(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 20 342 T2** 2005.10.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 973 136 B1**
(21) Deutsches Aktenzeichen: **699 20 342.2**
(96) Europäisches Aktenzeichen: **99 305 639.9**
(96) Europäischer Anmeldetag: **15.07.1999**
(97) Erstveröffentlichung durch das EPA: **19.01.2000**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **22.09.2004**
(47) Veröffentlichungstag im Patentblatt: **06.10.2005**

(51) Int Cl.[7]: **G07F 7/10**
G06F 12/14, G06F 1/00

(30) Unionspriorität:
20149898 16.07.1998 JP

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Sony Corp., Tokio/Tokyo, JP

(74) Vertreter:
Mitscherlich & Partner, Patent- und Rechtsanwälte, 80331 München

(72) Erfinder:
Kusakabe, Susumu, Shinagawa-ku, Tokyo 141, JP; Takada, Masayuki, Shinagawa-ku, Tokyo 141, JP; Sasaki, Masachika, Shinagawa-ku, Tokyo 141, JP

(54) Bezeichnung: **Datenspeichervorrichtung und -verfahren**

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Datenspeichervorrichtung und ein Datenspeicherverfahren.

[0002] Es ist bekannt, dass zum Beispiel eine IC(integrierte Schaltungs)-Karte (Chip-Karte) entwickelt worden ist, bei der erwartet wird, dass sie bei einem elektronischen Geldsystem, einem Sicherheitssystem usw. benutzt wird.

[0003] Die IC-Karte weist eine CPU (Zentraleinheit) zur Durchführung verschiedener Verarbeitungsarten und einen Speicher zum Speichern von zur Verarbeitung notwendigen Daten auf, und eine Datenübertragung zu/ein Datenempfang von der IC-Karte werden ausgeführt, während sie mit einem vorbestimmten Leser/Schreiber (R/W (reader/writer)) oder in einem berührungs- bzw. kontaktlosen Zustand durch Benutzung einer elektromagnetischen Welle elektrisch verbunden ist. Einer IC-Karte, die eine Datenübertragung/einen Datenempfang mit einem R/W in einem kontaktlosen Zustand durch Benutzung einer elektromagnetischen Welle ausführt, wird generell elektrische Energie durch die elektromagnetische Welle zugeführt.

[0004] Beispielsweise ist in ISO7816 (ISO = International Organisation for Standardization (internationale Organisation für Standardisierung)) der Standard von Kontakttyp-IC-Karten definiert. Gemäß diesem Standard kann die Datenverwaltung bzw. das Datenverwalten auf der Basis von beispielsweise einer (mit einer sogenannten Datei korrespondierenden) EF (Elementary File (elementare Kartei)) zum Speichern von Daten und einer DF zum Speichern der EF und der (mit einem sogenannten Adressbuch bzw. Verzeichnis (Ordner) korrespondierenden) DF (Dedicated File (dedizierte Datei)) ausgeführt werden. Demgemäss ist die auf der Schichtstruktur basierende Datenverwaltung durch Setzen einer gewissen DF als eine Eltern- bzw. Vaterschicht und Bereitstellen einer DF einer Kindschicht dafür möglich.

[0005] Wenn IC-Karten für die Dienstversorgung bzw. -zufuhr durch mehrere Manager bzw. Verwalter benutzt werden, kann ein Verfahren zur Zuordnung einer DF als eine Schicht zu jedem der mehreren Verwalter und Speicherung einer EF als für die Dienstzufuhr jedes Verwalters in der DF zuzuführende Daten in Betracht gezogen werden.

[0006] Jedoch ist es bei ISO7816 usw. schwierig, die benutzbare Kapazität und die Ressourcen der IC-Karte solcher Identifikationscodes zur Identifizierung einer (mit einem Dateinamen und einem Verzeichnisnamen korrespondierenden) DF und EF bei jeder DF zu beschränken.

[0007] Deshalb ist es schwierig zu verhindern, dass ein Identifikationscode zwischen unterschiedlichen Verwaltern dupliziert wird, und es ist auch schwierig, einem Verwalter zu verbieten, dass er einen in einer IC-Karte enthaltenen Speicher mit einer Kapazität benutzt, die eine durch einen Vertrag oder dgl. bestimmte vorbestimmte Kapazität überschreitet.

[0008] Außerdem sind in dem Fall, dass IC-Karten in einem elektronischen Geldsystem oder Sicherheitssystem benutzt werden, Sicherheiten wie die Geheimhaltung von Daten, die Verhinderung einer Fälschung von IC-Karten usw. wichtig, und beispielsweise bei ISO 7816 wird ein Zugriff auf eine DF und eine zur DF gehörende EF durch Sperren der DF beschränkt. Das heißt, bei ISO7816 ist es für einen Zugriff auf eine gewisse DF notwendig, alle sich über die betreffende DF erstreckenden DF-Schlüssel oberer Schichten (Vaterschichten) auf dem Bus zu kennen.

[0009] Wenn deshalb beispielsweise ein gewisser als Vaterverwalter dienender Verwalter einen Teil von ihm zugeordneten Ressourcen einem als Kindverwalter dienenden anderen Verwalter zuteilt und die vom Kindverwalter verwaltete DF in der vom Vaterverwalter verwalteten DF ausgebildet ist, damit der Kindverwalter auf seine DF zugreifen kann, muss der Kindverwalter einen Schlüssel zum Zugriff auf die DF der Vaterschicht, das heißt die DF des Vaterverwalters kennen, und da tritt ein Problem bei der Sicherheit auf.

[0010] Aus dem Dokument US-A-5410598 gehen die Merkmale des Oberbegriffs der Ansprüche 1, 11 hervor.

[0011] Gemäß einem ersten Aspekt der Erfindung ist eine Datenspeichervorrichtung zur Speicherung von Daten zum Zuführen eines vorbestimmten Dienstes bereitgestellt, die dadurch gekennzeichnet ist, dass sie aufweist: eine Datenspeichereinrichtung zur Speicherung der Daten, eine Management- bzw. Verwaltungseinrichtung zum Managen bzw. Verwalten eines Speicherbereichs der Datenspeichereinrichtung während eines Setzens des Speicherbereichs in eine geschichtete Struktur, eine Schichtschlüssel-Speichereinrichtung zur Speicherung eines Schichtschlüssels für jede Schicht des Speicherbereichs der Datenspeichereinrichtung, eine Datenspeicherbereichschlüssel-Speichereinrichtung zur Speicherung eines Datenspeicherbereichschlüssels für den Speicherbereich, in welchem die Daten gespeichert sind, wobei das Verfahren aufweist: einen Erzeugungsschritt zur Erzeugung eines oder mehrerer zu einer Zertifizierung zum Zugriff auf den Speicherbereich durch Benutzung zweier oder mehrerer Schichtschlüssel oder Datenspeicherbereichsschlüssel benutzter Zertifizierungsschlüssel, und eine Zertifizierungseinrichtung zur Ausführung einer Zertifizierung auf der Basis des Zertifizierungsschlüs-

sels.

[0012] Gemäß einem zweiten Aspekt der Erfindung ist ein Datenspeicherverfahren für eine Datenspeichervorrichtung zur Speicherung von Daten und Zuführen eines vorbestimmten Dienstes bereitgestellt, das dadurch gekennzeichnet ist, dass die Datenspeichervorrichtung aufweist: eine Speichereinrichtung zur Speicherung von Daten, eine Management- bzw. Verwaltungseinrichtung zum Managen bzw. Verwalten eines Speicherbereichs der Datenspeichervorrichtung während eines Setzens des Speicherbereichs in eine Schichtstruktur, eine Schichtschlüssel-Speichereinrichtung zur Speicherung eines Schichtschlüssels für jede Schicht des Speicherbereichs der Datenspeichervorrichtung und eine Datenspeicherbereichsschlüssel-Speichereinrichtung zur Speicherung eines Datenspeicherbereichsschlüssels für den Speicherbereich, in welchen die Daten gespeichert sind, wobei das Verfahren aufweist: einen Erzeugungsschritt zur Erzeugung eines oder mehrerer zur Zertifizierung für einen Zugriff auf den Speicherbereich durch Verwendung zweier oder mehrerer Schichtschlüssel oder Datenspeicherbereichsschlüssel benutzter Zertifizierungsschlüssel, und einen Zertifizierungsschritt zur Ausführung einer Zertifizierung auf der Basis des Zertifizierungsschlüssels.

[0013] Ausführungsformen der vorliegenden Erfindung betreffen eine Datenspeichervorrichtung und ein Datenspeicherverfahren, die Ressourcen von IC-Karten verwalten und eine Zugriffssteuerung zu IC-Karten mit hoher Flexibilität und Sicherheit in dem Fall, dass mehrere Verwalter ihre Dienste unter Benutzung einer IC-Karte (IC = Integrated Circuit (integrierte Schaltung)) zuführen, ausführen können.

[0014] Andere Ausführungsformen der vorliegenden Erfindung ermöglichen ein Ressourcenverwaltung zum Speichern von Daten und eine Zugriffssteuerung, die eine hohe Flexibilität und Sicherheit bei Daten aufweisen.

[0015] Für ein besseres Verständnis der vorliegenden Erfindung wird nun mittels eines Beispiels auf die beigefügten Zeichnungen Bezug genommen, in denen:

[0016] Fig. 1 ein Blockdiagramm ist, das die Ausbildung eines eine IC-Karte entsprechend einer Ausführungsform der vorliegenden Erfindung benutzenden Kartensystems zeigt;

[0017] Fig. 2 ein Blockdiagramm ist, das die Ausbildung eines Lesers/Schreibers **1** der Fig. 1 zeigt;

[0018] Fig. 3 ein Blockdiagramm ist, das die Ausbildung einer IC-Karte **2** der Fig. 1 zeigt;

[0019] Fig. 4 ein Diagramm ist, das ein logisches Format eines EEPROM **66** der Fig. 3 zeigt;

[0020] Fig. 5 ein Diagramm ist, welches die Verzeichnisstruktur des EEPROM **66** der Fig. 3 zeigt;

[0021] Fig. 6 ein Diagramm ist, das einen Prozess zur Bildung der Schichtstruktur der Fig. 5 zeigt;

[0022] Fig. 7 ein Flussdiagramm ist, das eine Bereich bildende Verarbeitung zeigt;

[0023] Fig. 8 ein Flussdiagramm ist, das eine Dienst bildende Verarbeitung zeigt;

[0024] Fig. 9 ein Diagramm ist, das einen Schlüsselempfang/eine Schlüsselabgabe zwischen Verwaltern zeigt;

[0025] Fig. 10 ein Diagramm ist, das Information zeigt, die notwendig ist, wenn ein Verwalter A Dienste zuführt;

[0026] Fig. 11 ein Diagramm ist, das die Verarbeitung der IC-Karte **2** zeigt, wenn der Verwalter A Dienste zuführt;

[0027] Fig. 12 ein Diagramm ist, das ein Zertifizierungsverfahren der IC-Karte **2** durch ein Dienstzuführgerät **111** zeigt;

[0028] Fig. 13 ein Diagramm ist, welches das Zertifizierungsverfahren des Dienstzufuhrgeräts **111** durch die IC-Karte **2** zeigt;

[0029] Fig. 14 ein Diagramm ist, das Information zeigt, die notwendig ist, wenn ein Verwalter B2 Dienste zuführt;

[0030] Fig. 15 ein Diagramm ist, das die Verarbeitung der IC-Karte **2** zeigt, wenn der Verwalter B2 Dienste zuführt;

[0031] Fig. 16 ein Diagramm ist, das Information zeigt, die notwendig ist, wenn ein Verwalter C Dienste zuführt;

[0032] Fig. 17 ein Diagramm ist, das die Verarbeitung der IC-Karte **2** zeigt, wenn der Verwalter C Dienste zuführt;

[0033] Fig. 18 ein Diagramm ist, das Information zeigt, die notwendig ist, wenn der Verwalter C Dienste zuführt;

[0034] Fig. 19 ein Diagramm ist, das die Verarbeitung der IC-Karte **2** zeigt, wenn der Verwalter C Dienste zuführt;

[0035] Fig. 20 ein Diagramm ist, das ein Verfahren

zur Erzeugung eines ersten Zugriffsschlüssels und eines zweiten Zugriffsschlüssels zeigt, die zu einer gegenseitigen Zertifizierung benutzt werden;

[0036] Fig. 21 ein Diagramm ist, das die Schichtstruktur des EEPROM **66** zeigt;

[0037] Fig. 22 ein Diagramm ist, das einen/eine Schlüssel-Empfang/Abgabe zwischen Verwaltern zeigt;

[0038] Fig. 23 ein Diagramm ist, das einen gemeinsamen Gebrauch von Diensten (Daten) zwischen Verwaltern zeigt;

[0039] Fig. 24 ein Diagramm ist, das die Schichtstruktur des EEPROM **66** zeigt; und

[0040] Fig. 25 ein Diagramm ist, das einen Schlüsselempfang/eine Schlüsselabgabe zwischen Verwaltern zeigt.

[0041] Bevorzugte Ausführungsformen gemäß der vorliegenden Erfindung werden nachstehend unter Bezugnahme auf die beigefügten Zeichnungen beschrieben.

[0042] Fig. 1 zeigt die Ausbildung eines kontaktlosen Kartensystems gemäß einer Ausführungsform der vorliegenden Erfindung (das System bedeutet eine logische Zusammenfügung mehrerer Vorrichtungen, und es hängt nicht davon ab, ob die jeweiligen Vorrichtungen im gleichen Gehäuse lokalisiert sind oder nicht).

[0043] Das kontaktlose Kartensystem weist einen R/W **1**, eine IC-Karte **2** und einen Kontroller **3** auf, und eine Datenübertragung/ein Datenempfang wird zwischen dem R/W **1** und der IC-Karte **2** in einem kontaktlosen Zustand unter Benutzung einer elektromagnetischen Welle ausgeführt.

[0044] Das heißt, der R/W **1** überträgt einen vorbestimmten Befehl zur IC-Karte **2**, und die IC-Karte **2** empfängt den Befehl, um die mit dem Befehl korrespondierende Verarbeitung auszuführen. Die IC-Karte **2** überträgt die mit dem Verarbeitungsresultat korrespondierenden Reaktions- bzw. Antwortdaten zum R/W **1**.

[0045] Der R/W **1** ist durch eine vorbestimmte (mit dem Standard von RS-485A oder dgl. in Einklang stehende) Schnittstelle mit dem Kontroller **3** verbunden, und der Kontroller **3** führt dem R/W **1** ein vorbestimmtes Steuersignal zu, so dass der R/W **1** eine vorbestimmte Verarbeitung ausführt.

[0046] Fig. 2 zeigt die Ausbildung des R/W **1** der Fig. 1.

[0047] In der IC **21** sind eine DPU (Data Processing Unit (Datenverarbeitungseinheit)) **31** zur Ausführung einer Datenverarbeitung, eine SPU (Signal Processing Unit (Signalverarbeitungseinheit)) **32** zur Verarbeitung von zur IC-Karte **2** zu übertragenden Daten und von der IC-Karte **2** empfangenen Daten, ein SCC (Serial communication Controller (Seriellkommunikationskontroller)) **33**, der mit dem Kontroller **3** kommuniziert, und eine Speichereinheit **34**, die einen ROM-Abschnitt **41** zum vorausgehenden Speichern von zum Verarbeiten von Daten erforderlicher Information und einen RAM-Abschnitt **42** zum zeitweiligen bzw. temporären Speichern von Daten während der Verarbeitung aufweist, durch einen Bus miteinander verbunden.

[0048] Außerdem ist auch ein Flash-Speicher **22** zum Speichern vorbestimmter Daten mit dem Bus verbunden.

[0049] Die DPU **31** gibt an die SPU **32** einen zur IC-Karte **2** zu übertragenden Befehl aus und empfängt von der SPU **32** Reaktions- bzw. Antwortdaten, die von der IC-Karte **2** empfangen werden.

[0050] Nach einer vorbestimmten Verarbeitung (beispielsweise BPSK (BiPhase Shift Keying (Zweiphasenumtastung bzw. -modulation)) wird bezüglich des zur IC-Karte **2** zu übertragenden Befehls eine Modulation (Codierung in einen Manchester-Code oder dgl.) ausgeführt, die SPU **32** gibt ihn an eine Modulationsschaltung **23** aus, und sie empfängt auch von einer Demodulationsschaltung **25** die von der IC-Karte **2** übertragenen Antwortdaten zum Ausführen einer vorbestimmten Verarbeitung bezüglich der Daten.

[0051] Die Modulationsschaltung **23** führt eine ASK-Modulation (ASK = Amplitude Shift Keying (Amplitudenumtastung)) bezüglich einer Trägerwelle, die eine vorbestimmte Frequenz (beispielsweise 13,56 MHz) aufweist und von einem Oszillator (OSZ) **26** auf der Basis von aus der SPU **32** zugeführten Daten zugeführt wird, aus und gibt die so erzeugte Modulationswelle durch eine Antenne **27** als eine elektromagnetische Welle an die IC-Karte **2** aus. Zu dieser Zeit ist die Modulationsschaltung **23** so eingestellt, dass der Modulationsfaktor auf kleiner als 1 eingestellt ist und die ASK-Modulation ausgeführt wird, wodurch verhindert wird, dass die maximale Amplitude der Modulationswelle auch bei einem niedrigen Pegel der Daten auf null reduziert wird.

[0052] Die Demodulationsschaltung **25** demoduliert die durch die Antenne **27** empfangene Modulationswelle (ASK-modulierte Welle) und gibt die so modulierten Daten an die SPU **32** aus.

[0053] Fig. 3 zeigt die Ausbildung der IC-Karte **2** der Fig. 1.

[0054] In der IC-Karte **2** empfängt die IC **51** die vom R/W **1** übertragene Modulationswelle durch die Antenne **53**. Ein Kondensator **52** bildet zusammen mit der Antenne **53** eine LC-Schaltung, und sie ist so ausgebildet, dass sie mit der eine vorbestimmte Frequenz (Trägerfrequenz) aufweisenden elektromagnetischen Welle abgestimmt (oszilliert) wird.

[0055] In der IC **51** detektiert und demoduliert eine HF- bzw. RF-Schnittstelleneinheit **61** (Kommunikationseinrichtung) die durch die Antenne **53** empfangene Modulationswelle (ASK-modulierte Welle) mit einem ASK-Demodulator **81** und gibt die so demodulierten Daten an eine BPSK-Demodulationsschaltung **62** und eine PLL-Einheit **63** (PLL = Phase Locked Loop (Phasenregelschaltung)) aus. Außerdem stabilisiert sie das im ASK-Demodulator **81** detektierte Signal durch einen Spannungsregler **82** und führt es jeder Schaltung als eine Gleichsignal- bzw. DC-Leistung zu.

[0056] Die RF-Schnittstelleneinheit **61** oszilliert ein die gleiche Frequenz wie die Taktfrequenz der Daten aufweisendes Signal in einer Oszillationsschaltung **83** und gibt das Signal an die PLL-Einheit **63** aus.

[0057] In der RF-Schnittstelleneinheit **61** wird die als die Energiequelle der IC-Karte **2** dienende Last der Antenne **53** in Verbindung mit Daten, die dem ASK-Modulator **81** bzw. **84** von der Operationseinheit **64** durch die BPSK-Modulationsschaltung **68** zugeführt werden, variiert (beispielsweise wird ein vorgeschriebenes Schaltelement in Verbindung mit den Daten ein-/ausgeschaltet, und nur wenn das Schaltelement eingeschaltet ist, wird eine vorbestimmte Last parallel mit der Antenne **53** verbunden), wodurch die durch die Antenne **53** empfangene Modulationswelle einer ASK-Modulation unterworfen wird (wenn die Daten von der IC-Karte **2** übertragen werden (die IC-Karte **2** ist so ausgebildet, dass sie Daten überträgt), setzt der R/W **1** die maximale Amplitude der von ihm ausgegebenen Modulationswelle auf einen festen Wert, und diese Modulationswelle wird auf der Basis der Variation der Last der Antenne **53** der ASK-Modulation unterworfen), und sie überträgt ihre Modulationskomponente durch die Antenne **53** zum R/W **1** (variiert die Endspannung der Antenne **27** des R/W **1**).

[0058] Auf der Basis der vom ASK-Demodulator **81** zugeführten Daten erzeugt die PLL-Einheit **63** ein mit den Daten synchrones Taktsignal und gibt das Taktsignal an die BPSK-Demodulationsschaltung **62** und die BPSK-Modulationsschaltung **68** aus.

[0059] Wenn die im ASK-Demodulator **81** demodulierten Daten BPSK-moduliert werden, demoduliert die BPSK-Demodulationsschaltung **62** die Daten (decodiert den Manchester-Code) entsprechend dem von der PLL-Einheit **63** zugeführten Taktsignal und gibt die so demodulierten Daten an die Operationseinheit **64** aus.

[0060] Wenn die von der BPSK-Demodulationsschaltung **62** zugeführten Daten verschlüsselt werden, decodiert die Operationseinheit **64** die Daten in einer Verschlüsselungs/Decodierungs-Einheit **92** und verarbeitet dann die Daten in einem Sequenzer **91**. Wenn die Daten nicht verschlüsselt werden, werden die von der BPSK-Demodulationsschaltung **62** zugeführten Daten direkt dem Sequenzer **91** zugeführt, wobei sie nicht durch die Verschlüsselungs/Decodierungs-Einheit **92** gehen.

[0061] Der Sequenzer **91** (Verwaltungeinrichtung) (Erzeugungseinrichtung) (Zertifizierungseinrichtung) ist so ausgebildet, dass er die Verarbeitung entsprechend Daten wie ein ihm zuzuführender Befehl ausführt. Das heißt beispielsweise, dass der Sequenzer **91** eine Datenschreib- und -leseoperation in den/vom EEPROM **6** und andere notwendige Operationsverarbeitung ausführt. Außerdem führt der Sequenzer **91** eine Zugriffssteuerung zum EEPROM **66** auf der Basis einer Zertifizierung aus und verwaltet bzw. managt auch den EEPROM **66**.

[0062] Ein Paritätsoperator **93** der Operationseinheit **64** berechnet auf der Basis der im EEPROM **66** gespeicherten Daten einen Reed-Solomon-Code als Parität.

[0063] Nachdem die Operationseinheit **64** die vorbestimmte Verarbeitung im Sequenzer **91** ausgeführt hat, gibt sie die mit der Verarbeitung korrespondierenden Antwortdaten (die zum R/W **1** zu übertragenden Daten) an die BPSK-Modulationsschaltung **68** aus.

[0064] Die BPSK-Modulationsschaltung **68** unterwirft die von der Operationseinheit **64** zugeführten Daten einer BPSK-Modulation und gibt die so modulierten Daten an den ASK-Modulator der RF-Schnittstelleneinheit **61** aus.

[0065] Ein ROM (Reed Only Memory (Nurlesespeicher)) **65** speichert ein Programm, mit welchem der Sequenzer **91** seine Verarbeitung ausführt, und andere notwendige Daten. Ein RAM **67** speichert im Lauf der Verarbeitung des Sequenzers **91** Daten und dgl. vorübergehend.

[0066] Der EEPROM (Electrically Erasable and Programmable ROM (elektrisch löschbarer und programmierbarer ROM)) **66** (Speichereinrichtung) (Datenspeichereinrichtung) ist ein nicht flüchtiger Speicher, und er fährt fort, Daten zu speichern, auch wenn die IC-Karte die Kommunikation mit dem R/W **1** beendet und die Energieversorgung gestoppt wird.

[0067] Als nächstes wird die Daten-Übertra-

gungs/Empfangs-Verarbeitung zwischen dem R/W **1** und der IC-Karte **2** beschrieben.

[0068] Der R/W **1** (Fig. 2) strahlt von der Antenne **27** eine vorbestimmte elektromagnetische Welle ab, überwacht den Lastzustand der Antenne **27** und wartet, bis die Variation des Lastzustandes aufgrund der Näherung der IC-Karte **2** detektiert wird. Der R/W **1** kann eine Verarbeitung (Abrufen) ausführen, bei der die auf der Basis von Daten eines vorbestimmten kurzen Musters ASK-modulierte elektromagnetische Welle abgestrahlt wird, um die IC-Karte **2** zu rufen, bis innerhalb einer festen Zeit von der IC-Karte **2** eine Antwort erhalten wird.

[0069] Wenn die Annäherung der IC-Karte **2** im R/W **1** detektiert wird, macht die SPU **32** des R/W **1** eine Rechteckwelle einer vorbestimmten Frequenz (beispielsweise eine Frequenz, die zweimal so hoch wie die Taktfrequenz der Daten ist) als eine Trägerwelle dienstbar, führt an ihr auf der Basis der zur IC-Karte **2** zu übertragenden Daten (der mit der von der IC-Karte **2** auszuführenden Verarbeitung korrespondierende Befehl, in die IC-Karte **2** zu schreibende Einschreibedaten usw.) eine BPSK-Modulation aus und gibt die so (Manchester-Code) erzeugte Modulationswelle (BPSK-Modulationssignal) an die Modulationsschaltung **23** aus.

[0070] Bei der BPSK-Modulationsverarbeitung können die Daten durch Verwendung einer differentiellen Umsetzung der Variation der Phase der Modulationswelle zugeordnet werden, und in diesem Fall kann das BPSK-Modulationssignal in die originalen Daten demoduliert werden, auch wenn sie invertiert sind. Deshalb ist es nicht nötig, bei der Demodulationsoperation die Polarität der Modulationswelle in Betracht zu ziehen.

[0071] Auf der Basis der BPSK-Modulationssignaleingabe unterwirft die Modulationsschaltung **23** die vorbestimmte Trägerwelle der ASK-Modulation mit einem Modulationsfaktor (= maximale Amplitude des Datensignals/maximale Amplitude der Trägerwelle), der kleiner als 1 (beispielsweise 0,1) ist, und überträgt die so erzeugte Modulationswelle (ASK-Modulationswelle) durch die Antenne **27** zur IC-Karte **2**.

[0072] Wenn keine Übertragung ausgeführt wird, erzeugt die Modulationsschaltung **23** die Modulationswelle beispielsweise mit einem hohen Pegel von zwei Pegeln (hoher Pegel und niedriger Pegel) von digitalen Signalen.

[0073] Bei der IC-Karte **2** (Fig. 3) wird ein Teil der von der Antenne **27** des R/W **1** abgestrahlten elektromagnetischen Welle in einer LC-Schaltung, die eine Antenne **53** und einen Kondensator **52** aufweist, in ein elektrisches Signal umgesetzt, und das elektrische Signal (Modulationswelle) wird an die RF-Schnittstelle **61** der IC **51** ausgegeben. Der ASK-Demodulator **81** der RF-Schnittstelle **61** detektiert durch Gleichrichten und Glätten der Modulationswelle eine Enveloppe und führt das so erzeugte Signal dem Spannungsregler **82** zu. Außerdem unterdrückt er die DC-Komponente des Signals, um das Datensignal zu extrahieren, und gibt das Datensignal an die BPSK-Demodulationsschaltung **62** und die PLL-Einheit **63** aus.

[0074] Zu diesem Zeitpunkt ist die Endspannung V_0 der Antenne **53** wie folgt:

$$V_0 = V_{10}(1 + k \times Vs(t)) \cos(\omega t).$$

[0075] Dabei stellt $V_{10} \cos(\omega t)$ die Trägerwelle dar, k stellt den Modulationsfaktor dar und Vs(t) stellt von der SPU **32** ausgegebenen Daten dar.

[0076] Der Wert V_{LR} des unteren Pegels der Spannung V_1 nach der Gleichrichtung durch den ASK-Demodulator **81** ist wie folgt:

$$V_{LR} = V_{10}(1 + k \times (-1)) - Vf.$$

[0077] Hier im ASK-Demodulator **81** stellt Vf einen Spannungsabfall in einer eine Gleichrichtungsschaltung zur Gleichrichtung und Glättung bildenden (nicht gezeigten) Diode dar, und er ist generell etwa gleich 0,7 Volt.

