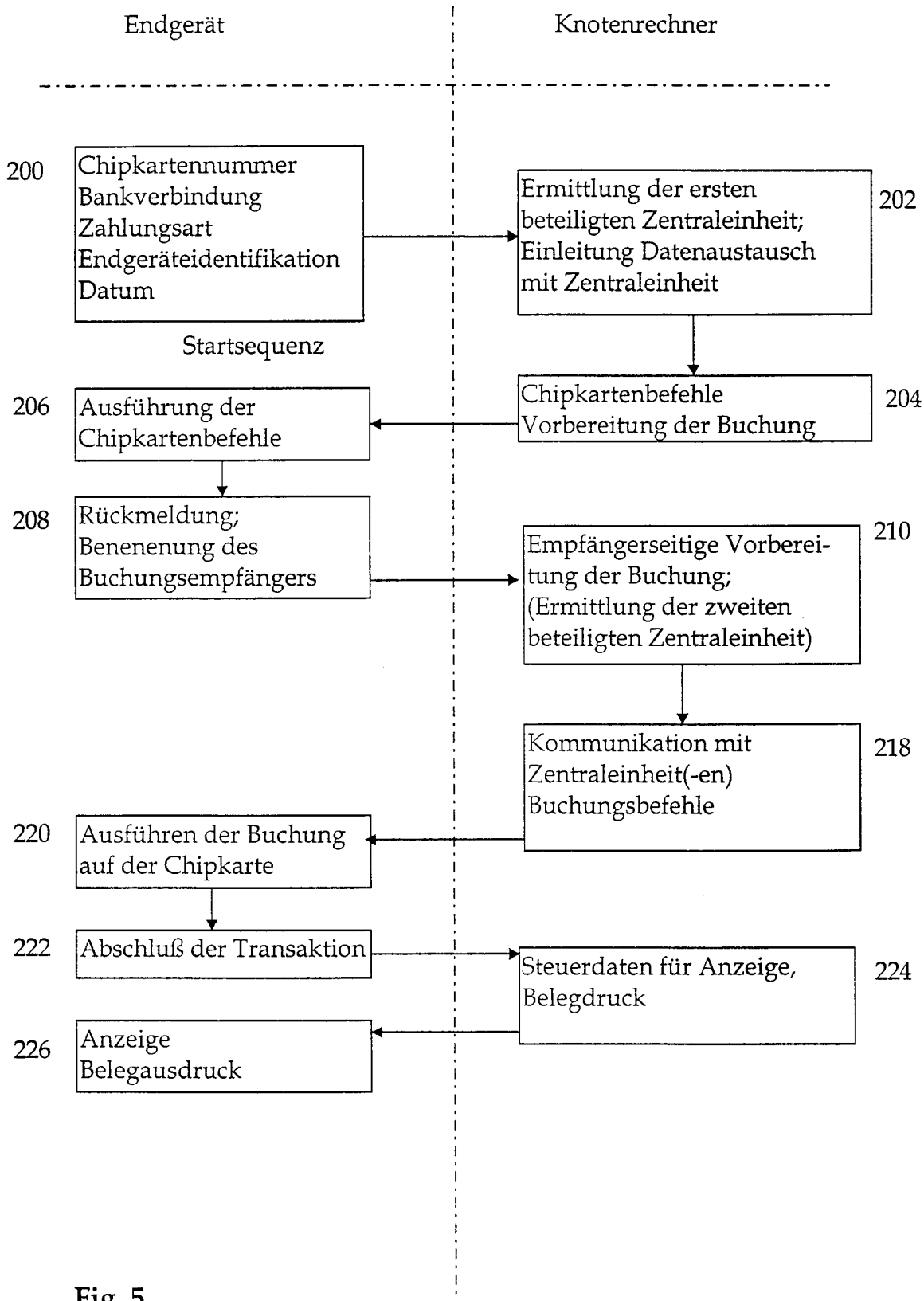
Endgerät
Knotenrechner
200
Chipkartennummer
Bankverbindung
Zahlungsart
Endgeräteidentifikation
Datum
Startsequenz
Ermittlung der ersten beteiligten Zentraleinheit; Einleitung Datenaustausch mit Zentraleinheit
202
Chipkartenbefehle Vorbereitung der Buchung
204
206
Ausführung der Chipkartenbefehle
208
Rückmeldung; Benenenung des Buchungsempfängers
Empfängerseitige Vorbereitung der Buchung; (Ermittlung der zweiten beteiligten Zentraleinheit)
210
Kommunikation mit Zentraleinheit(-en) Buchungsbefehle
218
220
Ausführen der Buchung auf der Chipkarte
222
Abschluß der Transaktion
Steuerdaten für Anzeige, Belegdruck
224
226
Anzeige Belegausdruck