[0078] Beim Empfang des vom ASK-Demodulator **81** gleichgerichteten und geglätteten Signals stabilisiert der Spannungsregler **82** das Signal und führt es jeweiligen Schaltungen sowie der Operationseinheit **64** als DC- Energie bzw. -Leistung zu. Da in diesem Fall der Modulationsfaktor k der Modulationswelle wie vorstehend beschrieben kleiner als 1 ist, ist die Spannungsvariation (die Differenz zwischen dem hohen Pegel und dem niedrigen Pegel) nach der Gleichrichtung klein. Demgemäss kann die DC-Leistung im Spannungsregler **82** leicht erzeugt werden.

[0079] Wenn hier die den Modulationsfaktor k von 5% aufweisende Modulationswelle empfangen wird, so dass V_{10} über 3 Volt ist, ist der niedrige Spannungspegel V_{LR} nach der Gleichrichtung gleich 2,15 (= 3 × (1 – 0,05) – 0,7) Volt oder mehr, und der Spannungsregler **82** kann jeder Schaltung eine ausreichende Spannung als Leistung zuführen. In diesem Fall ist die Amplitude $2 \times k \times V_{10}$ (Spitze-zu-Spitze-Wert) der Wechselsignal- bzw. AC-Komponente (Datenkomponente) der Spannung V_1 nach der Gleichrichtung gleich 0,3 (= 2 × 0,05 × 3) Volt oder mehr, und der ASK-Demodulator **81** kann die Daten mit einem ausreichend hohen Signal/Rauschen-Verhältnis bzw. S/N-Verhältnis demodulieren.

[0080] Wie vorstehend beschrieben kann durch Verwendung der einen Modulationsfaktor k kleiner

als 1 aufweisenden ASK-Modulationswelle eine Kommunikation, die eine niedrige Fehlerrate (in einem hohen S/N-Verhältnis-Zustand) aufweist, ausgeführt werden, und kann der IC-Karte **2** eine DC-Spannung, die als Leistung ausreichend ist, zugeführt werden.

[0081] Beim Empfang des Datensignals (BPSK-Demodulationssignals) vom ASK-Demodulator **81** demoduliert die BPSK-Demodulationsschaltung **62** das Datensignal entsprechend dem von der PLL-Einheit **63** zugeführten Taktsignal und gibt die so demodulierten Daten an die Operationseinheit **64** aus.

[0082] Wenn die von der BPSK-Demodulationsschaltung **62** zugeführten Daten verschlüsselt sind, decodiert die Operationseinheit **64** die Daten in der Verschlüsselungs/Decodierungs-Einheit **92** und führt dann die Daten (Befehl) dem Sequenzer **91** zu, um die Daten zu verarbeiten. Während dieser Zeitperiode, das heißt während der Periode vom Zeitpunkt, bei dem die Daten zur IC-Karte **2** übertragen werden, bis eine Antwort auf das Übertragen empfangen wird, überträgt der R/W **1** Daten, die den Wert 1 aufweisen, und ist auf Bereitschaft bzw. Standby. Demgemäss empfängt die IC-Karte **2** während dieser Zeit die Modulationswelle, deren maximale Amplitude konstant ist.

[0083] Nach Beendigung der Verarbeitung gibt der Sequenzer **91** die Daten bezüglich des Verarbeitungsresultats usw. (zum R/W **1** zu übertragende Daten) an die BPSK-Modulationsschaltung **68** aus. Die BPSK-Modulationsschaltung **68** unterwirft die Daten wie im Fall der SPU **32** des R/W **1** der BPSK-Modulation (Codierung in den Manchester-Code) und gibt dann die modulierten Daten an den ASK-Modulator **84** der RF-Schnittstelleneinheit **61** aus.

[0084] Der ASK-Modulator **84** variiert die mit beiden Enden der Antenne **53** verbundene Last entsprechend Daten von der BPSK-Modulationsschaltung **68** durch Benutzung eines Schaltelements oder dgl., wodurch die empfangene Modulationswelle (die maximale Amplitude der vom R/W **1** ausgegebenen Modulationswelle ist, wie vorstehend beschrieben, zur Übertragungszeit von Daten von der IC-Karte **2** konstant) entsprechend den zu übertragenden Daten einer ASK-Modulation unterworfen wird, um die Endspannung der Antenne **27** des R/W **1** zu variieren, und überträgt die so modulierten Daten zum R/W **1**.

[0085] Die Modulationsschaltung **23** des R/W **1** setzt die Übertragung von Daten, die den Wert 1 (hoher Pegel) aufweisen, zur Empfangszeit der Daten von der IC-Karte **2** fort. In der Demodulationsschaltung **25** werden die von der IC-Karte **2** übertragenen Daten auf der Basis einer winzigen Variation (beispielsweise mehrere 10 Mikrovolts) der Anschlussspannung der Antenne **27**, die elektromagnetisch an die Antenne **53** der IC-Karte **2** gekoppelt ist, detektiert.

[0086] Außerdem wird in der Demodulationsschaltung **25** das detektierte Signal (ASK-Modulationswelle) verstärkt und von einem Hochverstärkungsverstärker (nicht gezeigt) moduliert, und die so erhaltenen digitalen Daten werden an die SPU **32** ausgegeben. Die SPU **32** demoduliert die Daten (BPSK-Modulationssignal) und gibt sie an die DPU **31** aus. Die DPU **31** verarbeitet die Daten von der SPU **32** und entscheidet auf der Basis des Verarbeitungsresultats, ob die Kommunikation beendet werden soll oder nicht. Wenn sie entscheidet, dass die Kommunikation wieder ausgeführt wird, wird die Kommunikation zwischen den R/W **1** und der IC-Karte **2** ähnlich wie im obigen Fall ausgeführt. Wenn sie andererseits entscheidet, dass die Kommunikation beendet wird, beendet der R/W **1** die Kommunikationsverarbeitung mit der IC-Karte **2**.

[0087] Wie vorstehend beschrieben überträgt der R/W **1** Daten zur IC-Karte **2** unter Verwendung der ASK-Modulation, bei welcher der Modulationsfaktor k kleiner als 1 ist, und die IC-Karte **2** empfängt die Daten, um die Verarbeitung entsprechend den Daten auszuführen, und bringt die Daten entsprechend dem Verarbeitungsresultat zum R/W **1** zurück.

[0088] Fig. 4 zeigt ein logisches Format des EEPROM **66** der Fig. 3.

[0089] Der EEPROM **66** ist auf einer Blockbasis aufgebaut, und bei einer Ausführungsform der Fig. 4 besteht ein einzelner Block aus beispielsweise 16 Bytes.

[0090] Außerdem ist bei der Ausführungsform der Fig. 4 die logische Adresse des obersten Blocks auf #0000h (h stellt eine hexadezimale Zahl dar) gesetzt, und andere logische Adressen sind in absteigender numerischer Ordnung zugeordnet. In der Fig. 4 sind #0000h bis #FFFFh als die logischen Adressen zugeordnet, und infolgedessen sind 65536 (= 2^{16}) Blöcke gebildet.

[0091] Die Blöcke sind so ausgebildet, dass sie als ein Benutzerblock oder Systemblock benutzt werden. Die Blöcke des EEPROM **66** sind den Benutzerblöcken in der absteigenden numerischen Ordnung der logischen Adressen zugeteilt und den Systemblöcken in der aufsteigenden numerischen Ordnung der logischen Adressen zugeteilt. Das heißt bei der Fig. 4, dass die Benutzerblöcke nach unten zunehmen und die Systemblöcke nach oben zunehmen. Zu dem Zeitpunkt, bei dem kein leerer Block vorhanden ist, können der Benutzerblock und der Systemblock nicht gebildet werden. Demgemäss ist die Grenze zwischen den Benutzerblöcken und den Systemblöcken nicht fest, und der Zahl der Benutzerblöcke und

der Zahl der Systemblöcke ist keine Beschränkung auferlegt (jedoch ist bei der Ausführungsform der Fig. 4 die Gesamtzahl der Benutzerblöcke und der Systemblöcke auf 65536 oder weniger beschränkt).

[0092] Die Systemblöcke sind in fünf Arten eines Herstellungs-Identifikations- bzw. Herstellungs-ID-Blocks, eines Ausgabe-ID-Blocks, eines System definierenden Blocks, eines Bereich definierenden Blocks und eines Dienst definierenden Blocks klassifiziert. Bei der Ausführungsform der Fig. 4 ist der als Bereich definierender Block oder Dienst definierender Block dienende Block als ein Bereich/Dienst definierender Block dargestellt.

[0093] Von bzw. außer den Systemblöcken sind die drei Arten von Blöcken des Herstellungs-ID-Blocks, des Ausgabe-ID-Blocks und des System definierenden Blocks grundsätzlich bei der Ausgabezeit der IC-Karte **2** angeordnet, und sie sind bei den logischen Adressen #FFFFh, #FFFEh bzw. #FFFDh angeordnet. Die Bereich/Dienst definierenden Blöcke sind in einer bildenden Ordnung bei logischen Adressen höher als die logische Adresse #FFFCh angeordnet.

[0094] Information bezüglich der Herstellung der IC-Karte **2** ist im Herstellungs-ID-Block angeordnet. Das heißt beispielsweise, dass eine eindeutige Herstellungs-ID, ein Herstellungsdatum, ein Herstellungscode usw. im Herstellungs-ID-Block angeordnet sind.

[0095] Information bezüglich der Ausgabe der IC-Karte **2** ist im Ausgabe-ID-Block angeordnet. Das heißt, im Ausgabe-ID-Block sind Codes eines Ausgabedatums der IC-Karte **2**, eine Ausgabeordnung der IC-Karte **2** usw, angeordnet.

[0096] Im System definierenden Block sind die Zahl von zum EEPROM **66** gehörenden Systemblöcken oder Benutzerblöcken, ein Systemschlüssel und dgl. angeordnet. Der Systemschlüssel wird benutzt, wenn eine gegenseitige Zertifizierung zwischen der IC-Karte **2**, dem R/W **1** und dem Kontroller **3** ausgeführt wird.

[0097] Der Bereich definierende Block ist durch Zuordnung eines Speicherbereichs (Bereich) des EEPROM **66** zum Verwalter gebildet, und Information zum Verwalten des dem Verwalter selbst zugeordneten Speicherbereichs usw, sind im Bereich definierenden Block angeordnet. Das heißt, im Bereich definierenden Block sind beispielsweise ein später beschriebener Codebereich, eine leere Kapazität, ein Bereichschlüssel usw. angeordnet.

[0098] Im Dienst definierenden Block ist Information zum Verwalten eines später beschriebenen Dienstbereichs (die Kapazität eines Dienstbereichs, ein Dienstschlüssel usw.) angeordnet.

[0099] Der Speicherbereich des EEPROM **66** wird im Sequenzer **91** verwaltet, wobei er geschichtet ist.

[0100] Als nächstes zeigt Fig. 5 die Verzeichnisstruktur des EEPROM **66**.

[0101] Der Speicherbereich des EEPROM **66** ist als eine geschichtete Struktur ausgebildet, bei welcher der Bereich definierende Bereich geschichtet ist, und der Bereich definierende Bereich ist so ausgebildet, dass er einen Bereich definierenden Bereich und einen Dienst definierenden Bereich aufweisen kann.

[0102] Der Bereich definierende Bereich (Schichtschlüsselspeichereinrichtung) ist dem Verwalter zugeordnet. Im Bereich definierenden Bereich sind ein Codebereich, der einen Bereich zur Identifikation von Codes, die als Namen zur Identifikation des Bereich definierenden Bereichs und des Dienst definierenden Bereichs durch den Verwalter benutzbar sind, darstellen, eine leere Kapazität, welche die Zahl verfügbarer leerer Blöcke darstellt, ein Bereichschlüssel zum Erzeugen eines später beschriebenen Zugriffschlüssels, der zur Zertifizierung benutzt wird, angeordnet. Hier korrespondiert der Bereich definierende Bereich von 1 mit dem in Bezug auf die Fig. 4 beschriebenen Bereich definierenden Block von 1.

[0103] Bei der Ausführungsform der Fig. 5 bildet der dem Verwalter A zugeordnete Bereich definierende Bereich die oberste Schicht, und die Bereich definierenden Bereiche der Verwalter B1 und B2 sind mit dem definieren Bereich des Verwalters A gebildet, der als eine Eltern- bzw. Vaterschicht gesetzt ist. Außerdem ist der Bereich definierende Bereich des Verwalters C mit dem definierenden Bereich des Verwalters B1 gebildet, der als eine Vaterschicht gesetzt ist.

[0104] Der Dienst definierende Bereich (Datenspeicherbereichschlüssel-Speichereinrichtung) ist einem vom Verwalter zugeführten Dienst zugeordnet, und die Kapazität eines Dienstbereichs zum Speichern von zur Zufuhr von Diensten notwendigen Daten, ein Dienstschlüssel zum Erzeugen eines Zugriffschlüssels usw. sind im Dienst definierenden Bereich angeordnet. Hier korrespondiert der Dienst definierende Bereich von 1 mit dem unter Bezugnahme auf die Fig. 4 beschriebenen Dienst definierenden Block von 1.

[0105] Der Dienstbereich ist ein Speicherbereich zum Speichern von zur Zufuhr von Diensten notwendigen Daten, und er korrespondiert mit dem Benutzerblock der Fig. 4. Das heißt, der Dienstbereich ist durch Benutzerblöcke über 0 gebildet, und die den Dienstbereich bildende Zahl von Benutzerblöcken ist als die Kapazität des Dienst definierenden Bereichs zum Verwalten des Dienstbereichs angeordnet.

[0106] Außerdem sind im Bereich definierenden Bereich und im Dienst definierenden Bereich Identifikationscodes zur Identifikation dieser Bereiche angeordnet. Hier werden die Identifikationscodes zum Identifizieren des Bereich definierenden Bereichs und des Dienst definierenden Bereichs nachstehend als ein Bereichcode und ein Dienstcode bezeichnet. Der Dienstcode dient zum Identifizieren des Dienst definierenden Bereichs zum Verwalten eines Dienstbereichs, und so kann er als ein Identifikationscode (Dienstbereich-Identifikationscode) zum Identifizieren des betreffenden Dienstbereichs betrachtet werden.

[0107] Bei der Ausführungsform der Fig. 5 ist der Bereich definierende Bereich der obersten Schicht dem Verwalter A zugeordnet. 0000h bis FFFFh sind als ein Bereich benutzbarer Identifikationscodes (Codebereich) definiert, und 0123456789abcdef ist als ein Bereichschlüssel definiert. Hier kann jeder Identifikationscode als der Bereichcode des Bereich definierenden Bereichs benutzt werden, wenn er ein Identifikationscode im Codebereich im Bereich definierenden Bereich ist. Bei dieser Ausführungsform wird der minimale Wert des Codebereichs des Bereich definierenden Bereichs als sein Bereichcode benutzt. Demgemäss ist der Bereichcode des Bereich definierenden Bereichs, dessen Codebereich von 0000h bis FFFFh ist, das heißt, der dem Verwalter A zugeordnete Bereich definierende Bereich auf 0000h gesetzt. Hier wird der Bereich definierende Bereich, dessen Bereichcode auf #xxxxh gesetzt ist, nachstehend als der Bereich definierende Bereich #xxxxh beschrieben.

[0108] Die Schicht des Bereich definierenden Bereichs #0000h des Verwalters A ist mit einem Dienst definierenden Bereich versehen, in welchem der Verwalter A Dienste zuführt. 00008h des Codebereichs von 0000h bis FFFFh des Bereich definierenden Bereichs #0000h ist dem Dienst definierenden Bereich als ein Dienstcode zugeordnet. Hier wird der Dienst definierende Bereich des Dienstcodes #xxxxh nachstehend als der Dienst definierende Bereich #xxxxh beschrieben.

[0109] Die Kapazität des Dienst definierenden Bereichs #0008h ist auf 8 gesetzt, und so ist der durch 8 Benutzerblöcke gebildete Dienstbereich benutzbar. Außerdem ist der Dienstschlüssel des Dienst definierenden Bereichs #0008h auf 0101010101010101 gesetzt.

[0110] Die Schicht des Bereich definierenden Bereichs #0000h des Verwalters A ist mit einem Bereich definierenden Bereich #0100h des Verwalters B1 und einem Bereich definierenden Bereich #1000h des Verwalters B2 als Kindschichten versehen. Außerdem ist die Schicht des Bereich definierenden Bereichs #0000h mit anderen Bereich definierenden Bereichen (nicht gezeigt) versehen, und so ist die Zahl von Blöcken (leere Kapazität), die vom Bereich definierenden Bereich #0000h benutzbar ist, auf beispielsweise 37 Blöcke gesetzt.

[0111] Als der Codebereich des Bereich definierenden Bereichs #0100h des Verwalters B1 ist 0100h bis 03FFh im Codebereich von 0000h bis FFFFh des Bereich definierenden Bereichs #0000h, der die Vaterschicht des Bereich definierenden Bereichs #0100h ist, zugeordnet. Da der Codebereich des Bereich definierenden Bereichs des Verwalters B1 von 0100h bis 03FFh ist, ist hier 0100h, das der minimale Wert des Codebereichs ist, als der Bereichcode des Bereich definierenden Bereichs des Verwalters B1 gesetzt.

[0112] Außerdem sind die leere Kapazität und der Bereichschlüssel des Bereich definierenden Bereichs #0100h auf 14 bzw. a0a0a0a0a0a0a0a0 gesetzt.

[0113] Außerdem ist die Schicht des Bereich definierenden Bereichs #0100h des Verwalters B1 mit dem Bereich definierenden Bereich #0300h des Verwalters C als eine Kindschicht von ihm versehen. Als der Codebereich des Bereich definierenden Bereichs #0300h des Verwalters C ist 0300h bis 03FFh im Codebereich von 0100h bis 03FFh des Bereich definierenden Bereichs #0100h, der seine Vaterschicht ist, zugeordnet. Da der Codebereich des Bereich definierenden Bereichs des Verwalters C von 0300h bis 03FFh ist, ist hier 0300h, welches das Minimum des Codebereichs ist, als der Bereichcode des Bereich definierenden Bereichs des Verwalters C gesetzt.

[0114] Die leere Kapazität und der Bereichschlüssel des Bereich definierenden Bereichs #0300h sind auf 0 bzw. b0b0b0b0b0b0b0b0 gesetzt.

[0115] Die Schicht des Bereich definierenden Bereichs #0300h des Verwalters C ist mit einem Dienst definierenden Bereich zur Dienstzufuhr durch den Verwalter C versehen. 030Ch im Codebereich von 0300h bis 03FFh des Bereich definierenden Bereichs #0300h ist dem Dienst definierenden Bereich als ein Dienstcode zugeordnet.

[0116] Die Kapazität des Dienst definierenden Bereichs, dem der Dienstcode 030Ch zugeordnet ist, das heißt des Dienst definierenden Bereich #030Ch, ist auf 16 gesetzt, und so kann der aus 16 Benutzerblöcken gebildete Dienstbereich benutzt werden. Außerdem ist der Dienstschlüssel des Dienst definierenden Bereichs #030Ch auf 0202020202020202 gesetzt.

[0117] Hier ist die Kapazität des vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereichs gleich 16, und der Dienst definierende Bereich

#030Ch selbst benutzt einen einzelnen Block als Dienst definierenden Block, so dass die Zahl von benutzten Blöcken gleich 17 (= 16 + 1) ist, da der Dienst definierende Bereich #030Ch existiert. Die Zahl von Blöcken, die vom Bereich definierenden Bereich #0300h einer Schicht, zu welcher der Dienst definierende Bereich #030Ch gehört, benutzbar sind, ist gleich null Blöcke, da ihre leere Kapazität gleich null ist. Außerdem benutzt der Bereich definierende Bereich #0300h selbst einen einzelnen Block als einen Bereich definierenden Block. Demgemäss ist in der Schicht des Bereich definierenden Bereichs #0300h die Zahl von benutzten Blöcken gleich 18 (= 17 + 1), und die Zahl benutzbarer Blöcke ist gleich null. Deshalb ergibt sich, dass die Zahl von Blöcken, die von dem als ihre Vaterschicht (obere Schicht) dienenden Bereich definierenden Bereich #0100h zugeordnet sind, gleich 18 (= 18 + 0) ist.

[0118] In Bezug auf die Schicht des Bereich definierenden Bereichs #0100h werden, wie vorstehend beschrieben, 18 Blöcke in dem als eine Kindschicht (untere Schicht) des Bereich definierenden Bereichs #0100h dienenden Bereich definierenden Bereich #0300h benutzt. Außerdem benutzt der Bereich definierende Bereich #0100h selbst einen einzelnen Block als einen Bereich definierenden Block. Die leere Kapazität des Bereich definierenden Bereichs #0100h ist, wie vorstehend beschrieben, gleich 14. Demgemäss ist in der Schicht des Bereich definierenden Bereichs #0100h die Zahl benutzter Blöcke gleich 19 (= 18 + 1), und die Zahl benutzbarer Blöcke ist gleich 14. Deshalb ist die Zahl von Blöcken, die von dem als ihre Vaterschicht dienenden Bereich definierenden Bereich #0000h zugeordnet sind, gleich 33 (= 19 + 14).

[0119] Andererseits sind dem Codebereich des Bereich definierenden Bereichs 1000h des Verwalters B2 1000h bis 1FFFh im Codebereich von 0000h bis FFFFh des als seine Vaterschicht dienenden Bereich definierenden Bereichs #0000h zugeordnet. Da der Codebereich des Bereich definierenden Bereichs des Verwalters B2 von 1000h bis 1FFFh ist, ist hier 1000h, das der minimale Wert des vorstehenden Codebereichs ist, als der Bereichcode des Bereich definierenden Bereichs des Verwalters B2 gesetzt. Außerdem sind die leere Kapazität und der Bereichschlüssel des Bereich definierenden Bereichs #1000h auf 43 bzw. c0c0c0c0c0c0c0c0 gesetzt.

[0120] Die Schicht des Bereich definierenden Bereichs #1000h des Verwalters B2 ist mit einem Dienst definierenden Bereich zur Dienstzufuhr des Verwalters B2 versehen. 1022h im Codebereich von 1000h bis 1FFFh des Bereich definierenden Bereichs #1000h ist dem Dienst definierenden Bereich als ein Dienstcode zugeordnet.

[0121] Die Kapazität des Dienst definierenden Bereichs, dem der Dienstcode 1022h zugeordnet ist, das heißt der Dienst definierende Bereich #1022h, ist auf 4 gesetzt, und so kann ein aus 4 Benutzerblöcken gebildeter Dienstbereich benutzt werden. Außerdem ist der Dienstschlüssel des Dienst definierenden Bereichs #1022h auf 0303030303030303 gesetzt.

[0122] Hier ist die Kapazität des vom Dienst definierenden Bereich #1022h verwalteten Dienstbereichs gleich 4, und der Dienst definierende Bereich #1022h selbst benutzt einen einzelnen Block als einen Dienst definierenden Block, so dass die Zahl benutzter Blöcke wegen der Existenz des Dienst definierenden Bereichs #1022h gleich 5 (= 4 + 1) ist. Außerdem ist die Zahl von Blöcken, die vom Dienst definierenden Bereich #1000h einer Schicht, zu welcher der Dienst definierende Bereich #1022h gehört, benutzbar sind, gleich 43, da ihre leere Kapazität gleich 43 ist. Außerdem benutzt der Bereich definierende Bereich #1000h selbst einen einzelnen Block als einen Bereich definierenden Block. Demgemäss ist in der Schicht des Bereich definierenden Bereichs #1000h die Zahl benutzter Blöcke gleich 6 (= 5 + 1), und die Zahl benutzbarer Blöcke ist gleich 43, so dass die Zahl von Blöcken, die dem Bereich definierenden Bereich #1000h zugeordnet sind, gleich 49 (= 6 + 43) ist.

[0123] Da der Codebereich, der als der Bereich von Identifikationscodes, die einem zu verwaltenden Bereich definierenden Bereich zugeordnet sein können, dient, wie vorstehend beschrieben im Bereich definierenden Bereich gespeichert ist, kann eine solche wie in Fig. 5 gezeigte Schichtstruktur, in der ein Bereich definierender Bereich eines Verwaltungsziels als eine Kindschicht gesetzt ist und ein Bereich definierender Bereich zum Verwalten des Bereich definierenden Bereichs als eine Vaterschicht gesetzt ist, auf der Basis des Codebereichs definiert sein.

[0124] Als nächstes wird unter Bezugnahme auf die Fig. 6 ein Prozess zur Bildung der in Fig. 5 gezeigten Schichtstruktur unter der Annahme, dass der Verwalter A, dem der Bereich definierende Bereich #0000h der obersten Schicht zugeordnet ist, ein Lieferant einer IC-Karte **2** ist, beschrieben.

[0125] Der Verwalter A gibt die IC-Karte **2** entsprechend der Anforderung des Benutzers aus (1). Nur der Bereich definierende Bereich #000h in der Schichtstruktur der Fig. 5 ist in der IC-Karte **2** ausgebildet.

[0126] Wenn der Verwalter A die Zufuhr eines vorbestimmten Dienstes durch Benutzung des vom Dienst definierenden Bereich #0008h verwalteten Dienstbereichs startet, registriert der Verwalter A in der registrierten Kartenausgabemaschine **101** Information, die zur Bildung des Dienst definierenden Bereichs #0008h notwendig ist (2).

[0127] Hier ist die registrierte Kartenausgabemaschine **101** beispielsweise durch den R/W **1** und den Kontroller **3**, die in Fig. 1 gezeigt sind, gebildet. Die registrierte Kartenausgabemaschine **101** kann in einem Bahnhof, einem Einzelhandelsgeschäft oder anderen Einrichtungen angeordnet sein.

[0128] Wenn danach ein Benutzer eine IC-Karte **2** in eine registrierte Kartenausgabemaschine **101** einsetzt (wenn die IC-Karte **2** in den Zustand gesetzt ist, dass sie mit dem in der registrierten Kartenausgabemaschine **101** enthaltenen R/W **1** kommunizieren kann), überträgt die registrierte Kartenausgabemaschine **101** einen Befehl und notwendige Daten zur IC-Karte **2** auf der Basis registrierter Information, um den Dienst definierenden Bereich #0008h zu bilden. Durch die vorstehende Operation kann dem Benutzer der Dienst des Verwalters A durch Benutzung des vom Dienst definierenden Bereich #0008h verwalteten Dienstbereichs zugeführt werden.

[0129] Wenn andererseits die Verwalter B1, B2 wollen, dass ihnen der Dienst unter Verwendung der IC-Karte **2** zugeführt wird, macht jeder von ihnen einen Vertrag mit dem Verwalter A, so dass der Verwalter A in der registrierten Kartenausgabemaschine **101** Information registriert, die zur Bildung der Bereich definierenden Bereiche #0100h und #1000h notwendig ist (3), (4). Wenn ein Benutzer eine IC-Karte **2** in die registrierte Kartenausgabemaschine **101** einsetzt, überträgt die registrierte Kartenausgabemaschine **101** einen Befehl und notwendige Daten zur IC-Karte **2** auf der Basis der registrierten Information, um die Bereich definierende Bereiche #0100h und #1000h zu bilden, wodurch die Verwalter B1 oder B2 die Ressource der IC-Karte **2** in dem im Bereich definierenden Bereich #0100h oder #1000h definierten Bereich benutzen können.

[0130] Wenn danach der Verwalter B2 beginnt, einen vorbestimmten Dienst durch Benutzung des vom Dienst definierenden Bereich #1022h verwalteten Dienstbereichs zuzuführen, registriert der Verwalter B2 in der registrierten Kartenausgabemaschine **101** Information, die zur Bildung des Dienst definierenden Bereichs #1022h notwendig ist (5). Wenn ein Benutzer eine IC-Karte **2** in die registrierte Kartenausgabemaschine **101** einsetzt, überträgt die registrierte Kartenausgabemaschine **101** auf der Basis der registrierten Information einen Befehl und notwendige Daten zur IC-Karte **2**, um den Dienst definierenden Bereich #1022h zu bilden. Deshalb kann dem Benutzer der Dienst des Verwalters B2 unter Verwendung des vom Dienst definierenden Bereich #1022h verwalteten Dienstbereichs zugeführt werden.

[0131] Wenn außerdem der Verwalter C wünscht, unter der Verwaltung des Verwalters B1 einen Dienst durch die IC-Karte **2** zuzuführen, macht der Verwalter C einen Vertrag mit dem Verwalter B1, so dass der Verwalter B1 in der registrierten Kartenausgabemaschine **101** Information registriert, die zur Bildung des Bereich definierenden Bereichs #0300h notwendig ist (6). Wenn ein Benutzer eine IC-Karte **2** in die registrierte Kartenausgabemaschine **101** einsetzt, überträgt die registrierte Kartenausgabemaschine **101** auf der Basis der registrierten Information einen Befehl und notwendige Daten zur IC-Karte **2**, um den Bereich definierenden Bereich #0300h zu bilden, wodurch der Verwalter C die Ressource der IC-Karte **2** in dem im Bereich definierenden Bereich #0300h definierten Bereich benutzen kann.

[0132] Wenn danach der Verwalter C beginnt, einen vorbestimmten Dienst durch Benutzung des vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereichs zuzuführen, registriert der Verwalter C in der registrierten Kartenausgabemaschine **101** Information, die zur Bildung des Dienst definierenden Bereichs #030Ch notwendig ist (7). Wenn ein Benutzer eine IC-Karte **2** in die registrierte Kartenausgabemaschine **101** einsetzt, überträgt die registrierte Kartenausgabemaschine **101** auf der Basis der registrierten Information einen Befehl und notwendige Daten zur IC-Karte **2**, um den Dienst definierenden Bereich #030Ch zu bilden, wodurch der Benutzer die Zufuhr des Dienstes vom Verwalter C unter Verwendung des vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereichs akzeptieren kann.

[0133] In der IC-Karte **2** werden, wie vorstehend beschrieben, der Bereich definierende Bereich und der Dienst definierenden Bereich entsprechend dem Befehl aus der registrierten Kartenausgabemaschine **101** gebildet. Die Bereich bildende Verarbeitung zur Bildung des Bereich definierenden Bereichs und die Dienst bildende Verarbeitung zur Bildung des Dienst definierenden Bereichs werden beispielsweise vom Sequenzer **91** ausgeführt. Die Bereich bildende Verarbeitung und die Dienst bildende Verarbeitung werden unter Bezugnahme auf die Fig. 7 und Fig. 8 beschrieben.

[0134] Zuerst wird die Bereichsbildungsverarbeitung unter Bezugnahme auf das Flussdiagramm der Fig. 7 beschrieben.

[0135] Wenn die IC-Karte in die registrierte Kartenausgabemaschine **101** eingesetzt ist, überträgt die registrierte Kartenausgabemaschine **101** an die IC-Karte **2** beispielsweise einen Befehl, der instruiert, einen Bereich definierenden Bereich zu bilden (nachstehend als ein Definierbefehl oder Bereichbildungsbefehl bezeichnet), Information, die zur Bildung des Bereich definierenden Bereichs notwendig ist, das heißt den Codebereich des zu bildenden Bereich definierenden Bereichs, die Zahl von Blöcken, die dem Bereich definierenden Bereich zugeordnet sind (nachstehend als Zuordnungsblockzahl bezeichnet), einen Bereichschlüssel und einen Bereichcode des

als die Vaterschicht dienenden Bereich definierenden Bereichs (nachstehend als Vaterbereichcode bezeichnet).

[0136] Hier ist es vom Gesichtspunkt der Sicherheit vorzuziehen, dass Information, die zur Bildung eines Bereich definierenden Bereichs notwendig ist, verschlüsselt zur IC-Karte **2** übertragen wird. Die Verschlüsselung kann beispielsweise durch Benutzung des gleichen Schlüssels wie der in dem den Vaterbereichcode aufweisenden Bereich definierenden Bereich gespeicherte Bereichschlüssel ausgeführt werden. Der in dem den Vaterbereichcode aufweisenden Bereich definierenden Bereich gespeicherte Bereichschlüssel ist im EEPROM **66** gespeichert, so dass die verschlüsselte Information in der IC-Karte **2** decodiert werden kann.

[0137] Beim Empfang des Bereichbildungsbefehls decodiert die IC-Karte **2** (Sequenzer **91**) die zusammen mit dem Bereichbildungsbefehl übertragene verschlüsselte Information, erkennt dadurch den Vaterbereichcode und den Codebereich sowie den Zuordnungsblock und den Bereichschlüssel des zu bildenden Bereich definierenden Bereichs. Außerdem wird in der IC-Karte **2** der Bereichcode des zu bildenden Bereich definierenden Bereichs erkannt. Das heißt, es wird in diesem Fall der minimale Wert des Codebereichs des zu bildenden Bereich definierenden Bereichs als sein Bereichcode erkannt.

[0138] In der IC-Karte **2** wird beim Schritt S1 entschieden, ob der zu bildende Bereich definierenden Bereich schon im EEPROM **66** gebildet worden ist. Das heißt, beim Schritt S1 wird entschieden, ob der den gleichen Bereichcode wie der Bereichcode des zu bildenden Bereich definierenden Bereichs aufweisende Bereich definierende Bereich schon gebildet worden ist.

[0139] Wenn beim Schritt S1 entschieden wird, dass der zu bildende Bereich definierenden Bereich schon gebildet worden ist, ist die Bereich bildende Verarbeitung beendet. Das heißt in dem Fall, dass der zu bildende Bereich definierende Bereich schon gebildet worden ist, wird keine nachfolgende Verarbeitung ausgeführt, da es nicht notwendig ist, den gleichen Bereich definierenden Bereich doppelt zu bilden.

[0140] Wenn beim Schritt S1 entschieden wird, dass der zu bildende Bereich definierende Bereich noch nicht gebildet worden ist, geht die Verarbeitung zum Schritt S2, um zu entscheiden, ob der Codebereich des zu bildenden Bereich definierenden Bereichs und die Zahl zugeordneter Blöcke (Kapazität) richtig sind oder nicht. Das heißt, es wird beim Schritt S2 entschieden, ob der Codebereich des zu bildenden Bereich definierenden Bereichs in dem Codebereich enthalten ist, der in dem Bereich definierenden Bereich gespeichert ist, welcher den Vatercode aufweist, und ob die Zuordnungsblockzahl des zu bildenden Bereich definierenden Bereichs unter der leeren Kapazität ist, die in dem Bereich definierenden Bereich, der den Vaterbereichcode aufweist, gespeichert ist.

[0141] Wenn beim Schritt S2 entschieden wird, dass der Codebereich des zu bildenden Bereich definierenden Bereichs und die Zuordnungsblockzahl nicht richtig sind, das heißt, wenn der Codebereich des zu bildenden Bereich definierenden Bereichs in dem Codebereich enthalten ist, der in dem Bereich definierenden Bereich, der den Vaterbereichcode aufweist gespeichert ist, oder die Zuordnungsblockzahl des zu bildenden Bereich definierenden Bereichs die in dem den Vaterbereichcode aufweisenden Bereich definierenden Bereich gespeicherte leere Kapazität überschreitet, wird beim Schritt S3 die Fehlerverarbeitung ausgeführt, und dann wird die Bereich bildende Verarbeitung beendet. Das heißt, beim Schritt S3 wird eine Nachricht, bei welcher der den Vaterbereichcode aufweisende Bereich definierende Bereich als eine Vaterschicht gesetzt ist, jedoch kein Bereich definierender Bereich, der als eine Kindschicht von ihr dient, gebildet werden kann, zur registrierten Kartenausgabemaschine **101** übertragen. Demgemäss wird in diesem Fall kein Bereich definierender Bereich gebildet.

[0142] Wenn andererseits beim Schritt S2 entschieden wird, dass der Codebereich des zu bildenden Bereich definierenden Bereichs und die Zuordnungsblockzahl richtig sind, das heißt entschieden wird, dass der Codebereich des zu bildenden Bereich definierenden Bereichs in dem Codebereich enthalten ist, der in dem Bereich definierenden Bereich gespeichert ist, welcher den Vaterbereichcode aufweist, und die Zuordnungsblockzahl des zu bildenden Bereich definierenden Bereichs unter der leeren Kapazität ist, die in dem den Vaterbereichcode aufweisenden Bereich definierenden Bereich gespeichert ist, wird beim Schritt S4 der zu bildende Bereich definierende Bereich als eine Kindschicht der Schicht (Vaterschicht) des den Vaterbereichcode aufweisenden Bereich definierenden Bereichs gebildet.

[0143] Das heißt, beim Schritt S4 wird der unterste Block (der die größte logische Adresse aufweisende leere Block) in den leeren Blöcken des EEPROM **66** (Fig. 4) als der mit dem zu bildenden Bereich definierenden Bereich korrespondierende Bereich definierende Block gesichert. Außerdem werden der Codebereich, die leere Kapazität, der Bereichschlüssel usw. in den Bereich definierenden Block geschrieben. Hier werden beim Schritt S4 von der registrierten Kartenausgabemaschine **101** übertragene Daten direkt als der Codebereich und der Codeschlüssel geschrieben. Der durch Subtrahieren von 1 von der von der registrierten Kartenausgabemaschine **101**

übertragenen Zuordnungsblockzahl erhaltene Wert wird als die leere Kapazität geschrieben. Der durch Subtrahieren von 1 von der Zuordnungsblockzahl erhaltene Wert wird geschrieben, da der so gebildete Bereich definierende Bereich einen einzelnen Block benutzt.

[0144] Danach geht die Verarbeitung zum Schritt S5, um die leere Kapazität des Bereich definierenden Bereichs des Vaterbereichcodes neu zu schreiben, und dann ist die Bereich bildende Verarbeitung beendet. Das heißt, beim Schritt S5 wird der durch Subtrahieren der Zuordnungsblockzahl von der leeren Kapazität des den Vaterbereichcode aufweisenden Bereich bildenden Bereichs erhaltene Wert als eine leere Kapazität des den Vaterbereichcode aufweisenden Bereich definierenden Bereichs neu geschrieben.

[0145] Die Bereich definierenden Bereiche #0100h, #1000h, #0300h der in Fig. 5 gezeigten Verwalter B1, B2, C werden durch die vorstehende Bereich bildende Verarbeitung gebildet.

[0146] Das heißt unter der Annahme, dass zur Ausgabezeit der IC-Karte **2** der Verwalter A, der auch der Ausgeber der IC-Karte **2** ist, alle Ressourcen der IC-Karte **2** hat, und die Identifikationscodes oder die Kapazität, die von der IC-Karte **2** benutzt werden können, von 0000h bis FFFFh sind oder 65533 Blöcke ist, nur der Bereich definierende Bereich #0000h der obersten Schicht, in welcher der Codebereich von 0000h bis FFFFh ist und die leere Kapazität gleich 65532 ist, zur Ausgabezeit der IC-Karte **2** als Bereich definierender Bereich existiert.

[0147] Bei dieser Ausführungsform weist, wie in Fig. 4 gezeigt, der EEPROM **66** 65536 Blöcke auf, jedoch ist die nutzbare Kapazität unmittelbar nach Ausgabe der IC-Karte **2** gleich 65533 Blöcke, welche Zahl um 3 kleiner als 65536 ist, da der Herstellungs-ID-Block, der Ausgabe-ID-Block und der System definierende Block existieren.

[0148] Außerdem ist die leere Kapazität des Bereich definierenden Bereichs #0000h der obersten Schicht gleich 65532 Blöcke, welche Zahl um einen Block kleiner als die nutzbare Kapazität von 65533 Blöcken ist, da der Bereich definierende Bereich #0000h selbst einen einzelnen Block benutzt.

[0149] Wenn der Verwalter A dem Verwalter B1 die Identifikationscodes im Bereich von 0100h bis 03FFh und 63 Blöcke in ihren Ressourcen zuteilt, wird die Bereich bildende Verarbeitung ausgeführt, um den Bereich definierenden Bereich #0100h zu bilden. Das heißt, in diesem Fall werden 0100h bis 03FFh und 32 Blöcke als ein Codebereich bzw. eine leere Kapazität in den Bereich definierenden Bereich #0100h geschrieben. Die leere Kapazität ist um einen einzelnen Block kleiner als die vom Verwalter A zugeteilte Zahl von 33 Blöcken, da der Bereich definierende Bereich #0100h selbst einen einzelnen Block benutzt.

[0150] Wenn der Bereich definierende Bereich #0100h gebildet wird, wird die leere Kapazität des Bereich definierenden Bereichs #0000h des Verwalters A um dem Verwalter B1 zugeteilte 33 Blöcke reduziert.

[0151] Wenn der Verwalter A dem Verwalter B2 die Identifikationscodes des Bereichs von 1000h bis 1FFFh und 49 Blöcke zuteilt, wird die Bereich bildende Verarbeitung ausgeführt, um den Bereich definierenden Bereich #1000h zu bilden. Das heißt, in diesem Fall werden 1000h bis 1FFFh und 48 Blöcke als ein Codebereich bzw. eine leere Kapazität in den Bereich definierenden Bereich #1000h geschrieben. Die leere Kapazität ist um einen einzelnen Block kleiner als die vom Verwalter A abgeteilte Zahl von 49 Blöcken, da der Bereich definierende Bereich #1000h selbst einen einzelnen Block benutzt.

[0152] Wenn der Bereich definierende Bereich #1000h gebildet wird, wird die leere Kapazität des Bereich definierenden Bereichs #0000h des Verwalters A um dem Verwalter B2 zugeteilte 33 Blöcke reduziert.

[0153] Wenn der Bereich definierende Bereich #0100h oder #1000h wie vorstehend beschrieben gebildet wird, kann der Verwalter B1 oder B2 in der Schicht des Bereich definierenden Bereichs #0100h oder #1000h einen Bereich definierenden Bereich und einen Dienst definierenden Bereich als Kindschichten der vorstehenden Schicht bilden.

[0154] Wenn beispielsweise der Verwalter B1 dem Verwalter C die Identifikationscodes des Bereichs von 0300h bis 03FFh und 18 Blöcke zuteilt, wird die Bereich bildende Verarbeitung ausgeführt, um den Bereich definierenden Bereich #0300h zu bilden. Das heißt, in diesem Fall werden 0300h bis 03FFh und 17 Blöcke als ein Codebereich und eine leere Kapazität in den Bereich definierenden Bereich #0300h geschrieben. Die leere Kapazität ist um einen einzelnen Block kleiner als die vom Verwalter B1 zugeteilte Zahl von 18 Blöcken, da der Bereich definierende Bereich #0300h selbst einen einzelnen Block benutzt.

[0155] Wenn der Bereich definierende Bereich #0300h gebildet wird, wird die leere Kapazität des Bereich definierenden Bereichs #0100h des Verwalters B1 um die vom Verwalter C zugeteilte Zahl von 18 Blöcken reduziert. Das heißt, die leere Kapazität des Bereich definierenden Bereichs #0100h ist, wie vorstehend beschrieben, gleich 32 Blöcke, wenn der Bereich definierende Bereich #0100h gebildet wird. Wie jedoch in Fig. 5 gezeigt, werden 18 Blöcke von der leeren Kapazität reduziert, und so ist die leere

Kapazität gleich 14 Blöcke.

[0156] Als nächstes wird die Dienst bildende Verarbeitung unter Bezugnahme auf das Flussdiagramm der Fig. 8 beschrieben.

[0157] Wenn die IC-Karte **2** in die registrierte Kartenausgabemaschine **101** eingesetzt ist, überträgt die registrierte Kartenausgabemaschine **101** zur die IC-Karte **2** einen Befehl, der instruiert, einen Dienst bildenden Bereich zu bilden, (nachstehend als Dienst bildender Befehl bezeichnet), eine zum Bilden des Dienst definierenden Bereichs notwendige Information, das heißt einen Dienstcode des zu bildenden Dienst definierenden Bereichs, die dem Dienst definierenden Bereich zugeordnete Zahl von Blöcken (nachstehend als Zuordnungsblockzahl bezeichnet), den Dienstschlüssel, den Bereichcode des Bereich definierenden Bereichs der Schicht, in welcher der Dienst definierende Bereich gebildet ist, (nachstehend als Vaterbereichcode bezeichnet), usw. zu übertragen.

[0158] Hier ist es vom Gesichtspunkt der Sicherheit zu bevorzugen, dass zum Bilden des Dienst definierenden Bereichs notwendige Information zur IC-Karte übertragen wird, während sie durch Benutzung des gleichen Schlüssels wie der in dem Bereich definierenden Bereich, der den Vaterbereichcode wie im Fall der Bereich bildenden Verarbeitung aufweist, gespeicherte Bereichsschlüssel verschlüsselt wird.

[0159] Wenn der Dienst bildende Befehl empfangen wird, decodiert die IC-Karte **2** (Sequenzer **91**) die zusammen mit dem Dienst bildenden Befehl übertragene verschlüsselte Information und erkennt dadurch den Vaterbereichcode, den Dienstcode, die Zuordnungsblockzahl und den Dienstschlüssel des zu bildenden Dienst definierenden Bereichs.

[0160] In der IC-Karte **2** wird beim Schritt S11 entschieden, ob der zu bildenden Dienst definierende Bereich im EEPROM **66** gebildet worden ist. Das heißt, es wird beim Schritt S11 entschieden, ob ein Dienst definierender Bereich, der den gleichen Dienstcode wie der zu bildenden Dienst definierende Bereich aufweist, schon gebildet worden ist.

[0161] Wenn beim Schritt S11 entschieden worden ist, dass der zu bildende Dienst definierende Bereich schon gebildet worden ist, wird die Dienst bildende Verarbeitung beendet. Das heißt, wenn der zu bildende Dienst definierende Bereich schon gebildet worden ist, wird die nachfolgende Verarbeitung nicht ausgeführt, da es nicht notwendig ist, den gleichen Dienst definierenden Bereich doppelt zu bilden.

[0162] Wenn außerdem beim Schritt S11 entschieden wird, dass der zu bildendende Dienst definierende Bereich nicht gebildet worden ist, geht die Verarbeitung zum Schritt S12, um zu entscheiden, ob der Dienstcode des zu bildenden Dienst definierenden Bereichs und die Zuordnungsblockzahl (Kapazität) richtig sind oder nicht. Das heißt, es wird beim Schritt S12 entschieden, ob der Dienstcode des zu bildenden Dienst definierenden Bereichs in dem den Vaterbereichcode aufweisenden Dienst definierenden Bereich enthalten ist und die Zuordnungsblockzahl des zu bildenden Dienst definierenden Bereichs unter der in dem den Vaterbereichcode aufweisenden Dienst definierenden Bereich gespeicherten leeren Kapazität ist.

[0163] Wenn beim Schritt S12 entschieden wird, dass der Dienstcode des zu bildenden Dienst definierenden Bereichs und die Zuordnungsblockzahl nicht richtig sind, das heißt, wenn der Dienstcode des zu bildenden Dienst definierenden Bereichs nicht in dem im Bereich definierenden Bereich der Vaterschicht gespeicherten Codebereich enthalten ist oder die Zuordnungsblockzahl des zu bildenden Dienst definierenden Bereichs die in dem Bereich definierenden Bereich der Vaterschicht gespeicherte leere Kapazität überschreitet, geht die Verarbeitung zum Schritt S13, um die Fehlerverarbeitung auszuführen, und dann wird die Bereich bildende Verarbeitung beendet. Das heißt, es wird eine Nachricht, bei der ein Dienst definierender Bereich in der Schicht des Bereich definierenden Bereichs der Vaterschicht nicht ausgebildet werden kann, zur registrierten Kartenausgabemaschine **101** übertragen. Demgemäss kann in diesem Fall ein Dienst definierender Bereich nicht gebildet werden.

[0164] Wenn andererseits beim Schritt S12 entschieden wird, dass der Dienstcode des zu bildenden Dienst definierenden Bereichs und die Zuordnungsblockzahl richtig sind, das heißt, wenn der Dienstcode des zu bildenden Dienst definierenden Bereichs in dem Code enthalten ist, der in dem den Vaterbereichcode aufweisenden Bereich definierenden Bereich gespeichert ist, und die Zuordnungsblockzahl des zu bildenden Dienst definierenden Bereichs unter der im Bereich definierenden Bereich des Vaterbereichcodes gespeicherten leeren Kapazität ist, geht die Verarbeitung zum Schritt S14, bei dem der zu bildende Dienst definierende Bereich in der Schicht des den Vaterbereichcode aufweisenden Dienst definierenden Bereichs gebildet wird.

[0165] Das heißt, beim Schritt S14 wird der unterste Block (ein die größte logische Adresse aufweisender leerer Block) in den leeren Blöcken des EEPROM **66** (Fig. 4) als der mit dem zu bildenden Dienst definierenden Bereich korrespondierende Dienst definierende Block gesichert. Außerdem werden der Dienstcode, die Kapazität, der Dienstschlüssel usw. in den Dienst definierenden Block geschrieben. In diesem Fall werden beim Schritt S14 der Dienstcode und der Dienstschlüssel, die von der registrierten Kartenaus-

gabemaschine **101** übertragen werden, direkt geschrieben. Der durch Subtraktion von der von der registrierten Kartenausgabemaschine **101** übertragenen Zuordnungsblockzahl um 1 erhaltene Wert wird als die Kapazität geschrieben. Der durch Subtraktion der Zuordnungsblockzahl um 1 erhaltene Wert wird geschrieben, da der zu bildende Dienst definierende Bereich einen einzelnen Block benutzt.

[0166] Beim Schritt S14 werden leere Blöcke, deren Zahl mit der in den so gebildeten Dienst definierenden Bereich geschriebenen Kapazität korrespondieren, in Logikadressen-Zunahmeordnung ausgewählt und als Benutzerblöcke gesichert, die den vom Dienst definierenden Bereich verwalteten Dienstbereich bilden. Danach geht die Verarbeitung zum Schritt S15.

[0167] Beim Schritt S15 wird die leere Kapazität des den Vaterbereichcode aufweisenden Bereich definierenden Bereichs neu geschrieben, und die Dienst bildende Verarbeitung wird beendet. Das heißt, beim Schritt S15 wird der durch Subtraktion der Zuordnungsblockzahl von der leeren Kapazität des den Vaterbereichcode aufweisenden Bereich definierenden Bereichs erhaltene Wert als die leere Kapazität des Bereich definierenden Bereichs neu geschrieben.

[0168] Die Dienst definierenden Bereiche #0008h, #1022h, #030Ch der in Fig. 5 gezeigten Verwalter A, B2, C werden durch Ausführen der vorstehenden Dienst bildenden Verarbeitung gebildet.

[0169] Das heißt, wenn der Verwalter A seine Dienste unter Verwendung des Identifikationscodes von 0008h und der Kapazität von 9 Blöcken in seinen Ressourcen zuführt, wird die Dienst bildende Verarbeitung ausgeführt, um den Dienst definierenden Bereich #0008h zu bilden, und 8 Blöcke werden in den Dienst definierenden Bereich #0008h als Kapazität geschrieben. Außerdem werden acht leere Blöcke als Benutzerblöcke gesichert und als ein vom Dienst definierenden Bereich #0008h verwalteter Dienstbereich gesetzt. Die in den Dienst definierenden Bereich #0008h geschriebene Kapazität ist um einen einzelnen Block kleiner als die Zahl von 9 Blöcken, da der Dienst definierende Bereich #0008h einen einzelnen Block benutzt.

[0170] Wenn der Dienst definierende Bereich #0008h gebildet wird, wird die leere Kapazität des Bereich definierenden Bereichs #0000h des Verwalters A um neun Blöcke, die dem Dienst definierenden Bereich #0008h zugeteilt sind, reduziert.

[0171] Wie vorstehend beschrieben kann der Verwalter A Dienste durch Benutzung des Dienstbereichs von acht Blöcken, der vom Dienst definierenden Bereich #0008h verwaltet wird, zuführen.

[0172] Wenn der Verwalter B2 Dienste durch Benutzung des Identifikationscodes von 1022h und einer Kapazität von 5 Blöcken in seinen Ressourcen zuführt, wird die Dienst bildende Verarbeitung ausgeführt, um den Dienst definierenden Bereich #1022h zu bilden, und in den Dienst definierenden Bereich #1022h werden 4 Blöcke als Kapazität geschrieben. Außerdem werden vier leere Blöcke als Benutzerblöcke gesichert, und sie werden als ein vom Bereich definierenden Bereich #1022h verwalteter Dienstbereich gesetzt. Die in den Dienst definierenden Bereich #1022h geschriebene Kapazität ist um einen einzelnen Block kleiner als die Zahl von 5 Blöcken, da der Dienst definierende Bereich #1022h selbst einen einzelnen Block benutzt.

[0173] Wenn der Dienst definierende Bereich #1022h gebildet wird, wird die leere Kapazität des Bereich definierenden Bereichs #1000h des Verwalters B2 um 5 Blöcke, die dem Dienst definierenden Bereich #1022h zugeteilt werden, reduziert. Das heißt, die leere Kapazität ist, wie vorstehend beschrieben, zu dem Zeitpunkt, bei dem der Bereich definierende Bereich #1000h gebildet wird, gleich 48 Blöcke, jedoch ist sie um 5 Blöcke reduziert und so, wie in Fig. 5 gezeigt, gleich 43 Blöcke.

[0174] Wie vorstehend beschrieben kann der Verwalter B2 Dienste durch Benutzung des Dienstbereiches von vier Blöcken, die vom Dienst definierenden Bereich #1022h verwaltet werden, zuführen.

[0175] Wenn außerdem der Verwalter C Dienste durch Benutzung beispielsweise des Identifikationscodes von 030Ch und der Kapazität von 17 Blöcken in seinen Ressourcen zuführt, wird die Dienst bildende Verarbeitung ausgeführt, um den Dienst definierenden Bereich #030Ch zu bilden, und es werden in den Dienst definierenden Bereich #030Ch 16 Blöcke als Kapazität geschrieben. Außerdem werden 16 leere Blöcke als Benutzerblöcke gesichert, und sie werden als ein Dienstbereich, der vom Bereich definierenden Bereich #030Ch verwaltet wird, gesetzt. Die in den Dienst definierenden Bereich #030Ch geschriebene Kapazität ist um einen einzelnen Block kleiner als die Zahl von 17 Blöcken, da der Dienst definierende Bereich #030Ch selbst einen einzelnen Block benutzt.

[0176] Wenn der Dienst definierende Bereich #030Ch gebildet wird, wird die leere Kapazität des Bereich definierenden Bereichs #0300h des Verwalters C um 17 Blöcke, die dem Dienst definierenden Bereich #030Ch zugeteilt werden, reduziert. Das heißt, die leere Kapazität ist, wie vorstehend beschrieben, zu dem Zeitpunkt, bei dem der Bereich definierende Bereich #0300h gebildet wird, gleich 17 Blöcke, jedoch ist sie um 17 Blöcke reduziert und so, wie in Fig. 5 gezeigt, gleich null.

[0177] Wie vorstehend beschrieben kann der Verwalter C Dienste durch Benutzung des Dienstbereichs von 16 Blöcken, der vom Dienst definierenden Bereich #030Ch verwaltet wird, zuführen.

[0178] Wie vorstehend beschrieben wird der EEPROM **66** auf der Basis des Dienst definierenden Bereichs, in welchem der Codebereich und die leere Kapazität gespeichert sind, verwaltet, so dass das Ressourcenverwaltung der IC-Karte **2** ausgeführt werden kann. Das heißt, es können die Kapazität und Identifikationscodes, die in der Schicht eines Dienst definierenden Bereichs benutzbar sind, beschränkt werden. Als Resultat kann, selbst wenn der Verwalter einen Teil von ihm zugeordneten Ressourcen (in diesem Fall Kapazität und Identifikationscodes, die benutzbar sind) einem anderen Verwalter zuteilt, so dass die IC-Karte **2** gemeinsam benutzbar ist, verhindert werden, dass der Identifikationscode zwischen unterschiedlichen Verwaltern überlappt wird, und es kann verhindert werden, dass der Verwalter den EEPROM **66** mit übermäßiger Kapazität, die durch einen Vertrag oder dgl. vorbestimmt ist, benutzt.