Fig. 5

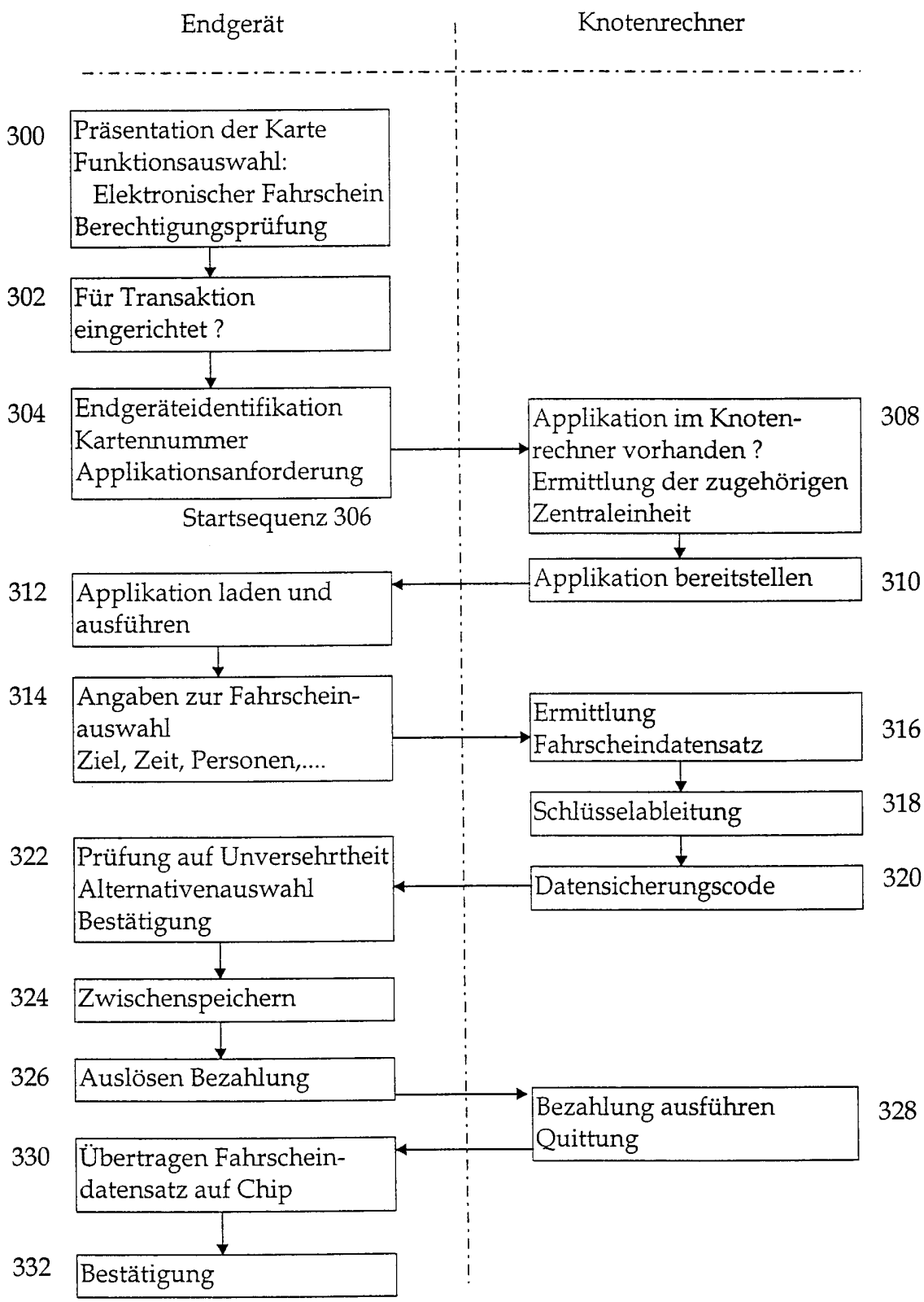
Endgerät
Knotenrechner
300
Präsentation der Karte
Funktionsauswahl:
Elektronischer Fahrschein
Berechtigungsprüfung
302
Für Transaktion eingerichtet ?
304
Endgeräteidentifikation
Kartennummer
Applikationsanforderung
Startsequenz 306
308
Applikation im Knoten-rechner vorhanden ?
Ermittlung der zugehörigen Zentraleinheit
310
Applikation bereitstellen
312
Applikation laden und ausführen
314
Angaben zur Fahrschein-auswahl
Ziel, Zeit, Personen,....
316
Ermittlung Fahrscheindatensatz
318
Schlüsselableitung
320
Datensicherungscode
322
Prüfung auf Unversehrtheit
Alternativenauswahl
Bestätigung
324
Zwischenspeichern
326
Auslösen Bezahlung
328
Bezahlung ausführen
Quittung
330
Übertragen Fahrschein-datensatz auf Chip
332
Bestätigung