[0179] In der IC-Karte **2** weist der Speicherbereich des EEPROM **66** die Schichtstruktur auf, in welcher der Bereich definierende Bereich wie in Bezug auf Fig. 5 beschrieben geschichtet ist, und Schlüssel zur Zertifizierung (bei dieser Ausführungsform sind ein Schlüssel für einen Bereich definierenden Bereich und ein Schlüssel für einen Dienst definierenden Bereich als ein Bereichschlüssel bzw. ein Dienstschlüssel bezeichnet) sind im Bereich definierenden Bereich bzw. Dienst definierenden Bereich gespeichert, so dass eine Zugriffssteuerung, die bei der IC-Karte **2** hoch in der Flexibilität und Sicherheit ist, ausgeführt werden kann.

[0180] Das heißt, es kann eine Zugriffsteuerung, die bei der IC-Karte **2** hoch in der Flexibilität und Sicherheit ist, durch wie in Fig. 9 gezeigte Abgabe von Information zwischen Verwaltern implementiert werden.

[0181] Insbesondere bestimmt der Verwalter A, der auch als der Ausgeber der IC-Karte **2** dient, einen im System definierenden Block des EEPROM **66** (Fig. 4) zu speichernden Systemschlüssel und einen Bereichschlüssel des Bereich definierenden Bereichs #0000h seiner selbst und speichert den Systemschlüssel im System definierenden Block, während er den Bereichschlüssel #0000h im Bereich definierenden Bereich #0000h speichert. Hier wird der Bereichschlüssel des Bereich definierenden Bereichs #xxxxh nachstehend als Bereichschlüssel #xxxxh bezeichnet.

[0182] Außerdem verschlüsselt der Verwalter A den Systemschlüssel mit dem Bereichschlüssel #0000h und erzeugt einen Bereichzwischenschlüssel K_A. Als ein Verschlüsselungsverfahren können DES (Data Encryption Standard (Datenverschlüsselungsstandard)), FEAL (Fast Data Encipherment Algorithm (schneller Datenentzifferungsalgorithmus)) oder dgl. benutzt werden.

[0183] Wenn der Verwalter A seine Ressourcen dem Verwalter B1 zuteilt, gibt der Verwalter A den Bereichzwischenschlüssel K_A zum Verwalter B1. Außerdem bestimmt der Verwalter A den Bereichschlüssel #0100h des Verwalters B1 und gibt (verteilt) ihn zum Verwalter B1 zusammen mit seinem Bereichcode #0000h.

[0184] Demgemäss kann der Verwalter B1 den Bereichzwischenschlüssel K_A und seinen Bereichschlüssel #0100h erkennen, jedoch kann er nicht den Systemschlüssel und den Bereichschlüssel #0000h des Verwalters A, der ein sogenannter Vater ist, erkennen. Jedoch ist der Bereichschlüssel #0100h des Verwalters B1 durch den Verwalter A, der als ein Vater dient, dem Verwalter B1, der als sogenannter Vater bzw. sogenanntes Kind dient, gegeben, und so erkennt der Verwalter A, der als der Vater dient, den Bereichschlüssel #0100h des Verwalters B1, der als das Kind dient.

[0185] Der vom Verwalter A dem Verwalter B1 gegebene Bereichschlüssel #0100h wird durch die Bereich bildende Verarbeitung (Fig. 7) des Bereich definierenden Bereichs #0100h des Verwalters B1 in den Bereich definierenden Bereich #0100h geschrieben.

[0186] Der Verwalter B1 verschlüsselt den vom als seine Vater dienenden Verwalter A erhaltenen Bereichzwischenschlüssel K_A auf der Basis des vom Verwalter A erhaltenen Bereichschlüssels #0100h, um einen Bereichzwischenschlüssel K_{B1} zu erzeugen.

[0187] Der Verwalter A gibt auch den Bereichzwischenschlüssel K_A dem Verwalter **82**, wenn er seine Ressourcen dem Verwalter B2 zuteilt. Außerdem bestimmt der Verwalter A den Bereichschlüssel #1000h des Verwalters B2 und gibt ihn dem Verwalter B2 zusammen mit seinem Bereichcode #0000h.

[0188] Demgemäss kann der Verwalter B2 den Bereichzwischenschlüssel K_A und seinen Bereichschlüssel #1000h erkennen, er kann jedoch nicht den Systemschlüssel und den Bereichschlüssel #0000h des als der Vater dienenden Verwalters A erkennen. Da jedoch der Bereichschlüssel #1000h des Verwalters B2 von dem als der Vater dienenden Verwalter A dem als das Kind dienenden Verwalter B2 gegeben wird, erkennt der als der Vater dienende Verwalter A den Bereichschlüssel #1000h des als das Kind dienenden Verwalters B2.

[0189] Der vom Verwalter A dem Verwalter B2 gegebene Bereichschlüssel #1000h wird bei der Bereich bildenden Verarbeitung des Bereich definierenden Bereichs #1000h des Verwalters B2 in seinen Bereich definierenden Bereich #1000h geschrieben.

[0190] Der Verwalter B2 verschlüsselt den vom als sein Vater dienenden Verwalter A erhaltenen Bereichzwischenschlüssel K_A auf der Basis des vom Verwalter A erhaltenen Bereichschlüssels #1000h, um einen Bereichzwischenschlüssel K_{B2} zu erzeugen.

[0191] Wenn andererseits der Verwalter B1 seine Ressourcen dem Verwalter C zuteilt, gibt der Verwalter B1 den Bereichzwischenschlüssel K_{B1} dem Verwalter C. Außerdem bestimmt der Verwalter B1 den Bereichschlüssel #0300h des Verwalters C und gibt ihn dem Verwalter C zusammen mit seinem Bereichcode #0100h und dem Bereichcode #0000h des als der Vater dienenden Verwalters A.

[0192] Demgemäss kann der Verwalter C den Bereichzwischenschlüssel K_{B1} und dessen Bereichschlüssel #03000h bzw. #0300h erkennen, er kann jedoch den Bereichschlüssel #0100h des als der Vater dienenden Verwalters B1 nicht erkennen. Da jedoch der Bereichschlüssel #0100h von dem als der Vater dienenden Verwalter B1 dem als Kind dienenden Verwalter C gegeben wird, erkennt der als der Vater dienende Verwalter B1 den Bereichschlüssel #0300h des als das Kind dienenden Verwalters C.

[0193] Der vom Verwalter B1 dem Verwalter C gegebene Bereichschlüssel #0300h wird durch die Bereichbildungsverarbeitung des Bereich definierenden Bereichs #0300h des Verwalters C in seinen Bereich definierenden Bereich #0300h geschrieben.

[0194] Der Verwalter C verschlüsselt den vom als der Vater dienenden Verwalter B1 erhaltenen Bereichzwischenschlüssel K_{B1} auf der Basis des vom Verwalter B1 erhaltenen Bereichschlüssels #0300h, um einen Bereichzwischenschlüssel K_C zu erzeugen.

[0195] Wenn der Verwalter A seine Dienste durch Benutzung des Dienstbereichs, der wie in Fig. 10 gezeigt durch den in der Schicht seines Bereich definierenden Bereichs #0000h gebildeten Dienst definierenden Bereich #0008h verwaltet wird, zuführt, verschlüsselt der Verwalter A den im Dienst definierenden Bereich #0008h gespeicherten Dienstschlüssel (der im Dienst definierenden Bereich #xxxxh gespeicherte Dienstschlüssel wird nachstehend als Dienstschlüssel #xxxxh bezeichnet) auf der Basis des Bereichzwischenschlüssels K_A, um einen Dienstzwischenschlüssel $K_{\#0008h}$ zu erzeugen, und registriert ihn in einer Dienstzuführmaschine **111** zusammen mit dem Bereichzwischenschlüssel K_A. Außerdem registriert der Verwalter A den Bereichcode 0000h seines Bereich definierenden Bereichs #0000h und den Dienstcode #0008h des in der Schicht des Bereich definierenden Bereichs #0000h gebildeten Dienst definierenden Bereichs #0008h in der Dienstzuführmaschine **111**.

[0196] Hier ist die Dienstzuführmaschine **111** beispielsweise aus dem R/W **1** und dem Kontroller **3**, die in Fig. 1 gezeigt sind, gebildet, und Daten werden von einem/in einen vorbestimmten Dienstbereich zum Zuführen eines vorbestimmten Dienstes gelesen/geschrieben.

[0197] Wenn in diesem Fall die IC-Karte **2** in die Dienstzuführmaschine **111** eingesetzt wird, wird die folgende gegenseitige Zertifizierung zwischen der Dienstzuführmaschine **111** und der IC-Karte **2** ausgeführt.

[0198] Das heißt, die wie in Fig. 11 gezeigte Dienstzuführmaschine **111** überträgt den Bereichcode #0000h und den Dienstcode #0008h, die in der IC-Karte **2** registriert sind. In der IC-Karte **2** (Sequenzer **91**) werden der Bereichcode #0000h und der Dienstcode #0008h von der Dienstzuführmaschine **111** empfangen.

[0199] In der IC-Karte **2** wird der im System definierende Block (Fig. 4) gespeicherte Systemschlüssel ausgelesen, und es wird auch der Bereichschlüssel #0000h von dem Bereich definierenden Bereich ausgelesen, der den von der Dienstzuführmaschine **111** empfangenen Bereichcode #0000h aufweist. Außerdem wird der Systemschlüssel auf der Basis des Bereichschlüssels #0000h verschlüsselt, so dass dieser Schlüssel als der in der Dienstzuführmaschine **111** der Fig. 10 registrierte Bereichzwischenschlüssel K_A erzeugt wird. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_A wird als ein zur Zertifizierung benutzter erster Zugriffschlüssel (Zertifizierungsschlüssel) K_{bc} gesetzt.

[0200] In der IC-Karte **2** wird der Dienstschlüssel #0008h vom Dienst definierenden Bereich, der den von der Dienstzuführmaschine **111** empfangenen Dienstcode #0008h aufweist, gelesen. Der Bereichzwischenschlüssel K_A wird auf der Basis des Dienstschlüssels #0008h verschlüsselt, so dass der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 10 registrierte Bereichzwischenschlüssel $K_{\#0008h}$ erzeugt wird. Der gleiche Schlüssel wie der Dienstzwischenschlüssel $K_{\#0008h}$ wird als ein zur Zertifizierung benutzter zweiter Zugriffsschlüssel K_{ac} gesetzt.

[0201] Demgemäss wird in diesem Fall in der Dienstzuführmaschine **111** der Bereichzwischenschlüssel K_A oder der Dienstzwischenschlüssel $K_{\#0008h}$, der als der erste Zugriffsschlüssel K_{bc} oder der zweite Zugriffsschlüssel K_{ac} dient, registriert, wo-

durch der Bereichzwischenschlüssel K_A oder der Dienstzwischenschlüssel $K_{\#0008h}$, der als der erste Zugriffsschlüssel K_{bc} oder der zweite Zugriffsschlüssel K_{ac} dient, in der IC-Karte **2** erzeugt.

[0202] Die Dienstzuführmaschine **111** zertifiziert beispielsweise die IC-Karte wie in Fig. 12 gezeigt.

[0203] Das heißt, in der Dienstzuführmaschine **111** wird eine Zufallszahl erzeugt, und sie wird entsprechend einem Algorithmus E1 umgesetzt. Das heißt, die Zufallszahl wird auf der Basis des zweiten Zugriffsschlüssels K_{ac} verschlüsselt (beispielsweise DES-verschlüsselt), und das Verschlüsselungsresultat wird auf der Basis des ersten Zugriffsschlüssels K_{bc} decodiert (beispielsweise DES-decodiert). Das Decodierungsresultat wird auf der Basis des zweiten Zugriffsschlüssels K_{ac} verschlüsselt. Das auf dem Algorithmus E1 basierende Umsetzungsresultat der Zufallszahl wird zur IC-Karte übertragen.

[0204] In der IC-Karte **2** wird das auf dem Algorithmus E1 basierende Umsetzungsresultat der Zufallszahl von der Diensteinrichtung **111** entsprechend dem Algorithmus D1 umgesetzt. Das heißt, das auf dem Algorithmus E1 basierende Umsetzungsresultat wird auf der Basis des zweiten Zugriffsschlüssels K_{ac} decodiert, und das Decodierungsresultat wird auf der Basis des ersten Zugriffsschlüssels K_{bc} verschlüsselt. Außerdem wird das Verschlüsselungsresultat auf der Basis des zweiten Schlüssels K_{ac} decodiert.

[0205] In der IC-Karte **2** wird das auf dem Algorithmus D1 basierende Umsetzungsresultat entsprechend dem Algorithmus E2 weiter umgesetzt. Das heißt, das auf dem Algorithmus D1 basierende Umsetzungsresultat wird auf der Basis des ersten Zugriffsschlüssels K_{bc} verschlüsselt, und der erste Zugriffsschlüssel K_{bc} wird auf der Basis des zweiten Zugriffsschlüssels K_{ac} verschlüsselt. Das auf dem ersten Zugriffsschlüssel K_{bc} für das auf dem Algorithmus D1 basierende Umsetzungsresultat basierende Verschlüsselungsresultat wird auf der Basis des auf dem zweiten Zugriffsschlüssels K_{ac} des ersten Zugriffsschlüssel K_{bc} basierenden Verschlüsselungsresultats decodiert. Das Decodierungsresultat wird auf der Basis des ersten Zugriffsschlüssels K_{bc} verschlüsselt und zur Dienstsuchmaschine **111** übertragen.

[0206] In der Dienstzuführmaschine **111** wird das auf dem Algorithmus E2 basierende Umsetzungsresultat von der IC-Karte **2** entsprechend dem Algorithmus D2 umgesetzt. Das heißt, das auf dem Algorithmus E2 basierende Umsetzungsresultat wird auf der Basis des ersten Zugriffsschlüssels K_{bc} decodiert, und der erste Zugriffsschlüssel K_{bc} wird auf der Basis des zweiten Zugriffsschlüssels K_{ac} verschlüsselt. Das auf dem ersten Zugriffsschlüssel K_{bc} für das auf dem Algorithmus E2 basierende Umsetzungsresultat basierende Decodierungsresultat wird auf der Basis des Verschlüsselungsresultats des auf dem zweiten Zugriffsschlüssel K_{ac} basierenden ersten Zugriffsschlüssels K_{bc} verschlüsselt.

[0207] In der Dienstzuführmaschine **111** werden die originale Zufallszahl und das auf dem Algorithmus D2 basierende Umsetzungsresultat miteinander verglichen, um die IC-Karte **2** zu zertifizieren. Das heißt, wenn die originale Zahl mit dem auf dem Algorithmus D2 basierenden Umsetzungsresultat koinzidiert, wird erkannt, dass die IC-Karte **2** richtig ist. Wenn sie andererseits nicht mit einander koinzident sind, wird die IC-Karte **2** als nicht richtig angesehen (ist sie beispielsweise gefälscht).

[0208] Wenn die IC-Karte **2** als richtig erkannt wird, wird die Zertifizierung des Dienstzuführmaschine **111** in der IC-Karte **2** beispielsweise wie in Fig. 13 gezeigt ausgeführt.

[0209] Das heißt, in der IC-Karte **2** wird die Zufallszahl erzeugt und die Zufallszahl entsprechend dem Algorithmus E2 umgesetzt und zur Dienstzuführmaschine **111** übertragen.

[0210] In der Dienstzuführmaschine **111** wird das auf dem Algorithmus E2 basierende Umsetzungsresultat der Zufallszahl von der IC-Karte **2** entsprechend dem Algorithmus D2 umgesetzt. Außerdem wird das auf dem Algorithmus D2 basierende Umsetzungsresultat entsprechend dem Algorithmus E1 umgesetzt und zur IC-Karte **2** übertragen.

[0211] In der IC-Karte **2** wird das auf dem Algorithmus E1 basierende Umsetzungsresultat von der Dienstzuführmaschine **111** entsprechend dem Algorithmus D1 umgesetzt, und das Umsetzungsresultat und die original Zufallszahl werden miteinander verglichen, um die Zertifizierung für die Dienstzuführmaschine **111** auszuführen. Das heißt, wenn die originale Zufallszahl mit dem auf dem Algorithmus D2 basierenden Umsetzungsresultat koinzidiert, wird die Dienstzuführmaschine **111** als richtig angesehen. Wenn sie andererseits nicht miteinander koinzident sind, wird die Dienstzuführmaschine **111** als nicht richtig (beispielsweise modifiziert) angesehen.

[0212] Wenn sowohl die IC-Karte **2** als auch die Dienstzuführmaschine **111** als richtig angesehen werden, wird in der IC-Karte **2** ein Zugriff nur auf den Dienstbereich, der von dem den von der Dienstzuführmaschine **111** übertragenen Dienstcode aufweisenden Dienst definierenden Bereich verwaltet wird, erlaubt. Demgemäss ist in dem in Bezug auf die Fig. 10 und Fig. 11 beschriebenen Fall ein Zugriff nur auf den vom Dienst definierenden Bereich #0008h verwalteten Dienstbereich möglich.

[0213] Das heißt, der Verwalter A, der den Bereichzwischenschlüssel K_A, den Bereichcode #0000h, den

Dienstschlüssel #0008h und den Dienstcode #0008h kennt, kann auf den vom Dienst definierenden Bereich #0008h verwalteten Dienstbereich zugreifen. Jedoch kennt der Verwalter A weder den Dienstschlüssel #1022h noch den Dienstschlüssel #030Ch, so dass er grundsätzlich nicht auf den vom Dienst definierenden Bereich #1022h oder #030Ch verwalteten Dienstbereich zugreifen kann.

[0214] Wenn als nächstes der Verwalter B2 seine Dienste durch Benutzung des Dienstbereichs, der von dem in der Schicht seines Bereich definierenden Bereichs #1000h ausgebildeten Dienst definierenden Bereich #1022h verwaltet wird, zuführt, verschlüsselt er den im Dienst definierenden Bereich #1022h auf der Basis des wie in Fig. 14 gezeigten Bereichzwischenschlüssels K_{B2} gespeicherten Dienstschlüssel #1022h, um einen Dienstzwischenschlüssel $K_{\#1022h}$ zu erzeugen, und registriert ihn zusammen mit dem Bereichzwischenschlüssel K_{B2} in der Dienstzuführmaschine **111**. Der Verwalter B2 registriert in der Dienstzuführmaschine **111** den Bereichcode des Bereich definierenden Bereichs einer oberen Schicht über der Schicht seines Bereichs definierenden Bereichs #1000h, das heißt in diesem Fall, den Bereichcode #0000h des Bereich definierenden Bereichs #0000h des Verwalters A und den Bereichcode #1000h seines Bereich definierenden Bereichs #1000h und den Dienstcode #1022h des in der Schicht des Bereich definierenden Bereichs #1000h gebildeten Dienst definierenden Bereichs #1022h.

[0215] Wenn in diesem Fall die IC-Karte **2** in die Dienstzuführmaschine **111** eingesetzt wird, wird die folgende gegenseitige Zertifizierung zwischen der Dienstzuführmaschine **111** und der IC-Karte **2** ausgeführt.

[0216] Das heißt, die Dienstzuführmaschine **111** überträgt, wie in Fig. 15 gezeigt, die registrierten Bereichcodes #0000h und #1000h und den Dienstcode #1022h zur IC-Karte **2**. In der IC-Karte **2** (Sequenzer **91**) werden die Bereichcodes #0000h und #1000h und der Dienstcode #1022h von der Dienstzuführmaschine **111** empfangen.

[0217] In der IC-Karte **2** wird der im System definierenden Block (Fig. 4) gespeicherte Systemschlüssel ausgelesen, und der Bereichschlüssel #0000h oder #1000h wird von dem Bereich definierenden Bereich, der den von der Dienstzuführmaschine **111** empfangenen Bereichcode #0000h oder #1000h aufweist, ausgelesen. Außerdem wird der Systemschlüssel auf der Basis des Bereichschlüssels #0000h verschlüsselt, so dass der gleiche Schlüssel wie der Bereichzwischenschlüssel K_A erzeugt wird. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_A wird auf der Basis des Bereichschlüssels #1000h verschlüsselt, so dass der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 4 registrierte Bereichzwischenschlüssel K_{B2} erzeugt wird. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_{B2} wird als ein zum Zertifizieren benutzter erster Zugriffschlüssel K_{bc} gesetzt.

[0218] In der IC-Karte **2** wird der Dienstschlüssel #1022h von dem Dienst definierenden Bereich, der den von der Dienstzuführmaschine **111** empfangenen Dienstcode #1022h aufweist, ausgelesen. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_{B2} wird auf der Basis des Dienstschlüssels #1022h verschlüsselt, so dass der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 14 registrierte Dienstzwischenschlüssel $K_{\#1022h}$ erzeugt wird. Der gleiche Schlüssel wie der Dienstzwischenschlüssel $K_{\#1022h}$ wird als ein zum Zertifizieren benutzter zweiter Zugriffsschlüssel K_{ac} gesetzt.

[0219] Demgemäss wird in diesem Fall in der Dienstzuführmaschine **111** der Bereichzwischenschlüssel K_{B2} oder der Dienstzwischenschlüssel $K_{\#1022h}$, welcher der erste Zugriffschlüssel K_{bc} oder der zweite Zugriffschlüssel K_{ac} ist, registriert, und in der IC-Karte **2** wird der Bereichzwischenschlüssel K_{B2} oder der Dienstzwischenschlüssel $K_{\#1022h}$, welcher der erste Zugriffschlüssel K_{bc} oder der zweite Zugriffschlüssel K_{ac} ist, erzeugt.

[0220] Die gegenseitige Zertifizierung wird zwischen der IC-Karte **2** und der Dienstzuführmaschine **111** wie in dem unter Bezugnahme auf die Fig. 12 und Fig. 13 beschriebenen Fall ausgeführt.

[0221] Als Resultat der gegenseitigen Zertifizierung wird in der IC-Karte **2**, wenn sowohl die IC-Karte **2** als auch die Dienstzuführmaschine **111** als richtig erkannt werden, der Zugriff nur auf den Dienstbereich, der vom Dienst definierenden Bereich, welcher den von der Dienstzuführmaschine **111** übertragenen Dienstcode aufweist, verwaltet wird, erlaubt. Demgemäss ist im Fall der Fig. 14 und Fig. 15 der Zugriff nur auf den Dienstbereich, der vom Dienst definierenden Bereich #1022h verwaltet wird, möglich.

[0222] Das heißt, der Verwalter B2 der den Bereichzwischenschlüssel K_{b2}, die Bereichcodes #0000h, #1000h, den Dienstschlüssel #1022h und den Dienstcode #1022h kennt, kann auf den vom Dienst definierenden Bereich #1022h verwalteten Dienstbereich zugreifen. Jedoch kennt der Verwalter B2 weder den Dienstschlüssel #0008h noch #030Ch, und so kann er grundsätzlich nicht auf den von den Dienst definierenden Bereichen #0008h und #030Ch verwalteten Dienstbereich zugreifen.

[0223] Wenn als nächstes der Verwalter C die Dienste unter Benutzung des Dienstbereich, der von dem in der Schicht seines Bereich definierenden Bereichs #0300h gebildeten Dienst definierenden Bereichs #030Ch verwaltet wird, zuführt, verschlüsselt

er wie in Fig. 16 gezeigt den im Dienst definierenden Bereich #030Ch gespeicherten Dienstschlüssel #030Ch auf der Basis des Bereichzwischenschlüssels K_C, um einen Dienstzwischenschlüssel $K_{\#030Ch}$ zu erzeugen, und registriert ihn zusammen mit dem Bereichzwischenschlüssels K_C in der Dienstzuführmaschine **111**. Der Verwalter C registriert auch in der Dienstzuführmaschine **111** den Bereichcode des Bereich definierenden Bereichs einer oberen Schicht über der Schicht seines Bereich definierenden Bereichs #0300h, das heißt in diesem Fall den Bereichcode #0000h des Bereich definierenden Bereichs #0000h des Verwalters A, den Bereichcode 0100h des Bereich definierenden Bereichs #0100h des Verwalters B1, den Bereichcode #0300h seines Bereich definierenden Bereichs #0300h und den Dienstcode #030Ch des in der Schicht des Bereich definierenden Bereichs #0300h gebildeten Dienst definierenden Bereichs #030Ch.

[0224] Wenn in diesem Fall die IC-Karte **2** in die Dienstzuführmaschine **111** eingesetzt wird, wird die folgende gegenseitige Zertifizierung zwischen der Dienstzuführmaschine **111** und der IC-Karte **2** ausgeführt.

[0225] Das heißt, es werden, wie in der Fig. 17 gezeigt, die registrierten Bereichcodes #0000h, #0100h und #0300h und der Dienstcode #030Ch zur IC-Karte **2** übertragen. In der IC-Karte **2** (Sequenzer **91**) werden die Bereichcodes #0000h, #0100h und #0300h und der Dienstcode #030Ch von der Dienstzuführmaschine **111** empfangen.

[0226] In der IC-Karte **2** wird der im System definierenden Block (Fig. 4) gespeicherte Systemschlüssel ausgelesen, und es wird auch der Bereichschlüssel #0000h, #0100h oder #0300h von dem Bereich definierenden Bereich, der den von der Dienstzufuhreinrichtung **111** empfangenen Bereichcode #0000h, #0100h oder #0300h aufweist, ausgelesen. Außerdem wird der Systemschlüssel auf der Basis des Bereichschlüssels #0000h verschlüsselt, so dass der gleiche Schlüssel wie der Bereichzwischenschlüssel K_A erzeugt wird. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_A wird auf der Basis des Bereichschlüssels #0100h verschlüsselt, so dass der gleiche Schlüssel wie der Bereichzwischenschlüssel K_{B1} erzeugt wird. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_{B1} wird auf der Basis des Bereichschlüssels #0300h verschlüsselt, so dass der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 16 registrierte Bereichzwischenschlüssel K_C erzeugt wird. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_C wird als ein zum Zertifizieren benutzter erster Zugriffsschlüssel K_{bc} gesetzt.

[0227] In der IC-Karte **2** wird der Dienstschlüssel #030Ch vom Dienst definierenden Bereich, der den von der Dienstzuführmaschine **111** empfangenen Dienstcode #030Ch aufweist, ausgelesen. Der Bereichzwischenschlüssel K_C wird auf der Basis des Dienstschlüssels #030Ch verschlüsselt, wobei der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 16 registrierte Dienstzwischenschlüssel $K_{\#030Ch}$ erzeugt wird. Der gleiche Schlüssel wie der Dienstzwischenschlüssel $K_{\#030Ch}$ wird als ein zum Zertifizieren benutzter zweiter Zugriffsschlüssel K_{ac} gesetzt.

[0228] Demgemäss wird im vorstehenden Fall der Bereichzwischenschlüssel K_C oder der Dienstzwischenschlüssel $K_{\#030Ch}$, welcher der erste Zugriffsschlüssel K_{bc} oder der zweite Zugriffsschlüssel K_{ac} ist, in der Dienstzuführmaschine **111** registriert, und in der IC-Karte **2** wird der Bereichzwischenschlüssel K_C oder der Dienstzwischenschlüssel $K_{\#030Ch}$, welcher der erste Zugriffsschlüssel K_{bc} oder der zweite Zugriffsschlüssel K_{ac} ist, erzeugt.

[0229] Die gegenseitige Zertifizierung wird zwischen der IC-Karte **2** und der Dienstzuführmaschine **111** wie im Fall der Fig. 12 und Fig. 13 ausgeführt.

[0230] Als Resultat der gegenseitigen Zertifizierung ist bei der IC-Karte **2**, wenn sowohl die IC-Karte **2** als auch die Dienstzuführmaschine als richtig erkannt werden, ein Zugriff nur auf den vom Dienst definierenden Bereich, der den von der Dienstzuführmaschine **111** übertragenen Dienstcode aufweist, verwalteten Dienstbereich erlaubt. Demgemäss ist im Fall der Fig. 16 und Fig. 17 der Zugriff nur auf den vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereich möglich.

[0231] Das heißt, der Verwalter C, der den Bereichzwischenschlüssel K_C, die Bereichcodes #0000h, #0100h, #0300h, den Dienstschlüssel #030Ch und den Dienstcode #030Ch kennt, kann auf den vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereich zugreifen. Jedoch kennt der Verwalter C weder den Dienstschlüssel #0008h noch den Dienstschlüssel #1022Ch, und er kann grundsätzlich nicht auf den vom Dienst definierenden Bereich #0008h oder #1022Ch verwalteten Dienstbereich zugreifen.

[0232] Wie vorstehend beschrieben kann der Verwalter auf seinen Dienstbereich zugreifen, selbst wenn er den Bereichschlüssel der oberen Schicht nicht kennt.

[0233] Wie vorstehend beschrieben kann jeder Verwalter auf keinen Dienstbereich, der von einem Dienst definierenden Bereich, für den der Verwalter nicht den Dienstschlüssel hat, verwaltet wird, zugreifen. Jedoch gibt es beispielsweise den Fall, bei dem der Verwalter C wünscht, nicht nur Dienste unter Benutzung des von seinem Dienst definierenden Be-

reich #030Ch verwalteten Dienstbereichs, sondern auch Dienste unter Verwendung des vom Dienst definierenden Bereich #1022h des Verwalters B verwalteten Dienstbereichs auszuführen.

[0234] Damit in diesem Fall der Verwalter C auf den vom Dienst definierenden Bereich #1022h verwalteten Dienstbereich zugreifen kann, ist es für den Verwalter C notwendig, den Bereichzwischenschlüssel K_{B2}, die Bereichcodes #0000h, #1000h, den Dienstschlüssel #1022h und den Dienstcode #1022h wie unter Bezugnahme auf die Fig. 14 und Fig. 15 beschrieben zu kennen. Demgemäss ist es notwendig, diese Information vom Verwalter B2 zu gewinnen.

[0235] Jedoch ist der dem Verwalter B2 bekannte Dienstschlüssel #1022h selbst dem als der Vater des Verwalters B2 dienenden Verwalter A nicht bekannt, und infolgedessen ist es vom Gesichtspunkt der Sicherheit nicht vorteilhaft, dass der Dienstschlüssel #1022h, der nur dem Verwalter B2 bekannt sein kann, dem Verwalter C mitgeteilt wird.

[0236] Selbst wenn in diesem Fall das Sicherheitsproblem vernachlässigt wird, ist es, damit der Verwalter C auf beide der vom Dienst definierenden Bereich #030Ch bzw. #1022h verwalteten zwei Dienstbereiche zugreifen kann, notwendig, die in Fig. 15 gezeigte Verarbeitung in der IC-Karte **2** auszuführen, um den ersten Zugriffschlüssel K_{bc} und den zweiten Zugriffschlüssel K_{ac} zu erzeugen, und eine gegenseitige Zertifizierung für einen Zugriff auf den vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereich auszuführen, und auch die in Fig. 17 gezeigte Verarbeitung auszuführen, um den ersten Zugriffschlüssel K_{bc} und den zweiten Zugriffschlüssel K_{ac} zu erzeugen, und eine gegenseitige Zertifizierung für einen Zugriff auf den vom Dienst definierenden Bereich #1022h verwalteten Dienstbereich auszuführen.

[0237] Wenn demgemäss die gegenseitige Zertifizierung für einen Zugriff auf einen Dienstbereich bei jedem Dienstbereich ausgeführt wird, ist es schwierig, schnell auf den Dienstbereich zuzugreifen. Als Resultat ist es, wenn das Kartensystem der Fig. 1 zur Prüfung von Fahrkarten in einem Bahnhof angewendet wird, schwierig, auf einen vorbestimmten Dienstbereich der IC-Karte **2** zuzugreifen und während einer relativ kurzen Dauer, in der ein Pendler durch einen bei einer Kartensperre vorgesehenen Durchgang geht, zu schreiben oder zu lesen.

[0238] Deshalb wird in dem Fall, bei dem der Verwalter C nicht nur Dienste unter Verwendung des von seinem Dienst definierenden Bereich #030Ch verwalteten Dienstbereichs, sondern auch Dienste unter Verwendung des vom Dienst definierenden Bereich #1022h des Verwalters B2 verwalteten Dienstbereichs zuführt, zum Lösen des Sicherheitsproblems und zur Sicherstellung eines schnellen Zugriffs auf den Dienstbereich eine wie in Fig. 18 gezeigte Informationsabgabe zwischen den Verwaltern C und B2 ausgeführt und in der Dienstzuführmaschine **111** registriert.

[0239] Das heißt, der Verwalter C verschlüsselt wie im Fall der Fig. 16 den im Dienst definierenden Bereich #030Ch auf der Basis des Bereichzwischenschlüssels K_C gespeicherten Dienstschlüssel #030Ch, um den Dienstzwischenschlüssel $K_{\#030Ch}$ zu erzeugen. Außerdem gibt der Verwalter C den Dienstzwischenschlüssel $K_{\#030Ch}$ an den Verwalter B2 ab, um ihn auf der Basis des Dienstschlüssels #1022h zu verschlüsseln. Der Verwalter C empfängt den Dienstzwischenschlüssel $K_{\#1022h}$, der ein Verschlüsselungsresultat des Dienstzwischenschlüssels $K_{\#030Ch}$ auf der Basis des Dienstschlüssels #1022h ist, zusammen mit dem Dienstcode #1022h.

[0240] Demgemäss werden nur die Dienstzwischenschlüssel $K_{\#030Ch}$ und $K_{\#1022h}$ zwischen den Verwaltern C und B2 abgegeben, und es gibt weder den Fall, bei dem der nur dem Verwalter C bekannte Dienstschlüssel #030Ch dem Verwalter B2 bekannt ist, noch den Fall, bei dem der nur dem Verwalter B2 bekannte Dienstschlüssel #1022h dem Verwalter C bekannt ist. Das heißt, es gibt kein Problem bei der Sicherheit.

[0241] Der Verwalter C, der den Dienstzwischenschlüssel $K_{\#1022h}$ und den Dienstcode #1022h vom Verwalter B2 empfängt, registriert in der Dienstzuführmaschine **111** die Bereichcodes der Bereich definierenden Bereiche in oberen Schichten über der Schicht seines Bereich definierenden Bereichs #0300h, das heißt in diesem Fall den Bereichcode #0000h des Bereich definierenden Bereichs #0000h des Verwalters A, den Bereichcode 0100h des Bereich definierenden Bereichs #0100h des Verwalters B1 und den Bereichcode #0300h des Bereich definierenden Bereichs #0300h des Verwalters C. Außerdem registriert der Verwalter C in der Dienstzuführmaschine **111** den Bereichzwischenschlüssel K_C und den Dienstcode #030Ch des in der Schicht des Bereich definierenden Bereichs #0300h gebildeten Dienst definierenden Bereichs #030Ch.

[0242] Wenn in diesem Fall die Dienstzuführmaschine **111** in die IC-Karte **2** eingesetzt wird, wird die folgende gegenseitige Zertifizierung zwischen der Dienstzuführmaschine **111** und der IC-Karte **2** ausgeführt.

[0243] Das heißt, die Dienstzuführmaschine **111** überträgt, wie in Fig. 19 gezeigt, zur IC-Karte **2** die registrierten Bereichcodes #0000h, #0100h und #0300h und die Dienstcodes #030Ch und #1022h. Von der Dienstzuführmaschine **111** werden die Bereichcodes #0000h, #0100h und #0300h und die Dienstcodes #030Ch und #1022h in der IC-Karte **2**

(Sequenzer **91**) erhalten.

[0244] In der IC-Karte **2** wird der im System definierenden Block (Fig. 4) gespeicherte Systemschlüssel ausgelesen, und der Bereichschlüssel #0000h, #0100h oder #0300h wird von dem Bereich definierenden Bereich, der den Bereichcode #0000h, #0100h oder #0300h, die von der Dienstzufuhreinrichtung **111** empfangen werden, aufweist, ausgelesen, und der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 18 registrierte Bereichzwischenschlüssel K_C wird wie im Fall der Fig. 17 erzeugt. Der gleiche Schlüssel wie der Bereichzwischenschlüssel K_C wird als ein zur Zertifizierung benutzter erster Zugriffschlüssel K_{bc} gesetzt.

[0245] In der IC-Karte **2** wird der Dienstschlüssel #030Ch oder #1022h von dem Dienst definierenden Bereich, der den von Dienstzuführmaschine **111** empfangenen Dienstcode #030Ch bzw. #1022h aufweist, ausgelesen. Der Bereichzwischenschlüssel K_C wird auf der Basis des Dienstschlüssels #030Ch verschlüsselt und als ein Resultat des gleichen Schlüssels wie der Dienstzwischenschlüssel $K_{\#030Ch}$ erzeugt. Außerdem wird der gleiche Schlüssel wie der Dienstzwischenschlüssel $K_{\#030Ch}$ auf der Basis des Dienstschlüssels #1022h verschlüsselt, und es wird der gleiche Schlüssel wie der in der Dienstzuführmaschine **111** der Fig. 18 registrierte Dienstzwischenschlüssel $K_{\#1022h}$ erzeugt. Der gleiche Schlüssel wie der Dienstzwischenschlüssel $K_{\#1022h}$ wird als ein zur Zertifizierung benutzter zweiter Zugriffschlüssel K_{ac} gesetzt.

[0246] Demgemäss wird im vorstehenden Fall in der Dienstzuführmaschine **111** der Bereichzwischenschlüssel K_C oder der Dienstzwischenschlüssel $K_{\#1022h}$, welcher der erste Zugriffschlüssel K_{bc} oder der zweite Zugriffschlüssel K_{ac} ist, registriert, und der Bereichzwischenschlüssel K_C oder der Dienstzwischenschlüssel $K_{\#1022}$ welcher der erste Zugriffschlüssel K_{bc} oder der zweite Zugriffschlüssel K_{ac} ist, in der IC-Karte **2** erzeugt.

[0247] Die gegenseitige Zertifizierung wird zwischen der IC-Karte und der Dienstzuführmaschine **111** wie im Fall der Fig. 12 und Fig. 13 ausgeführt.

[0248] Wenn sowohl die IC-Karte als auch die Dienstzuführmaschine **111** als richtig entschieden werden, ist als ein Resultat der gegenseitigen Zertifizierung in der IC-Karte **2** ein Zugriff nur auf den vom Dienst definierenden Bereich, der den von der Dienstzuführmaschine **111** übertragenen Dienstcode aufweist, verwalteten Dienstbereich erlaubt. Demgemäss ist im Fall der Fig. 18 und Fig. 19 der Zugriff auf den vom Dienst definierenden Bereich #030Ch verwalteten Dienstbereich und den vom Dienst definierenden Bereich #1022Ch verwalteten Dienstbereich erlaubt.

[0249] Wie vorstehend beschrieben werden durch Verschlüsselung des Systemschlüssels auf der Basis der zwei oder mehreren Bereichschlüssel oder Dienstschlüssel die zwei oder mehreren Bereichschlüssel oder Dienstschlüssel in die zwei Schlüssel des ersten Zugriffschlüssels K_{bc} und des zweiten Zugriffschlüssels K_{ac} degeneriert (zusammengesetzt), und die gegenseitige Zertifizierung zum Ermöglichen des Zugriffs auf den vom Dienst definierenden Bereich, der den von der Dienstzuführmaschine **111** übertragenen Dienstcode aufweist, verwalteten Dienstbereich wird durch Benutzung des ersten Zugriffschlüssels K_{bc} und des zweiten Zugriffschlüssels K_{ac} ausgeführt. Selbst wenn deshalb der Zugriff auf mehrere Dienst definierende Bereiche angezielt wird, kann die gegenseitige Zertifizierung in kurzer Zeit vollendet werden, wodurch ein schneller Zugriff auf den Dienstbereich gesichert ist.

[0250] Im Fall der Fig. 12 und Fig. 13 wird die gegenseitige Zertifizierungsverarbeitung durch Benutzung der zwei Schlüssel des ersten Zugriffschlüssels K_{bc} und des zweiten Zugriffschlüssels K_{ac} ausgeführt, jedoch ist es möglich, die gegenseitige Zertifizierungsverarbeitung beispielsweise durch Benutzung nur des zweiten Zugriffschlüssels K_{ac} auszuführen. In diesem Fall werden in der IC-Karte **2** die zwei oder mehreren Bereichschlüssel oder Dienstschlüssel durch Verschlüsselung des Systemschlüssels auf der Basis der zwei oder mehreren Bereichschlüssel oder Dienstschlüssel in einen einzelnen zweiten Zugriffschlüssel K_{ac} degeneriert.

[0251] Außerdem ist es, wie in Fig. 20 gezeigt, möglich, ein beispielsweise durch Verschlüsselung des ersten Zugriffschlüssels K_{bc} und des zweiten Zugriffschlüssels K_{ac} auf der Basis einer Herstellungs-ID, die im Herstellungs-ID-Block gespeichert ist und bei der IC-Karte **2** ein inhärenter Wert ist, erhaltenes Verschlüsselungsresultat zu benutzen. Hier, bei der Fig. 20, wird in Bezug auf den ersten Zugriffschlüssel K_{bc} die Verschlüsselung durch Unterwerfen des ersten Zugriffschlüssels K_{bc} und der Herstellungs-ID einem EXOR (exlusives 0der) ausgeführt. In Bezug auf den zweiten Zugriffschlüssel K_{ac} wird die Verschlüsselung auf der Basis des DES-Systems ausgeführt. In Bezug auf den zweiten Zugriffschlüssel K_{ac} kann die auf dem DES-System basierende Verschlüsselung durch Benutzung des EXOR-Resultats des ersten Zugriffschlüssels K_{bc} und der Herstellungs-ID als ein Schlüssel ausgeführt werden.

[0252] Wie vorstehend beschrieben kann, wenn das durch Verschlüsselung des ersten Zugriffschlüssels K_{bc} und zweiten Zugriffschlüssels K_{ac} erhaltene Verschlüsselungsresultat zur gegenseitigen Zertifizierung benutzt wird, die Sicherheit noch weiter verbessert werden. In diesem Fall ist die Herstellungs-ID in der Dienstzuführmaschine **111** notwendig, und sie kann von der IC-Karte **2** übertragen werden.

[0253] Als nächstes weist der Speicherbereich des EEPROM **66** eine geschichtete Struktur auf, in welcher der Bereich definierende Bereich geschichtet ist, und jeder Bereich definierende Bereich und jeder Dienst definierende Bereich ist so ausgebildet, dass er einen Bereichschlüssel und einen Dienstschlüssel zur Zertifizierung speichert. Als Resultat kann die folgende Zugriffsteuerung ausgeführt werden.

[0254] Das heißt, wenn ein Verwalter als ein Vaterverwalter dient und eine Dienstzufuhr durch einen Kindverwalter, dem eine Ressource des Verwalters zugeteilt ist, zu stoppen wünscht, weil der Kindverwalter einen unrechten Dienst macht, kann der Verwalter durch Änderung des im Bereich definierenden Bereich gespeicherten Bereichschlüssels den Kindverwalter vom Zugriff auf die IC-Karte **2** abhalten.

[0255] Insbesondere wenn beispielsweise der Verwalter B1 die Dienstzufuhr des Verwalters C in Fig. 5 stoppt, ändert der Verwalter B1 den im Bereich definierenden Bereich #0100h der IC-Karte **2** gespeicherten Bereichschlüssel #0100h. In diesem Fall werden der in der IC-Karte **2** gebildete Bereichzwischenschlüssel K_{B1} und außerdem der Bereichzwischenschlüssel K_C in Fig. 14 ebenfalls geändert, so dass der Verwalter C, der vor der Änderung nur den Bereichzwischenschlüssel K_C kennt, nicht auf den Dienst definierenden Bereich #030Ch zugreifen kann.

[0256] Der Verwalter A, welcher der Vaterverwalter des als Vaterverwalter des Verwalters C dienenden Verwalters B1 ist, kann den im Bereich definierenden Bereich #0000h gespeicherten Bereichschlüssel #0000h ändern, um den Zugriff auf den Dienst definierenden Bereich #030Ch zu verhindern. Jedoch kann in diesem Fall der Verwalter B2, der ein Kind des Verwalters A ist, nicht auf den vom Dienst definierenden Bereich #1022h des Verwalters B2 verwalteten Dienstbereich zugreifen. Das heißt, wenn ein Verwalter seinen Bereichschlüssel ändert, ist es nicht möglich, auf Dienst definierende Bereiche zuzugreifen, die von Bereich definierenden Bereichen in Schichten (Kindschicht, Enkelkindschicht, ...) des mit dem Bereichschlüssel korrespondierenden Bereich definierenden Bereichs verwaltet werden.

[0257] Bei den Fig. 18 und Fig. 19 benutzt der Verwalter C den Dienst definierenden Bereich #1022h (den von ihm verwalteten Dienstbereich) des Verwalters B2 gemeinsam mit dem Verwalter B2. Jedoch ist eine kompliziertere gemeinsame Benutzung des Dienst definierenden Bereichs zwischen Verwaltern für gewisse Typen von Schlüsselverwaltung möglich.

[0258] Insbesondere sei beispielsweise angenommen, dass eine in Fig. 21 gezeigte Schichtstruktur im EEPROM **66** ausgebildet ist. Das heißt, in Fig. 21 sind ein Bereich definierender Bereich #5000h eines Verwalters E und ein Bereich definierender Bereich #7000h eines Verwalters G als Kindschichten der Schicht des Bereich definierender Bereichs #0000h des als einen Herausgeber der IC-Karte **2** dienenden Verwalters A gebildet. Außerdem sind in der Schicht des Bereich definierender Bereichs #5000h des Verwalters E die Dienst definierende Bereiche #5008h, #5048h, #5088h und #50C8h ausgebildet, und es ist ein Bereich definierender Bereich #6000h eines Verwalters F gebildet.

[0259] Außerdem sind in der Schicht des Bereich definierenden Bereich #6000h des Verwalters F die Dienst definierenden Bereiche #6008h und #6048h ausgebildet, und in der Schicht des Bereich definierenden Bereichs #7000h des Verwalters G sind die Dienst definierenden Bereiche #7008h und #70C8h ausgebildet.

[0260] Bei der vorstehend erwähnten Schichtstruktur verschlüsselt der Verwalter A den Systemschlüssel auf der Basis des Bereichschlüssels #0000h wie bei (A) der Fig. 22 gezeigt, und gibt das Verschlüsselungsresultat an die als die Kindverwalter dienenden Verwalter E und G ab.

[0261] Wie bei (B) der Fig. 22 gezeigt, verschlüsselt der Verwalter E auf der Basis des Bereichschlüssels #5000h das Verschlüsselungsresultat des Systemschlüssels auf der Basis des Bereichschlüssels #0000h des Verwalters A und benutzt das Resultat als einen ersten Zugriffschlüssel K_{E1}. Außerdem verschlüsselt der Verwalter E den ersten Zugriffschlüssel K_{E1} (das Verschlüsselungsresultat auf der Basis des Bereichschlüssels #5000h) sukzessive auf der Basis jedes der Dienstschlüssel #5008h, #5048h, #5088h und #50C8h und benutzt das Verschlüsselungsendresultat als einen zweiten Zugriffschlüssel K_{E2}.

[0262] Wie bei (C) der Fig. 22 gezeigt, wird dem Verwalter F vom Verwalter E der erste Zugriffschlüssel K_{E1} (das Verschlüsselungsresultat auf der Basis des Bereichschlüssels #5000h) zugeführt, verschlüsselt es der Verwalter F auf der Basis des Bereichschlüssels #6000h, und setzt der Verwalter F das Verschlüsselungsresultat als einen ersten Zugriffschlüssel K_{F1}. Außerdem verschlüsselt der Verwalter F den ersten Zugriffschlüssel K_{F1} (das Verschlüsselungsresultat auf der Basis des Bereichschlüssels #6000h) sukzessive auf der Basis jedes der Dienstschlüssel #6008h und #6048h und gibt das Verschlüsselungsresultat an den Verwalter E ab, um es sukzessive auf der Basis jedes der Dienstschlüssel #5048h und #5088h zu verschlüsseln. Danach wird dem Verwalter F das Verschlüsselungsresultat des Verwalters E zugeführt, und er gibt es an den Verwalter G ab, um es auf der Basis des Dienstschlüssels #70C8h zu verschlüsseln. Dem Verwalter F wird das Verschlüsselungsresultat des Verwalters G zuge-

führt, und er benutzt es als einen zweiten Zugriffschlüssel KF2.

[0263] Wie bei (D) der Fig. 22 gezeigt verschlüsselt der Verwalter G das Verschlüsselungsresultat des Systemschlüssels auf der Basis des Bereichschlüssels #0000h vom Verwalter A auf der Basis des Bereichschlüssels #7000h und benutzt das Verschlüsselungsresultat als einen ersten Zugriffschlüssel K_{G1}. Außerdem verschlüsselt der Verwalter G den ersten Zugriffschlüssel K_{G1} (das Verschlüsselungsresultat auf der Basis des Bereichschlüssels #7000h) sukzessive auf der Basis jedes der Dienstschlüssel #7008h und #70C8h und gibt das Verschlüsselungsendresultat an den Verwalter F ab, um es auf der Basis des Dienstschlüssels #6048h zu verschlüsseln. Danach gibt der Verwalter G das Verschlüsselungsresultat unter Benutzung des Dienstschlüssels #6048h vom Verwalter F an den Verwalter E ab, um das Verschlüsselungsresultat sukzessive auf der Basis jedes der Dienstschlüssel #5088h und #50C8h zu verschlüsseln. Dem Verwalter G wird das Verschlüsselungsresultat vom Verwalter E zugeführt, und er benutzt es als einen zweiten Zugriffschlüssel K_{G2}.

[0264] In diesem Fall wird in der IC-Karte **2** der Systemschlüssel durch Benutzung des Bereichschlüssels und des Dienstschlüssels, die im EEPROM **66** gespeichert sind, entsprechend der gleichen Prozedur wie im Fall der Fig. 22 verschlüsselt, um den ersten Zugriffschlüssel und den zweiten Zugriffschlüssel zu erzeugen, wodurch die gemeinsame Benutzung des wie in Fig. 23 gezeigten Dienst definierenden Bereichs zwischen den Verwaltern E, F und G gegenseitig ausgeführt werden kann.

[0265] Das heißt, der Verwalter E kann nur auf seine Dienst definierenden Bereiche #5008h, #5048h, #5088h und #50C8h zugreifen. Der Verwalter F kann nicht nur auf seine Dienst definierenden Bereiche #6008h und #6048h zugreifen, sondern auch auf die Dienst definierenden Bereiche #5048h und #5088h des Verwalters E und den Dienst definierenden Bereich #70C8h des Verwalters G zugreifen. Der Verwalter G kann nicht nur auf seine Dienst definierenden Bereiche #7008h und #70C8h, sondern auch auf die Dienst definierenden Bereiche #5088h und #50C8h des Verwalters E und den Dienst definierenden Bereich #6048h des Verwalters F zugreifen.

[0266] Bei der wie in Fig. 22 gezeigten Schlüsselabgabe gibt es keinen Fall, bei dem der Dienstschlüssel selbst eines Verwalters einem anderen Verwalter bekannt ist. Das heißt die Dienstschlüssel #50008h, #5048h, #5088h, #50C8h des Verwalters E sind nicht nur beim Verwalter A bei den Verwaltern F und G niemals bekannt. Ähnlich sind die Dienstschlüssel #6008h und #6048h des Verwalters F bei den Verwaltern E und G niemals bekannt, und die Dienstschlüssel #7008h und #70C8h des Verwalters G sind bei den Verwaltern E und F niemals bekannt.

[0267] Außerdem ist es, wie vorstehend beschrieben, wenn gewisse Verwalter ihren Bereichschlüssel ändern, nicht möglich, auf alle vom Bereich definierenden Bereich der Schicht in der Schicht des Bereich definierenden Bereichs verwalteten Dienst definierenden Bereiche zuzugreifen, das heißt, wenn der Vaterverwalter den Bereichschlüssel ändert, kann der Kindverwalter nicht auf die IC-Karte zugreifen. Jedoch entsprechend einem spezifischen Schlüsselverwaltungverfahren kann ein Zugriff eines spezifischen Kindverwalters verhindert werden.

[0268] Insbesondere sei beispielsweise angenommen, dass eine Schichtstruktur im EEPROM **66** wie in Fig. 24 gezeigt ausgebildet ist. Das heißt, bei der Fig. 24 sind ein Bereich definierender Bereich #8000h eines Verwalters H ein Bereich definierender Bereich #9000h eines Verwalter I und ein Bereich definierender Bereich #A000h eines Verwalter J als Kindschichten der Schicht des Bereichs definierender Bereichs #0000h des als der Ausgeber der IC-Karte **2** dienenden Verwalters A ausgebildet. Außerdem sind die Dienst definierenden Bereiche #8008h, #8104h und #8105h in der Schicht des Bereich definierenden Bereichs #8000h des Verwalters H ausgebildet.

[0269] Bei der vorstehenden Schichtstruktur verschlüsselt der Verwalter A, wie bei (A) der Fig. 25 gezeigt, den Systemschlüssel auf der Basis des Bereichsschlüssels #0000h und gibt das Verschlüsselungsresultat an die als seine Kindverwalter dienenden Verwalter I und J ab.

[0270] Wie bei (C) der Fig. 25 gezeigt, verschlüsselt der Verwalter I das Verschlüsselungsresultat des Systemschlüssels auf der Basis des Bereichschlüssels #0000h des Verwalters A auf der Basis des Bereichschlüssels #9000h und benutzt das Verschlüsselungsresultat als einen ersten Zugriffschlüssel K_{I1}. Außerdem gibt der Verwalter I den ersten Zugriffschlüssel K_{I1} (das Verschlüsselungsresultat auf der Basis des Bereichschlüssels #9000h) an den Verwalter H ab, um ihn sukzessive auf der Basis jedes der Dienstschlüssel #8008h und #8104h wie in **Fig.** 25(B) gezeigt zu verschlüsseln. Dann benutzt der Verwalter I das Verschlüsselungsresultat wie in **Fig.** 25(C) gezeigt als einen zweiten Zugriffschlüssel K_{I2}.

[0271] Wie bei (D) der Fig. 25 gezeigt, verschlüsselt der Verwalter J das Verschlüsselungsresultat des Systemschlüssels auf der Basis des Bereichschlüssels #0000h vom Verwalter A auf der Basis des Bereichschlüssels #A000h und benutzt das Verschlüsselungsresultat als einen ersten Zugriffschlüssel K_{J1}. Außerdem gibt der Verwalter J den ersten Zugriffschlüssel K_{J1} (das auf dem Bereichschlüssel #A000h

basierende Verschlüsselungsresultat) an den Verwalter H ab, um das Verschlüsselungsresultat, wie bei (B) der Fig. 25 gezeigt, sukzessive auf der Basis jedes der Dienstschlüssel #8008h und #8105h zu verschlüsseln. Der Verwalter J benutzt das Verschlüsselungsresultat, wie bei (D) der Fig. 25 gezeigt, als einen zweiten Zugriffschlüssel K_{J2}.

[0272] In diesem Fall wird in der IC-Karte **2** der Systemschlüssel durch Benutzung des Bereichschlüssels und des Dienstschlüssels, die im EEPROM **66** gespeichert sind, entsprechend der gleichen Prozedur wie im Fall der Fig. 25, um den ersten Zugriffschlüssel und den zweiten Zugriffschlüssel zu erzeugen, wodurch der Verwalter I auf die Dienst definierenden Bereiche #8008h und #8104h des Verwalters H zugreifen kann, und der Verwalter J auf die Dienst definierenden Bereiche #8008h und #8105h des Verwalters H zugreifen kann.