Fig. 6

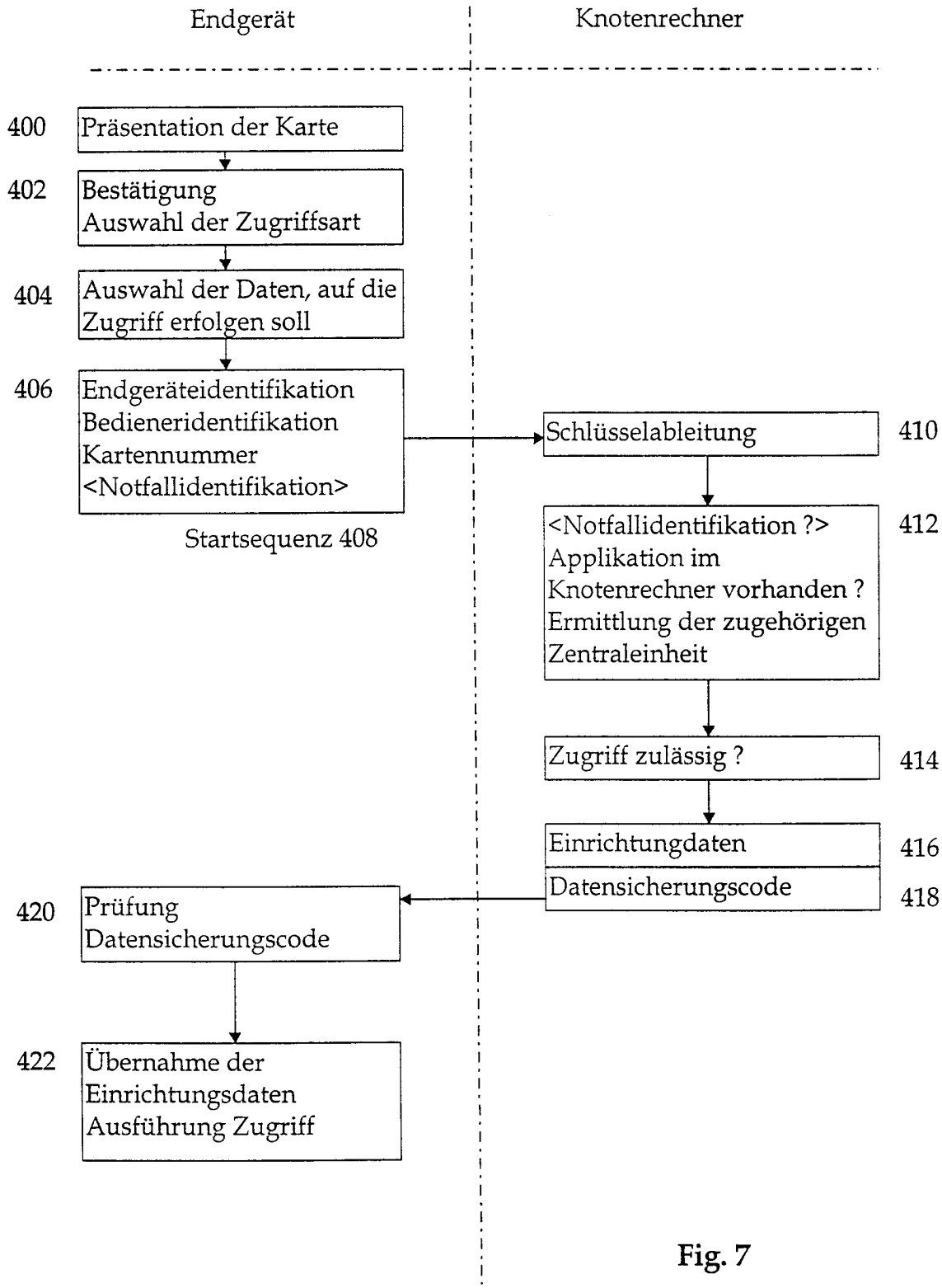
Endgerät
Knotenrechner
400
Präsentation der Karte
402
Bestätigung
Auswahl der Zugriffsart
404
Auswahl der Daten, auf die Zugriff erfolgen soll
406
Endgeräteidentifikation
Bedieneridentifikation
Kartennummer
<Notfallidentifikation>
Startsequenz 408
Schlüsselableitung
410
<Notfallidentifikation ?>
Applikation im Knotenrechner vorhanden ?
Ermittlung der zugehörigen Zentraleinheit
412
Zugriff zulässig ?
414
Einrichtungdaten
416
Datensicherungscode
418
420
Prüfung
Datensicherungscode
422
Übernahme der Einrichtungsdaten
Ausführung Zugriff

Fig. 7