[0273] Der Verwalter H bildet den Dienst definierenden Bereich #8008h, um seine Daten zwischen den Verwaltern I und J gemeinsam zu benutzen, und bildet den Dienst definierenden Bereich #8104h oder #8105h als einen sogenannten Dienst definierenden Leer- bzw. Dummybereich zum Steuern des Zugriffs auf den Dienst definierenden Bereich #8008h durch jeden der Verwalter I oder J. Demgemäss sind die von den Dienst definierenden Bereichen #9104h und #8105h verwalteten Dienstbereiche nicht notwendig, und ihre Kapazität kann gleich null sein.

[0274] In diesem Fall kann beispielsweise, wenn der Verwalter H den Dienstschlüssel #8104h ändert, der Verwalter I, in welchem der zweite Zugriffschlüssel K_{I2} durch Benutzung des Dienstschlüssels #8104h erzeugt wird, um die Zertifizierungsverarbeitung der IC-Karte **2** auszuführen, nicht auf den Dienst definierenden Bereich #8008h zugreifen. Das heißt, nur der Zugriff auf den Dienst definierenden Bereich #8008h durch den Verwalter I ist verhindert. Andererseits kann beispielsweise, wenn der Verwalter H den Dienstschlüssel #8105h ändert, der Verwalter J, bei dem der zweite Zugriffschlüssel K_{J2} durch Benutzung des Dienstschlüssels #8105h erzeugt wird, um die Zertifizierungsverarbeitung in der IC-Karte **2** auszuführen, nicht auf den Dienst definierenden Bereich #8008h zugreifen. Das heißt, nur der Zugriff auf den Dienst definierenden Bereich #8008h durch den Verwalter J ist verhindert.

[0275] Wie vorstehend beschrieben kann durch Benutzung eines Dienst definierenden Dummybereichs verhindert werden, dass ein spezieller Kindverwalter zugreift.

[0276] Bei der vorstehenden Beschreibung beziehen sich Ausführungsformen der vorliegenden Erfindung auf ein kontaktloses Kartensystem, bei dem die Kommunikation in einem kontaktlosen Zustand ausgeführt wird. Jedoch können Ausführungsformen der Erfindung ein Kartensystem aufweisen, bei dem die Kommunikation unter einem Kontaktzustand ausgeführt wird. Außerdem sind Ausführungsformen der vorliegenden Erfindung nicht auf das Kartensystem beschränkt.

[0277] Bei dieser Ausführungsform wird die Zertifizierung durch ein sogenanntes geheimes Schlüsselsystem ausgeführt, jedoch kann sie durch ein sogenanntes offenes öffentliches Schlüsselsystem (open-public key system) ausgeführt werden.

[0278] Wenn bei dieser Ausführungsform auf den Dienst definierenden Bereich der Schicht eines Bereich definierenden Bereichs zugegriffen wird, wird der erste Zugriffschlüssel durch sukzessive Benutzung der Bereichschlüssel der Bereich definierenden Bereiche auf dem Bus von der Schicht des Bereich definierenden Bereichs zur obersten Schicht erzeugt, jedoch ist das Erzeugungsverfahren des ersten Zugriffschlüssels nicht auf die vorstehende Art und Weise beschränkt. Außerdem wird gemäß dieser Ausführungsform der zweite Zugriffschlüssel durch sukzessive Benutzung der Dienstschlüssel des Dienst definierenden Bereichs, auf den zuzugreifen ist, erzeugt. Jedoch ist das Erzeugungsverfahren des zweiten Zugriffschlüssels nicht auf die vorstehende Art und Weise beschränkt. Das heißt, der erste Zugriffschlüssel und der zweite Zugriffschlüssel können durch sukzessive Benutzung irgendwelcher zweier oder mehrerer Bereichschlüssel oder Dienstschlüssel erzeugt werden.

[0279] Außerdem ist bei dieser Ausführungsform vom Benutzerblock und Systemblock jeder im EEPROM **66**, der ein einzelner Speicher ist, gespeichert. Jedoch können der Benutzerblock und der Systemblock in physikalisch verschiedenen Speichern gespeichert sein.

[0280] Bei dieser Ausführungsform sind Daten im EEPROM gespeichert, jedoch können die Daten in einem Halbleiterspeicher, einer magnetischen Platte oder dgl. anders als der EEPROM gespeichert sein.

[0281] Gemäß Ausführungsformen der vorliegenden Erfindung wird die Speichereinrichtung auf der Basis des Speicherinhalts des Bereich definierenden Bereichs der den Bereich definierenden Bereich zum Speichern des Bereichs des Speicherbereich identifizierenden Codes, der dem zu verwaltenden Speicherbereich zugeordnet werden kann und zum Identifizieren des Speicherbereichs benutzt wird, und zum Speichern der leeren Kapazität des zu verwaltenden Speicherbereichs aufweisenden Speichereinrichtung verwaltet. Demgemäss kann die Ressourcenverwaltung der Speichereinrichtung ausgeführt werden.

[0282] Gemäß Ausführungsformen der vorliegenden Erfindung wird der Speicherbereich der Datenspeichervorrichtung verwaltet, während er in einer Schichtstruktur ausgebildet ist, und ein oder mehrere zum Zertifizieren benutzte Zertifizierungsschlüssel werden durch Benutzung zweier oder mehrerer Schichtschlüssel bezüglich jeder Schicht des Speicherbereichs der Datenspeichervorrichtung oder Datenspeicherbereichschlüssel bezüglich des Speicherbereichs, in welchem Daten gespeichert sind, erzeugt, und die Zertifizierung wird auf der Basis des Zertifizierungsschlüssel ausgeführt. Demgemäss kann bei der Datenspeichervorrichtung eine Zugriffssteuerung, die Flexibilität und hohe Sicherheit aufweist, ausgeführt werden.

Patentansprüche

1. Datenspeichervorrichtung (**2**) zur Speicherung von Daten zum Bereitstellen eines vorbestimmten Dienstes, aufweisend:
eine Datenspeichereinrichtung zur Speicherung der Daten,
eine Verwaltungseinrichtung zur Verwaltung eines Speicherbereichs der Speichereinrichtung während eines Setzens des Speicherbereichs in eine geschichtete Struktur,
eine Schichtschlüssel-Speicherungseinrichtung zur Speicherung eines Schichtschlüssels für jede Schicht des Speicherbereiches der Datenspeichereinrichtung,
eine Datenspeicherbereichschlüssel-Speicherungseinrichtung zur Speicherung eines Datenspeicherbereichschlüssels für den Speicherbereich, in welchem die Daten gespeichert sind, **dadurch gekennzeichnet**, dass die Datenspeichervorrichtung aufweist:
eine Erzeugungseinrichtung zur Erzeugung eines oder mehrerer zu einer Zertifizierung zum Zugriff auf den Speicherbereich durch Verwendung zweier oder mehrerer Schichtschlüssel oder Datenspeicherbereichschlüssel verwendeter Zertifizierungsschlüssel (Kac, Kbc, KE1, KE2, KF1, KF2), und
eine Zertifizierungseinrichtung zur Ausführung einer Zertifizierung auf der Basis des Zertifizierungsschlüssels (Kac, Kbc, KE1, KE2, KF1, KF2).

2. Datenspeichervorrichtung nach Anspruch 1, wobei die Zertifizierungseinrichtung eine Verschlüsselung oder Decodierung auf der Basis des Zertifizierungsschlüssels ausführt.

3. Datenspeichervorrichtung nach Anspruch 1, wobei die Erzeugungseinrichtung eine vorbestimmte Information auf der Basis des Schichtschlüssels für eine vorbestimmte Schicht verschlüsselt.

4. Datenspeichervorrichtung nach Anspruch 3, wobei die vorbestimmte Information auf der Basis des Schichtschlüssels für die Elternschicht der vorbestimmten Schicht verschlüsselt wird.

5. Datenspeichervorrichtung nach Anspruch 1, wobei die Erzeugungseinrichtung eine vorbestimmte Information durch sukzessive Verwendung von Schichtschlüsseln für Schichten auf einem Bus bis zu einer vorbestimmten Schicht verschlüsselt und das Verschlüsselungsresultat durch Verwendung des Datenspeicherbereichschlüssels verschlüsselt und dadurch den Zertifizierungsschlüssel erzeugt.

6. Datenspeichervorrichtung nach Anspruch 1, außerdem aufweisend eine Kommunikationseinrichtung zur Ausführung von Kommunikationen mit einer externen Einrichtung, wobei die Erzeugungseinrichtung zwei oder mehr zum Erzeugen des Zertifizierungsschlüssels auf der Basis von Information aus der externen Einrichtung verwendete Schichtschlüssel oder Datenspeicherbereichschlüssel erkennt.

7. Datenspeichervorrichtung nach Anspruch 1, wobei die Erzeugungseinrichtung den Zertifizierungsschlüssel auf der Basis von der Vorrichtung inhärenter Information umwandelt, und die Zertifizierungseinrichtung eine Zertifizierung auf der Basis des Umwandlungsresultats des auf der inhärenten Information basierenden Zertifizierungsschlüssels ausführt.

8. Datenspeichervorrichtung nach Anspruch 1, wobei die Speichereinrichtung nicht flüchtig ist.

9. Datenspeichervorrichtung nach Anspruch 1, außerdem aufweisend eine Kommunikationseinrichtung zur Ausführung von Kommunikationen mit einer externen Einrichtung, und wobei die Zertifizierungseinrichtung eine Zertifizierung mit der externen Einrichtung ausführt.

10. Datenspeichervorrichtung nach Anspruch 9, wobei die Kommunikationseinrichtung Kommunikationen mit der externen Einrichtung unter einem Kontakt- oder Nichtkontaktzustand ausführt.

11. Datenspeicherverfahren für eine Datenspeichervorrichtung zur Speicherung von Daten zum Bereitstellen eines vorbestimmten Dienstes, wobei die Datenspeichervorrichtung aufweist:
eine Speichereinrichtung zur Speicherung von Daten,
eine Verwaltungseinrichtung zur Verwaltung eines Speicherbereichs der Datenspeichereinrichtung während eines Setzens des Speicherbereichs in eine Schichtstruktur,
eine Schichtschlüsselspeichereinrichtung zur Speicherung eines Schichtschlüssels für jede Schicht des Speicherbereichs der Datenspeichereinrichtung, und
eine Datenspeicherbereichschlüssel-Speicherungseinrichtung zur Speicherung eines Datenspeicherbereichschlüssels für den Speicherbereich, in welchem die Daten gespeichert sind, und wobei das Verfahren gekennzeichnet ist durch

einen Erzeugungsschritt zur Erzeugung eines oder mehrerer zu einer Zertifizierung zum Zugriff auf den Speicherbereich durch Verwendung zweier oder mehrerer Schichtspeicher oder Datenspeicherbereichschlüssel verwendeter Zertifizierungsschlüssel, und
einen Zertifizierungsschritt zur Ausführung einer Zertifizierung auf der Basis des Zertifizierungsschlüssels.

12. Datenspeicherverfahren nach Anspruch 11, wobei der Zertifizierungsschritt eine Verschlüsselung oder Decodierung auf der Basis des Zertifizierungsschlüssels ausführt.

13. Datenspeicherverfahren nach Anspruch 11, wobei der Erzeugungsschritt den Zertifizierungsschlüssel durch Verschlüsselung vorbestimmter Information auf der Basis des Schichtschlüssels für eine vorbestimmte Schicht erzeugt.

14. Datenspeicherverfahren nach Anspruch 13, wobei die vorbestimmte Information auf der Basis des Schichtschlüssels für die Elternschicht der vorbestimmten Schicht verschlüsselt wird.

15. Datenspeicherverfahren nach Anspruch 11, wobei der Erzeugungsschritt vorbestimmte Information durch sukzessive Verwendung der Schichtschlüssel für Schichten auf einem Bus bis zu einer vorbestimmten Schicht verschlüsselt und das Verschlüsselungsresultat durch Verwendung des Datenspeicherschlüssels verschlüsselt und dadurch den Zertifizierungsschlüssel erzeugt.

16. Datenspeicherverfahren nach Anspruch 11, wobei die Datenspeichervorrichtung außerdem eine Kommunikationseinrichtung zur Ausführung von Kommunikationen mit einer externen Einrichtung aufweist, und der Erzeugungsschritt zwei oder mehr zum Erzeugen des Zertifizierungsschlüssels auf der Basis der Information von der externen Einrichtung verwendete Schichtschlüssel oder Datenspeicherbereichschlüssel erkennt.

17. Datenspeicherverfahren nach Anspruch 11, wobei der Erzeugungsschritt den Zertifizierungsschlüssel auf der Basis von der Vorrichtung inhärenter Information umwandelt, und der Zertifizierungsschritt die Zertifizierung auf der Basis des Umwandlungsresultats des Zertifizierungsschlüssels auf der Basis der Information, die der Vorrichtung inhärentist, ausführt.

18. Datenspeicherverfahren nach Anspruch 11, wobei die Speichereinrichtung nicht flüchtig ist.

19. Datenspeicherverfahren nach Anspruch 11, wobei die Datenspeichervorrichtung außerdem eine Kommunikationseinrichtung zur Ausführung von Kommunikationen mit einer externen Einrichtung aufweist, und der Zertifizierungsschritt eine Zertifizierung mit der externen Einrichtung ausführt.

20. Datenspeicherverfahren nach Anspruch 19, wobei die Kommunikationseinrichtung die Kommunikationen mit der externen Einrichtung unter einem Kontakt- oder Nichtkontaktzustand ausführt.

Es folgen 25 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

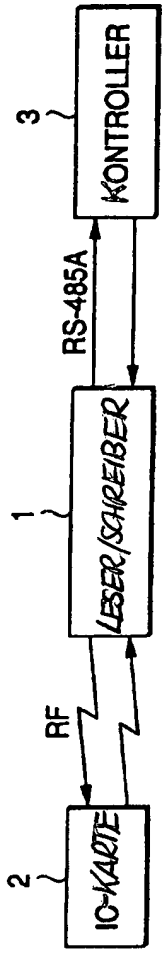


FIG. 2

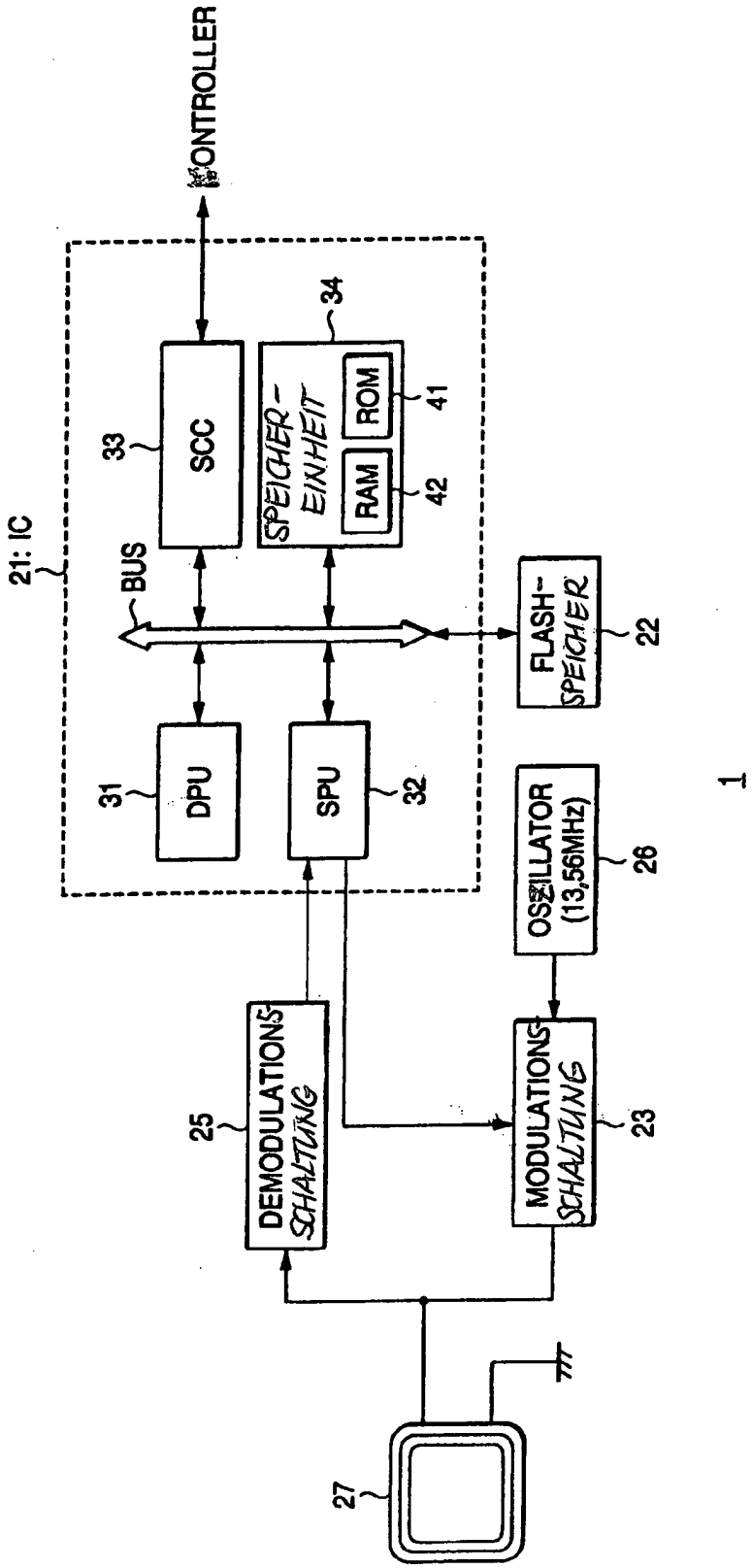

CONTROLLER
21: IC
BUS
33
SCC
34
SPEICHER-EINHEIT
ROM
41
RAM
42
FLASH-SPEICHER
22
31
DPU
SPU
32
OSZILLATOR (13,56MHz)
26
1
25
DEMODULATIONS SCHALTUNG
MODULATIONS SCHALTUNG
23
27

FIG. 3

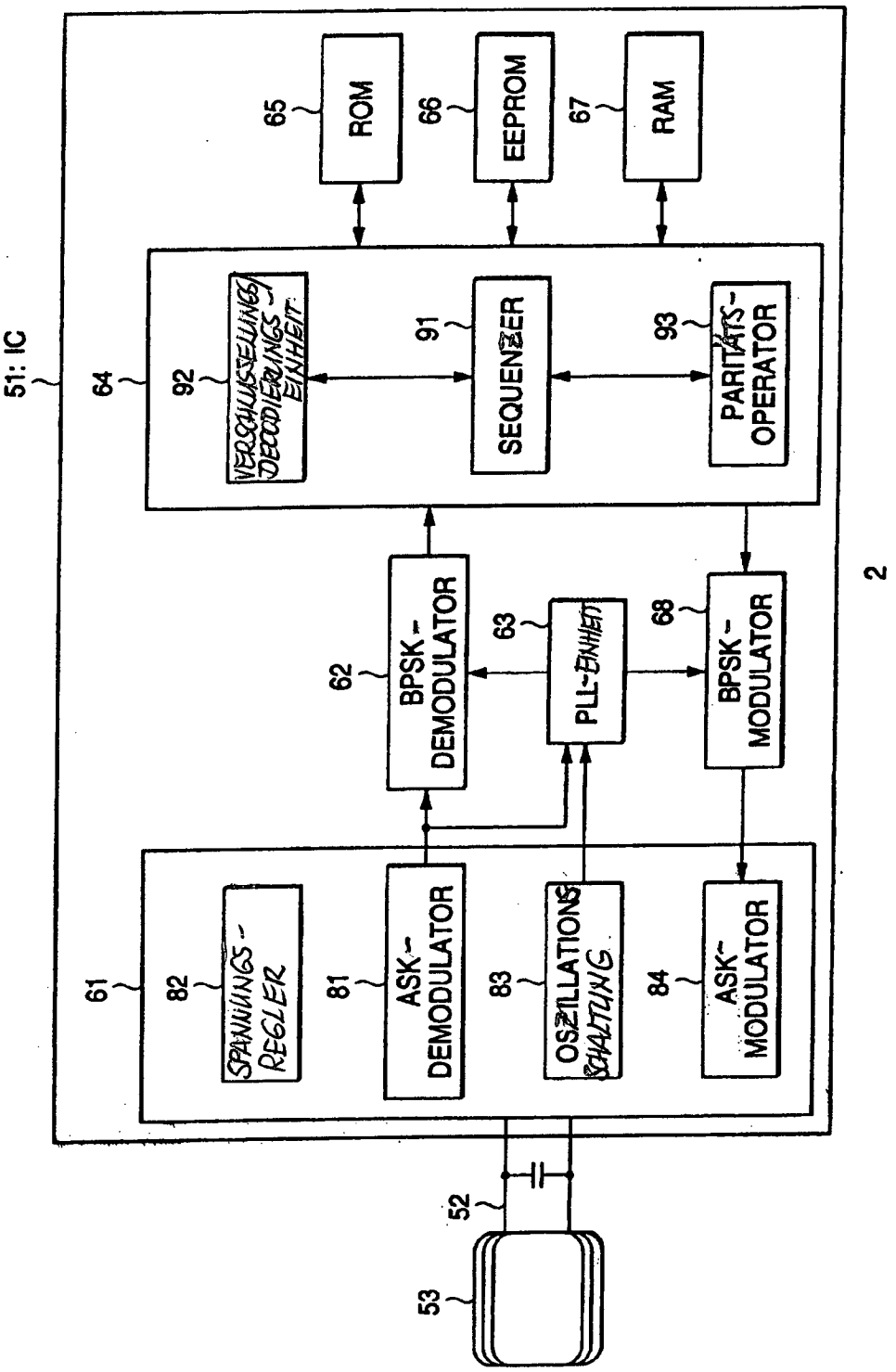
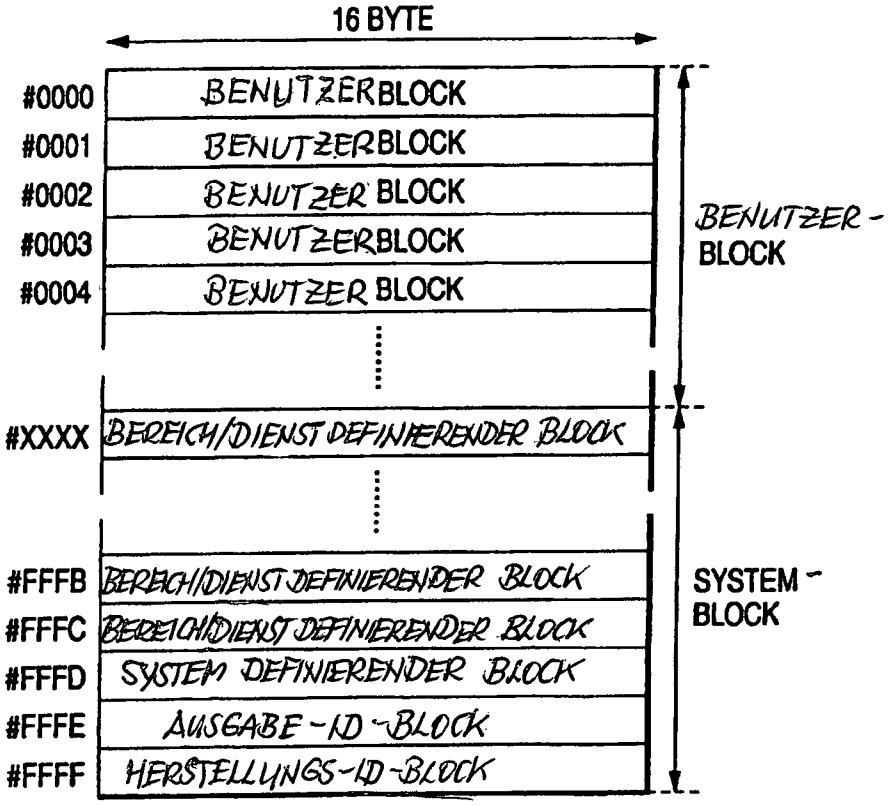

51: IC
2
61
64
65
66
67
ROM
EEPROM
RAM
92
VERSCHLÜSSELUNGS-/DECODIERUNGS-EINHEIT
91
SEQUENZER
93
PARITÄTS-OPERATOR
62
BPSK-DEMODULATOR
63
PLL-EINHEIT
68
BPSK-MODULATOR
82
SPANNUNGS-REGLER
81
ASK-DEMODULATOR
83
OSZILLATIONS-SCHALTUNG
84
ASK-MODULATOR
52
53

FIG. 4



LOGISCHES FORMAT DES EEPROM 66

FIG. 5

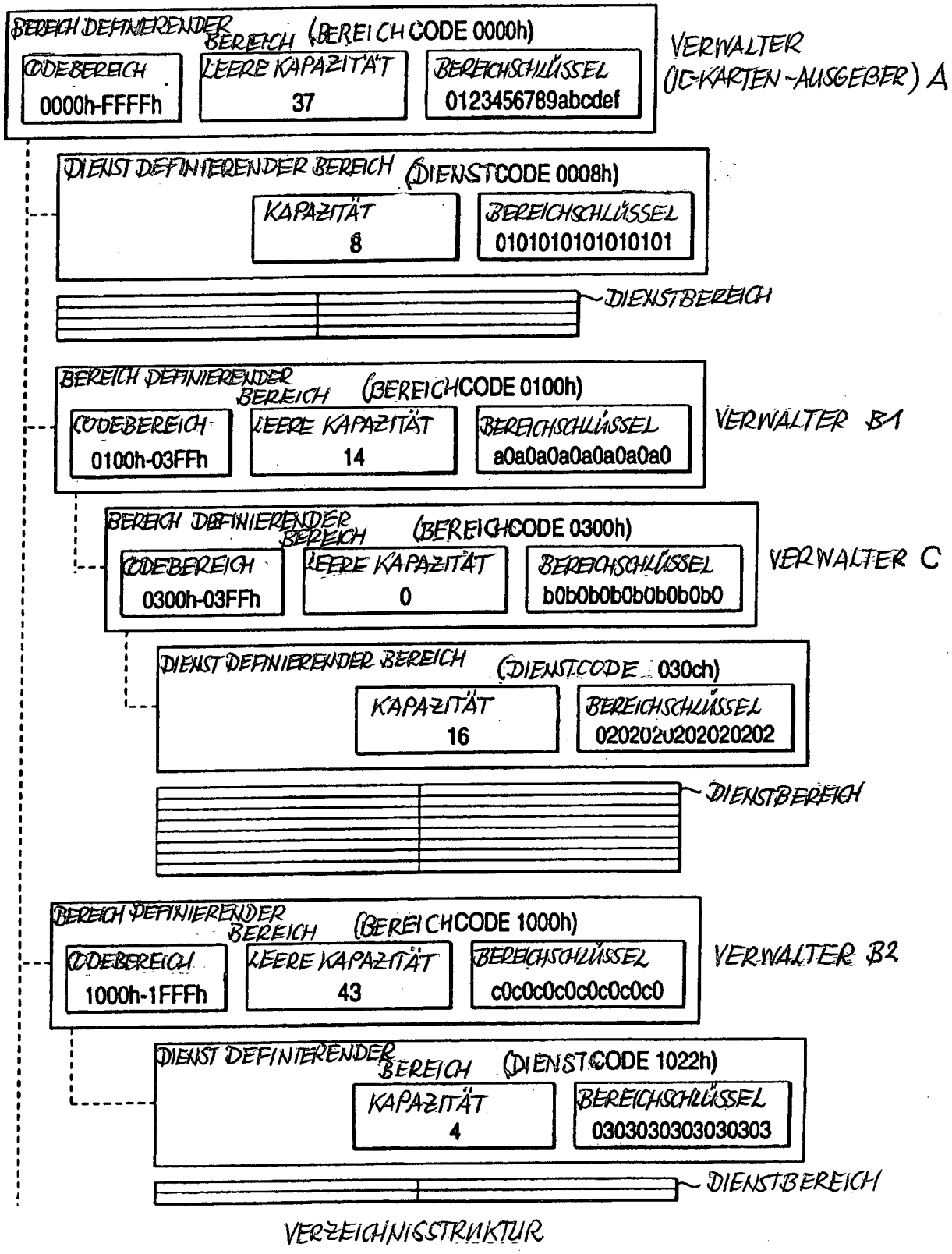

BEREICH DEFINIERENDER BEREICH (BEREICHCODE 0000h)
CODEBEREICH
0000h-FFFFh
LEERE KAPAZITÄT
37
BEREICHSCHLÜSSEL
0123456789abcdef
VERWALTER (IC-KARTEN-AUSGEBER) A
DIENST DEFINIERENDER BEREICH (DIENSTCODE 0008h)
KAPAZITÄT
8
BEREICHSCHLÜSSEL
0101010101010101
DIENSTBEREICH
BEREICH DEFINIERENDER BEREICH (BEREICHCODE 0100h)
CODEBEREICH
0100h-03FFh
LEERE KAPAZITÄT
14
BEREICHSCHLÜSSEL
a0a0a0a0a0a0a0a0
VERWALTER B1
BEREICH DEFINIERENDER BEREICH (BEREICHCODE 0300h)
CODEBEREICH
0300h-03FFh
LEERE KAPAZITÄT
0
BEREICHSCHLÜSSEL
b0b0b0b0b0b0b0b0
VERWALTER C
DIENST DEFINIERENDER BEREICH (DIENSTCODE 030ch)
KAPAZITÄT
16
BEREICHSCHLÜSSEL
020202u202020202
DIENSTBEREICH
BEREICH DEFINIERENDER BEREICH (BEREICHCODE 1000h)
CODEBEREICH
1000h-1FFFh
LEERE KAPAZITÄT
43
BEREICHSCHLÜSSEL
c0c0c0c0c0c0c0c0
VERWALTER B2
DIENST DEFINIERENDER BEREICH (DIENSTCODE 1022h)
KAPAZITÄT
4
BEREICHSCHLÜSSEL
0303030303030303
DIENSTBEREICH
VERZEICHNISSTRUKTUR

FIG. 6

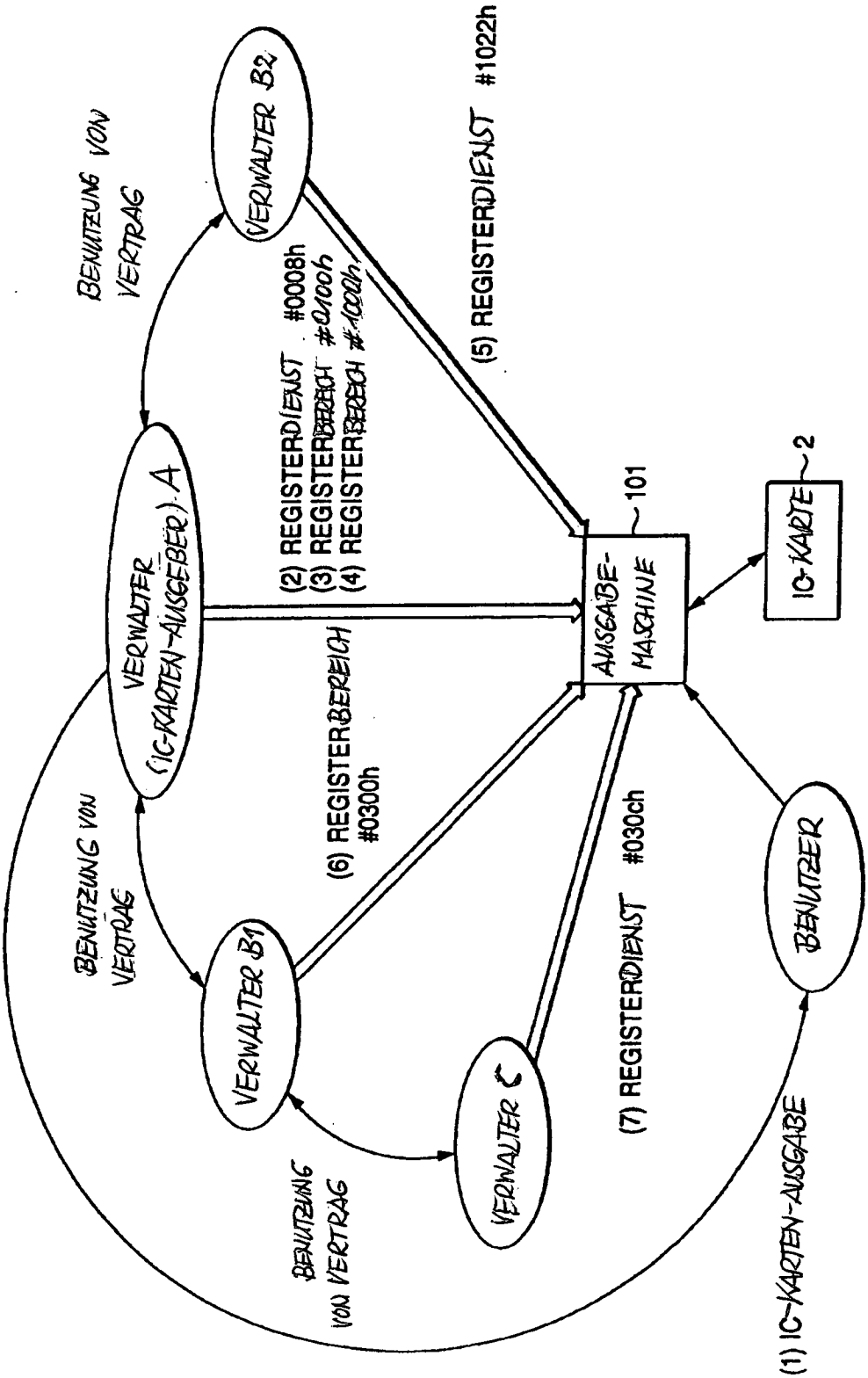

VERWALTER B2
BENUTZUNG VON VERTRAG
VERWALTER (IC-KARTEN-AUSGEBER) A
VERWALTER B1
BENUTZUNG VON VERTRAG
VERWALTER C
BENUTZUNG VON VERTRAG
(2) REGISTERDIENST #0008h
(3) REGISTERBEREICH #0100h
(4) REGISTERBEREICH #1000h
(5) REGISTERDIENST #1022h
(6) REGISTERBEREICH #0300h
(7) REGISTERDIENST #030ch
AUSGABE-MASCHINE
101
IC-KARTE
2
BENUTZER
(1) IC-KARTEN-AUSGABE

FIG. 7

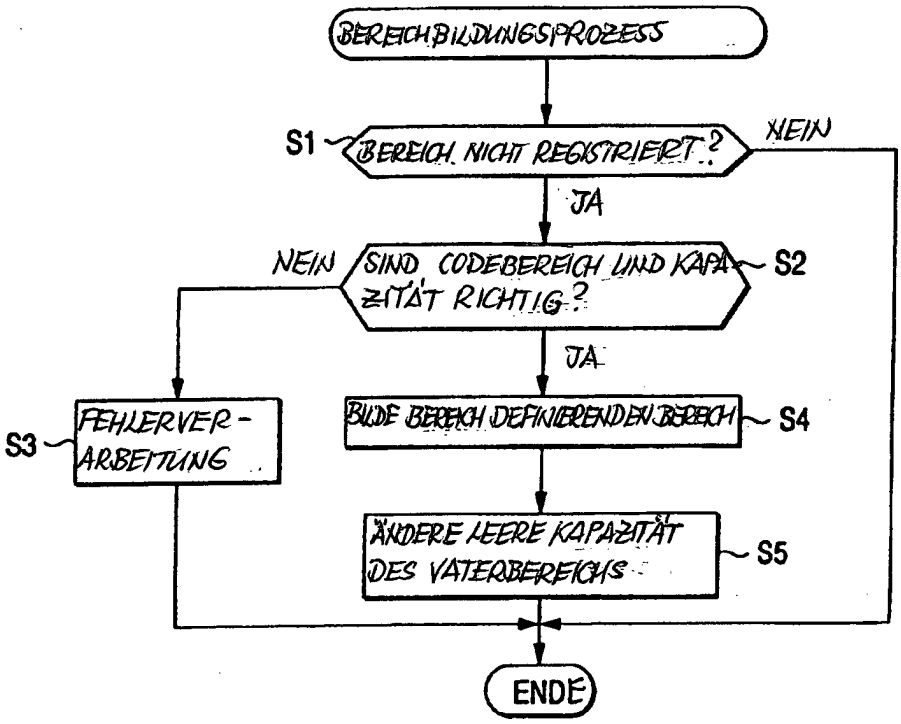

BEREICHBILDUNGSPROZESS
S1
BEREICH NICHT REGISTRIERT?
NEIN
JA
NEIN
SIND CODEBEREICH UND KAPAZITÄT RICHTIG?
S2
JA
S3
FEHLERVERARBEITUNG
BILDE BEREICH DEFINIERENDEN BEREICH
S4
ÄNDERE LEERE KAPAZITÄT DES VATERBEREICHS
S5
ENDE

FIG. 8

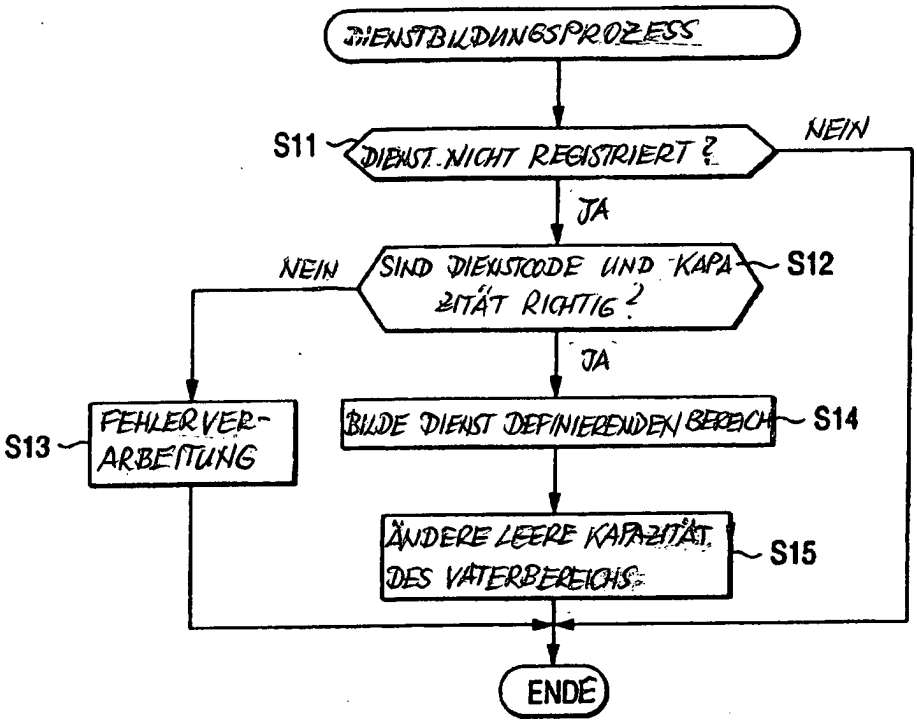

DIENSTBILDUNGSPROZESS
S11
DIENST NICHT REGISTRIERT ?
NEIN
JA
NEIN
SIND DIENSTCODE UND KAPAZITÄT RICHTIG ?
S12
JA
S13
FEHLERVERARBEITUNG
BILDE DIENST DEFINIERENDEN BEREICH
S14
ÄNDERE LEERE KAPAZITÄT DES VATERBEREICHS
S15
ENDE

FIG. 9

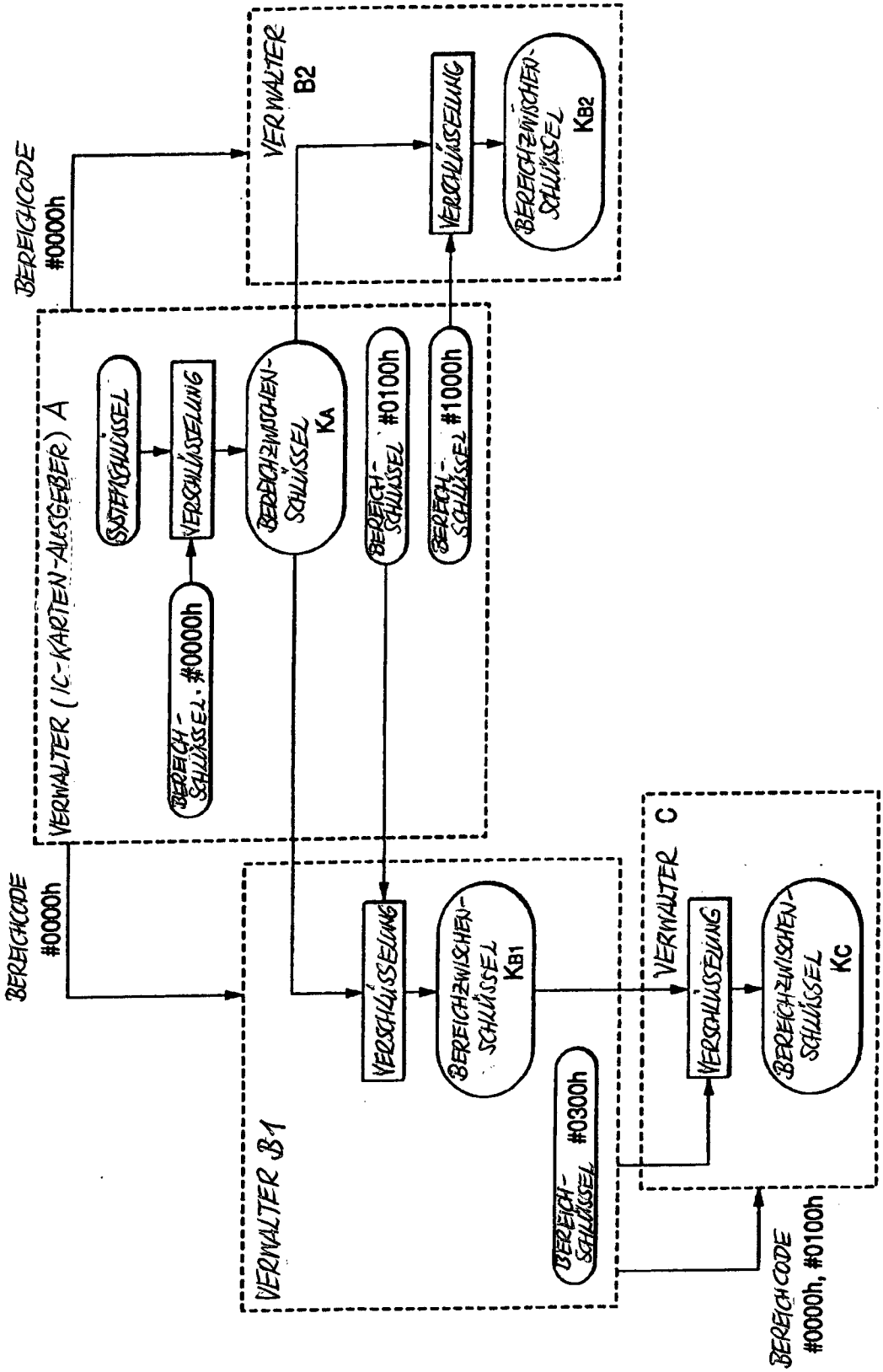

BEREICHCODE
#0000h
VERWALTER (IC-KARTEN-AUSGEBER) A
SYSTEMSCHLÜSSEL
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #0000h
BEREICHZWISCHEN-SCHLÜSSEL KA
BEREICH-SCHLÜSSEL #0100h
BEREICH-SCHLÜSSEL #1000h
VERWALTER B2
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL KB2
BEREICHCODE
#0000h
VERWALTER B1
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL KB1
BEREICH-SCHLÜSSEL #0300h
VERWALTER C
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL KC
BEREICHCODE
#0000h, #0100h

FIG. 10

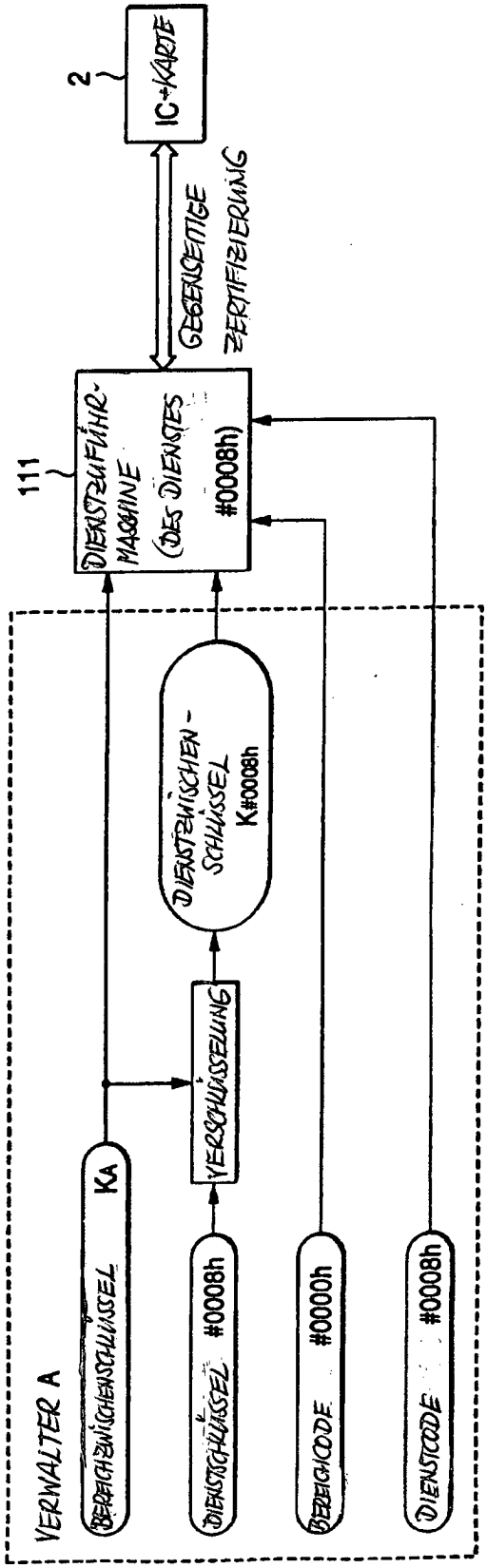

2
IC-KARTE
GEGENSEITIGE ZERTIFIZIERUNG
111
DIENSTZUFÜHR-MASCHINE (DES DIENSTES #0008h)
VERWALTER A
BEREICHZWISCHENSCHLÜSSEL KA
DIENSTSCHLÜSSEL #0008h
VERSCHLÜSSELUNG
DIENSTZWISCHEN-SCHLÜSSEL K#0008h
BEREICHCODE #0000h
DIENSTCODE #0008h

FIG. 11

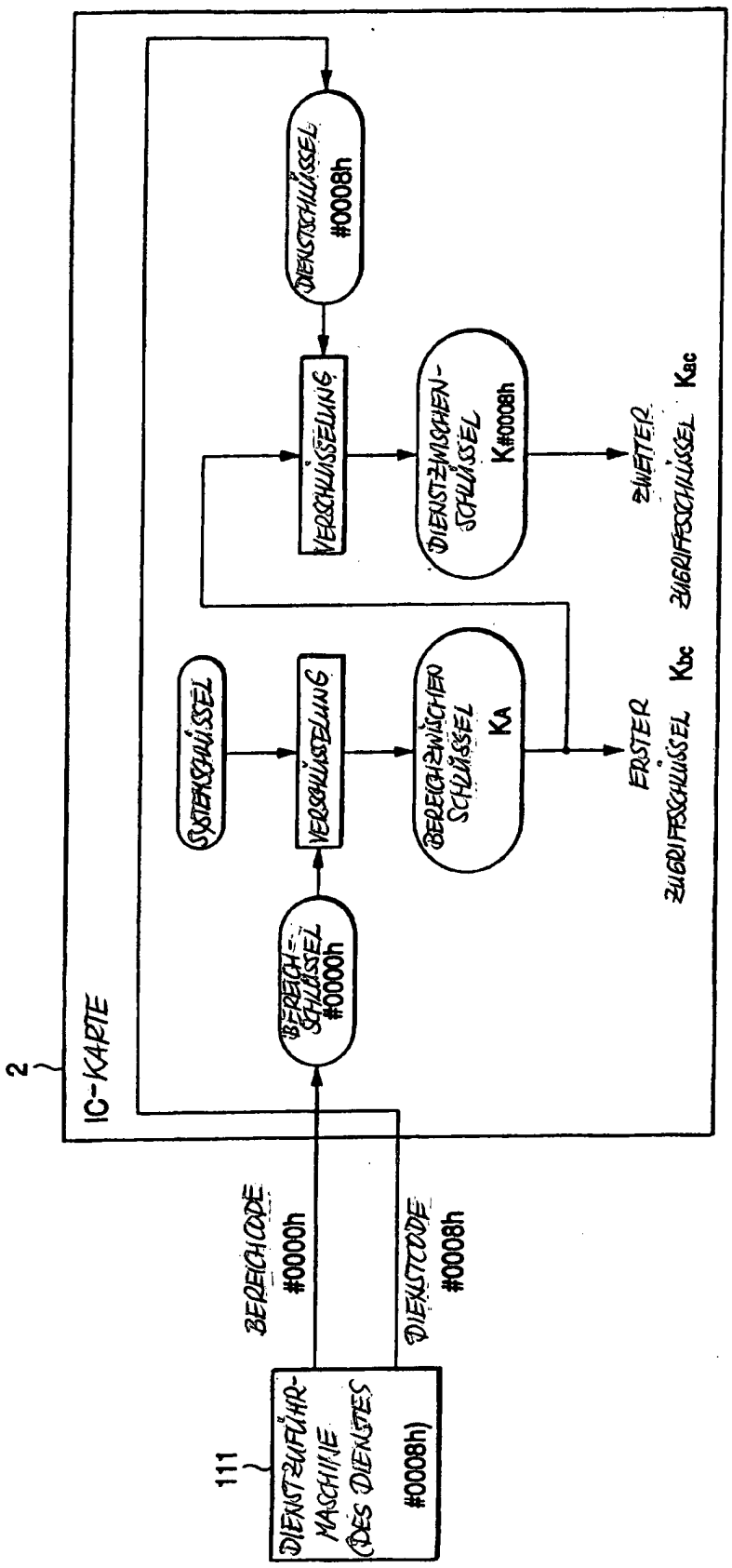

2
IC-KARTE
BEREICH-SCHLÜSSEL #0000h
SYSTEMSCHLÜSSEL
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL KA
DIENSTSCHLÜSSEL #0008h
VERSCHLÜSSELUNG
DIENSTZWISCHEN-SCHLÜSSEL K#0008h
ERSTER ZUGRIFFSSCHLÜSSEL Kbc
ZWEITER ZUGRIFFSSCHLÜSSEL Kac
BEREICHCODE #0000h
DIENSTCODE #0008h
111
DIENSTAUSFÜHR-MASCHINE DES DIENSTES #0008h)

FIG. 12

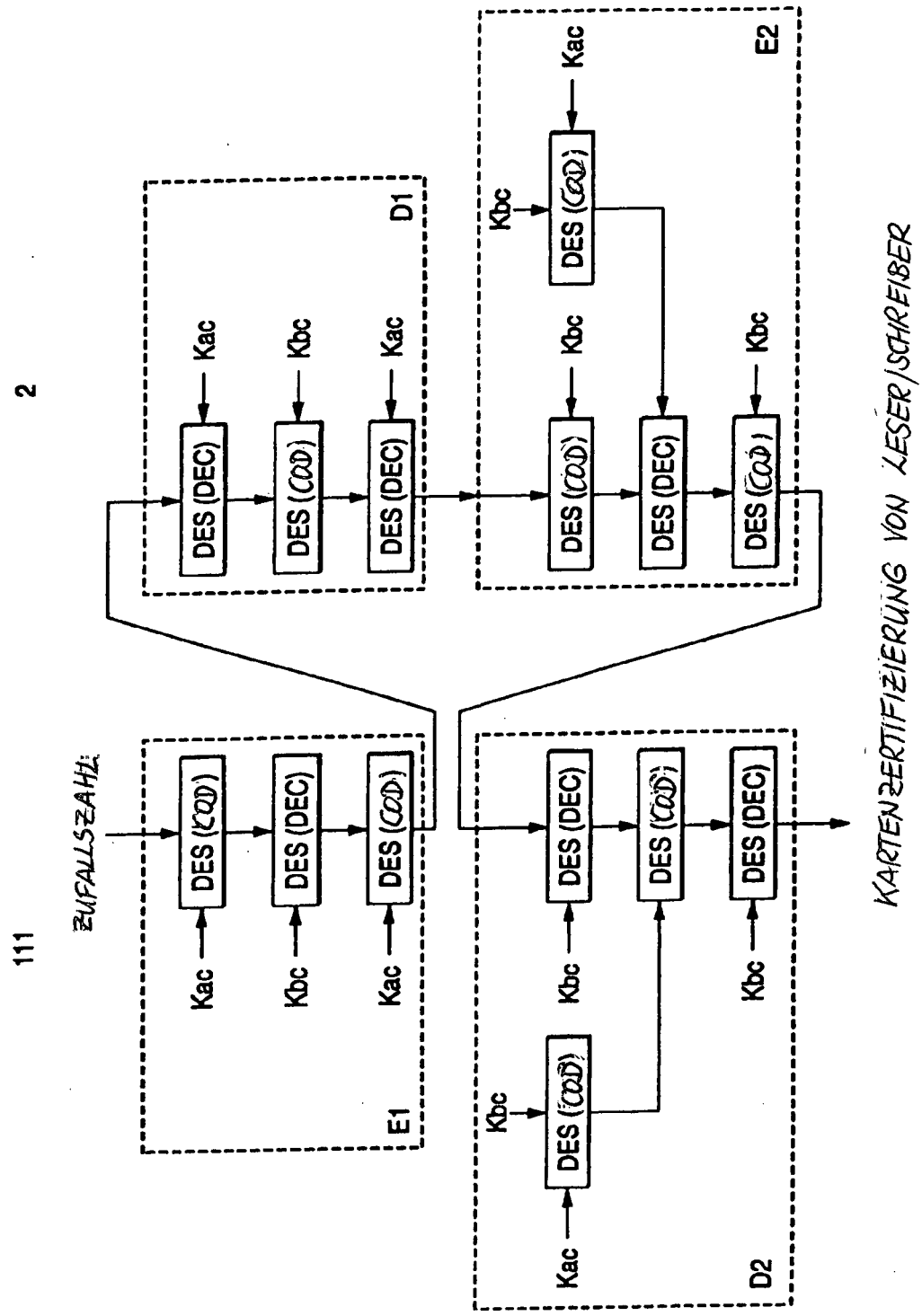

111
2
ZUFALLSZAHL
DES (DEC)
DES (COD)
Kac
Kbc
E1
D1
E2
D2
KARTENZERTIFIZIERUNG VON LESER/SCHREIBER

FIG. 13

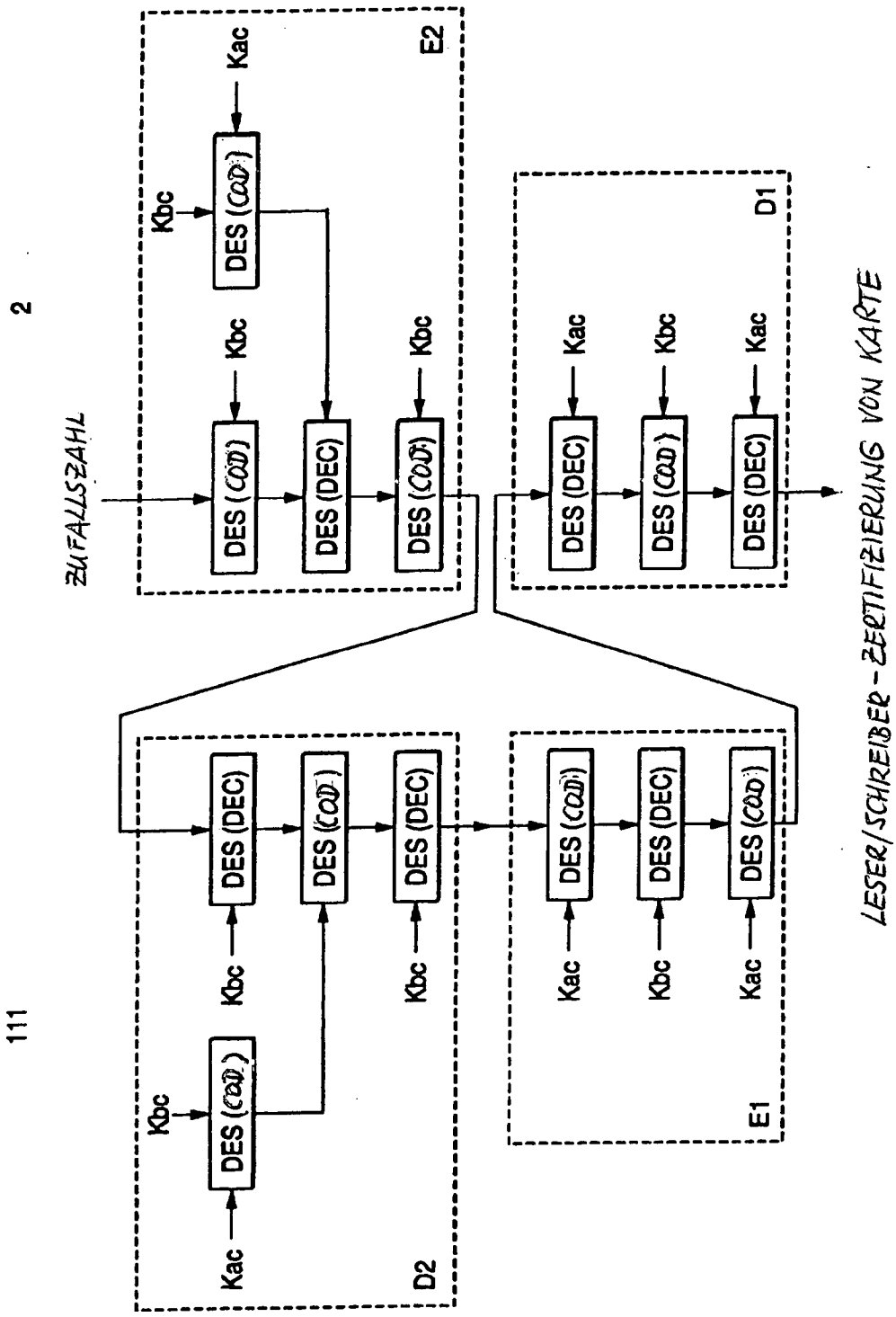

111
2
ZUFALLSZAHL
E2
D1
E1
D2
Kac
Kbc
DES (ENC)
DES (DEC)
LESER/SCHREIBER - ZERTIFIZIERUNG VON KARTE

FIG. 14

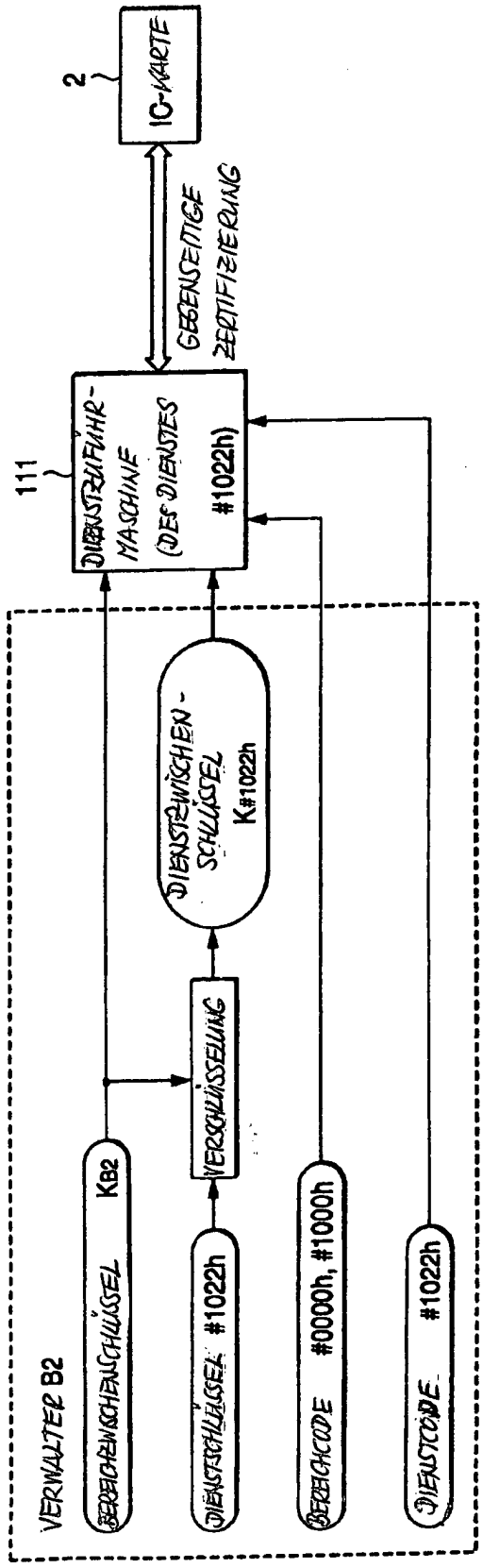

2
IC-KARTE
GEGENSEITIGE ZERTIFIZIERUNG
111
DIENSTZUFÜHR-MASCHINE (DES DIENSTES #1022h)
VERWALTET B2
DIENSTZWISCHEN-SCHLÜSSEL K#1022h
VERSCHLÜSSELUNG
BEREICHSZWISCHENSCHLÜSSEL KB2
DIENSTSCHLÜSSEL #1022h
BEREICHSCODE #0000h, #1000h
DIENSTCODE #1022h

FIG. 15

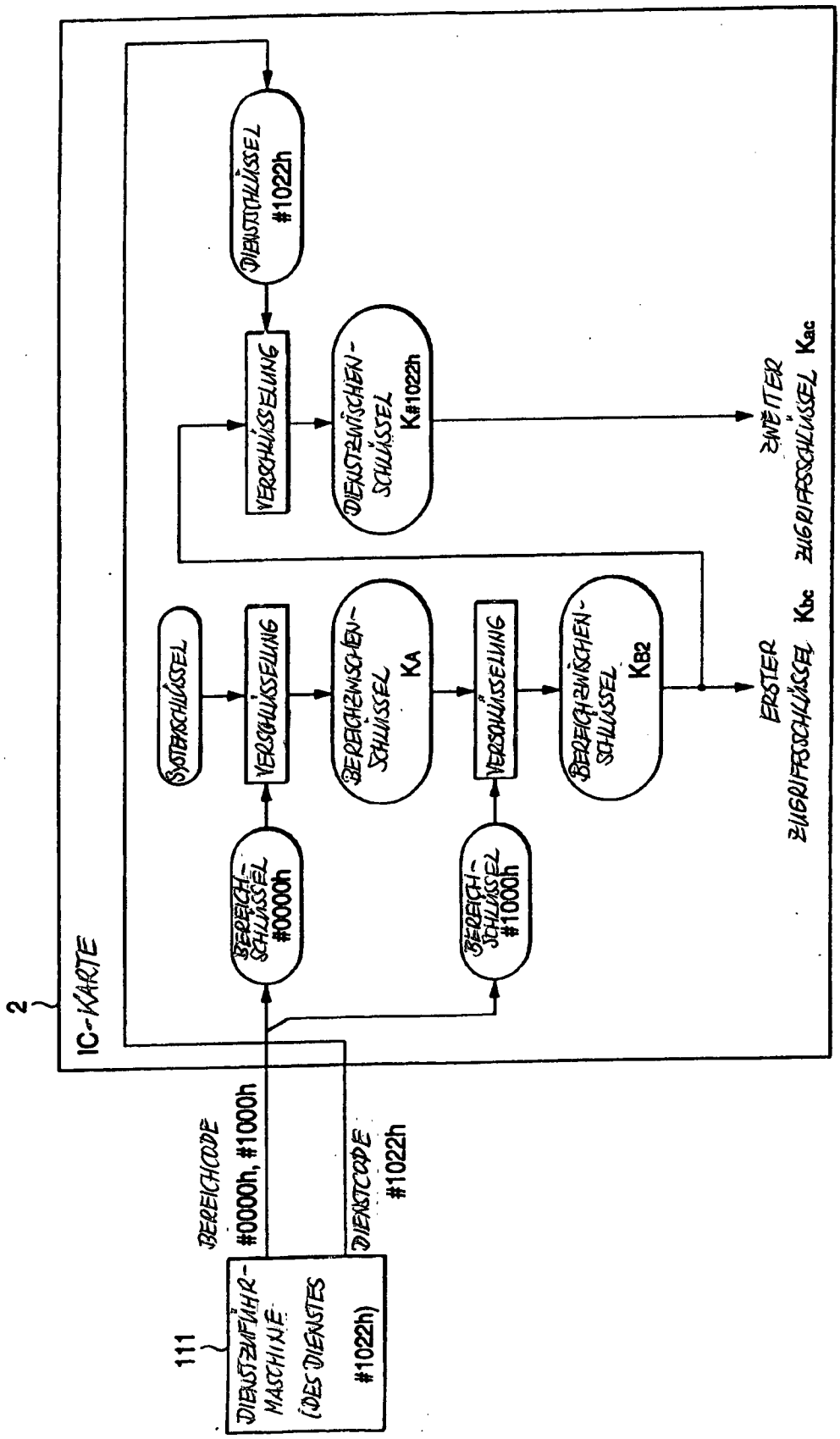

2
IC-KARTE
SYSTEMSCHLÜSSEL
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #0000h
BEREICHSPEZIFISCHER SCHLÜSSEL KA
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #1000h
BEREICHSPEZIFISCHER SCHLÜSSEL KB2
ERSTER ZUGRIFFSSCHLÜSSEL Kbc
DIENSTSCHLÜSSEL #1022h
VERSCHLÜSSELUNG
DIENSTSPEZIFISCHER SCHLÜSSEL K#1022h
ZWEITER ZUGRIFFSSCHLÜSSEL Kac
111
DIENSTZUFÜHR-MASCHINE (DES DIENSTES #1022h)
BEREICHCODE #0000h, #1000h
DIENSTCODE #1022h

FIG. 16

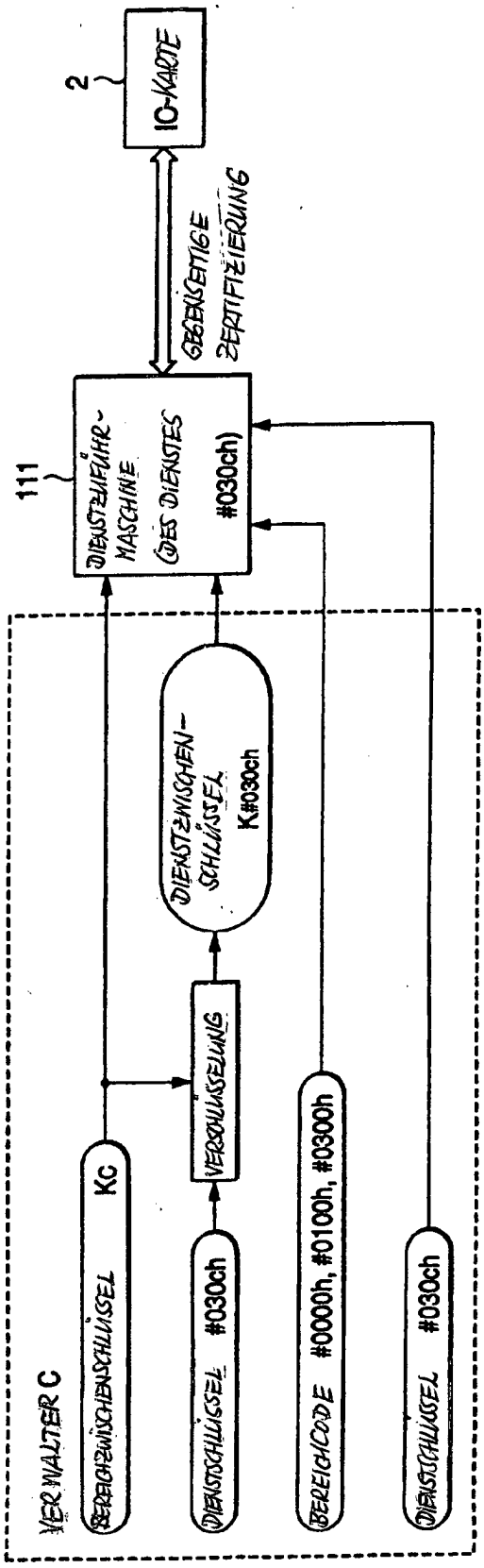

2
IC-KARTE
GEGENSEITIGE ZERTIFIZIERUNG
111
DIENSTBEREITSTELLUNGS-MASCHINE (DES DIENSTES #030ch)
VERWALTER C
BEREICHSZWISCHENSCHLÜSSEL Kc
DIENSTSCHLÜSSEL #030ch
VERSCHLÜSSELUNG
DIENSTZWISCHEN-SCHLÜSSEL K#030ch
BEREICHCODE #0000h, #0100h, #0300h
DIENSTSCHLÜSSEL #030ch

FIG. 17

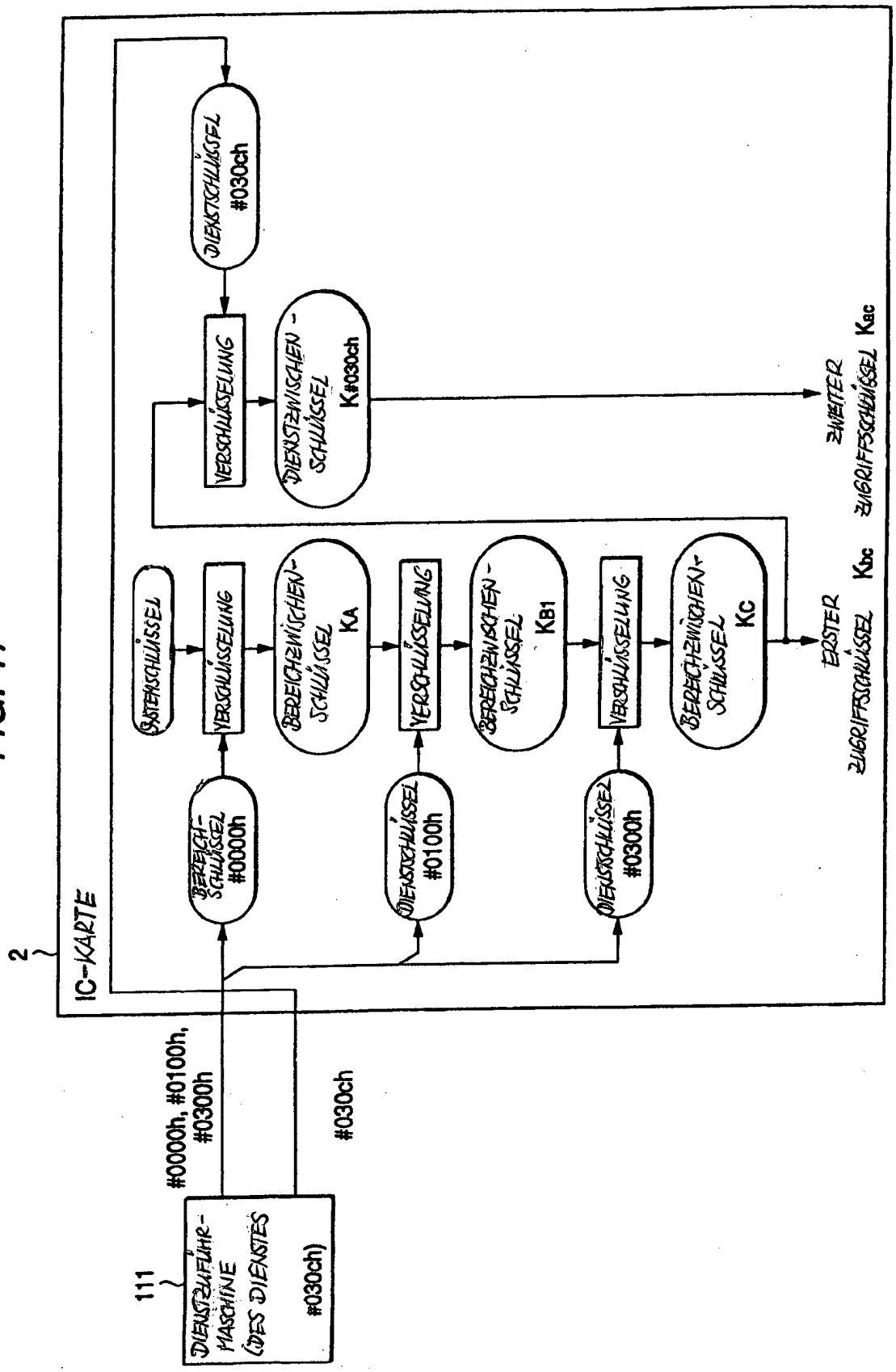

2
IC-KARTE
111
DIENSTZUFÜHR-MASCHINE (DES DIENSTES #030ch)
#0000h, #0100h, #0300h
#030ch
BASISSCHLÜSSEL
BEREICH-SCHLÜSSEL #0000h
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL KA
DIENSTSCHLÜSSEL #0100h
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL KB1
DIENSTSCHLÜSSEL #0300h
VERSCHLÜSSELUNG
BEREICHZWISCHEN-SCHLÜSSEL Kc
DIENSTSCHLÜSSEL #030ch
VERSCHLÜSSELUNG
DIENSTZWISCHEN-SCHLÜSSEL K#030ch
ZUGRIFFSSCHLÜSSEL Kbc
ZUGRIFFSSCHLÜSSEL Kac
EMPFÄNGER
SENDER

FIG. 18

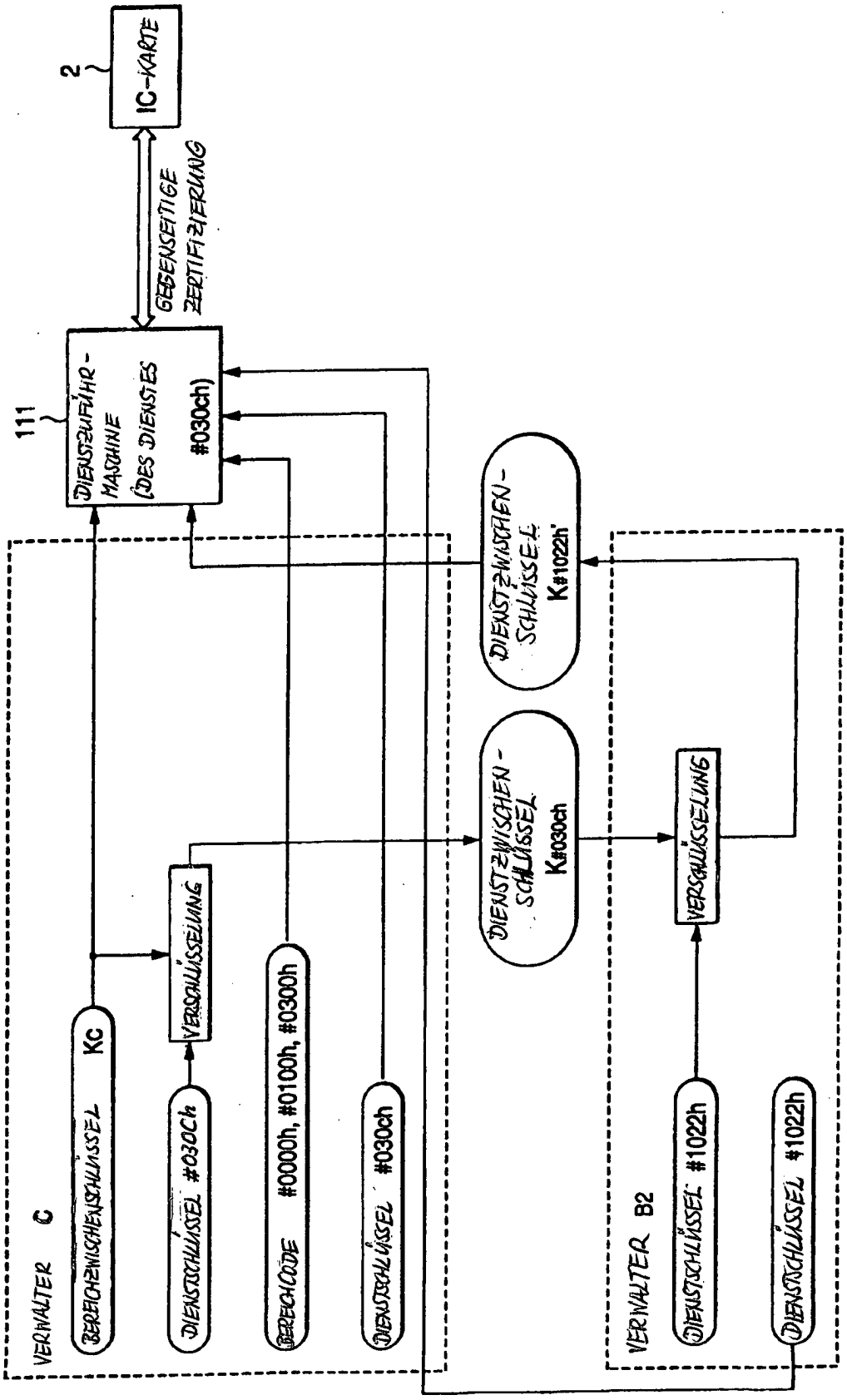

2
IC-KARTE
GEGENSEITIGE ZERTIFIZIERUNG
111
DIENSTAUSFÜHR-MASCHINE (DES DIENSTES #030ch)
VERWALTER C
BEREICHZWISCHENSCHLÜSSEL Kc
VERSCHLÜSSELUNG
DIENSTSCHLÜSSEL #030Ch
BEREICHCODE #0000h, #0100h, #0300h
DIENSTSCHLÜSSEL #030ch
DIENSTZWISCHEN-SCHLÜSSEL K#030ch
DIENSTZWISCHEN-SCHLÜSSEL K#1022h
VERSCHLÜSSELUNG
VERWALTER B2
DIENSTSCHLÜSSEL #1022h
DIENSTSCHLÜSSEL #1022h

FIG. 19

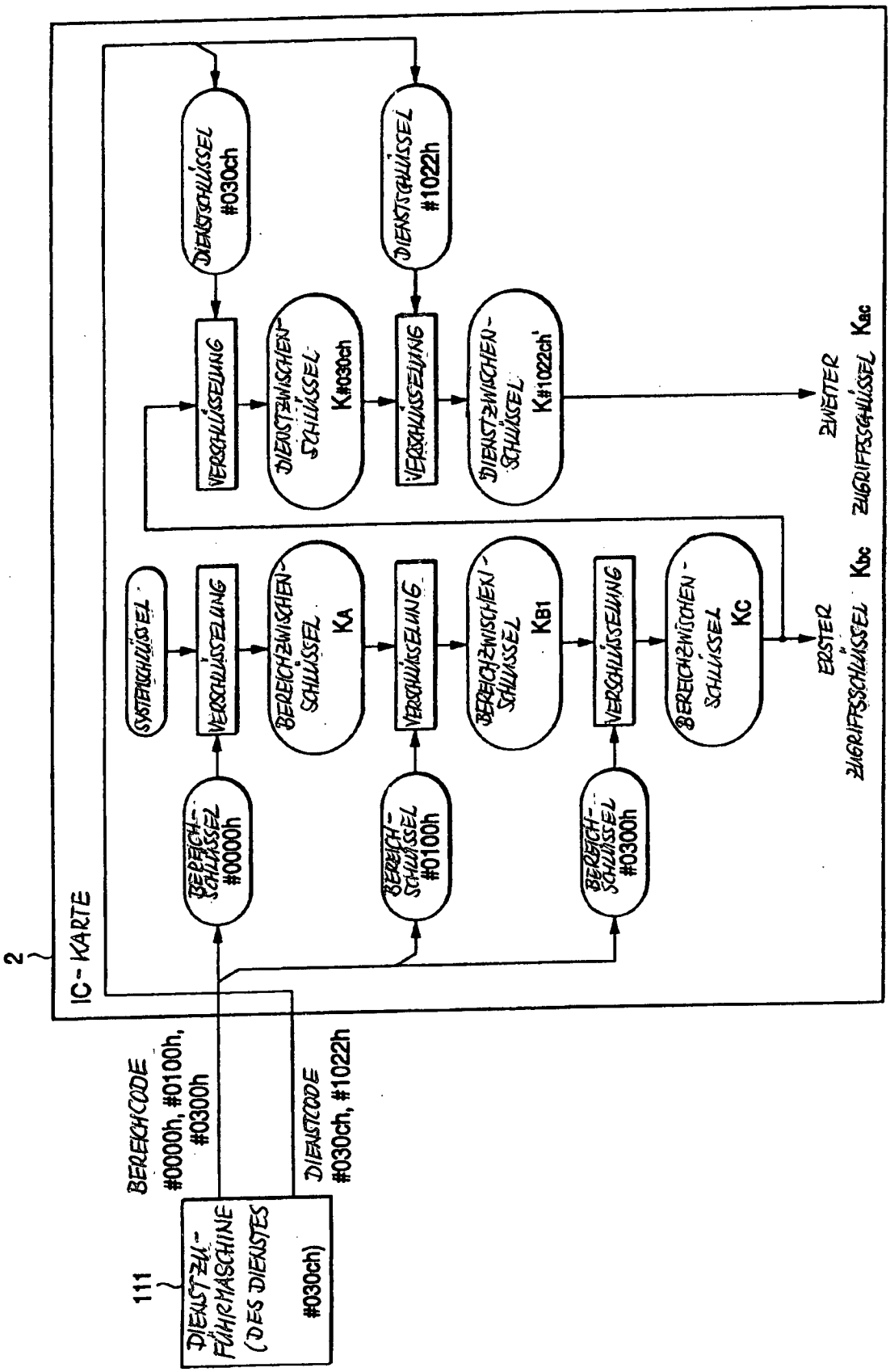

2
IC-KARTE
SYSTEMSCHLÜSSEL
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #0000h
BEREICHZWISCHEN-SCHLÜSSEL KA
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #0100h
BEREICHZWISCHEN-SCHLÜSSEL KB1
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #0300h
BEREICHZWISCHEN-SCHLÜSSEL KC
ERSTER ZUGRIFFSSCHLÜSSEL Kbc
DIENSTSCHLÜSSEL #030ch
VERSCHLÜSSELUNG
DIENSTZWISCHEN-SCHLÜSSEL K#030ch
DIENSTSCHLÜSSEL #1022h
VERSCHLÜSSELUNG
DIENSTZWISCHEN-SCHLÜSSEL K#1022ch'
ZWEITER ZUGRIFFSSCHLÜSSEL Kac
111
DIENSTZU-FÜHRMASCHINE (DES DIENSTES #030ch)
BEREICHCODE #0000h, #0100h, #0300h
DIENSTCODE #030ch, #1022h

FIG. 20

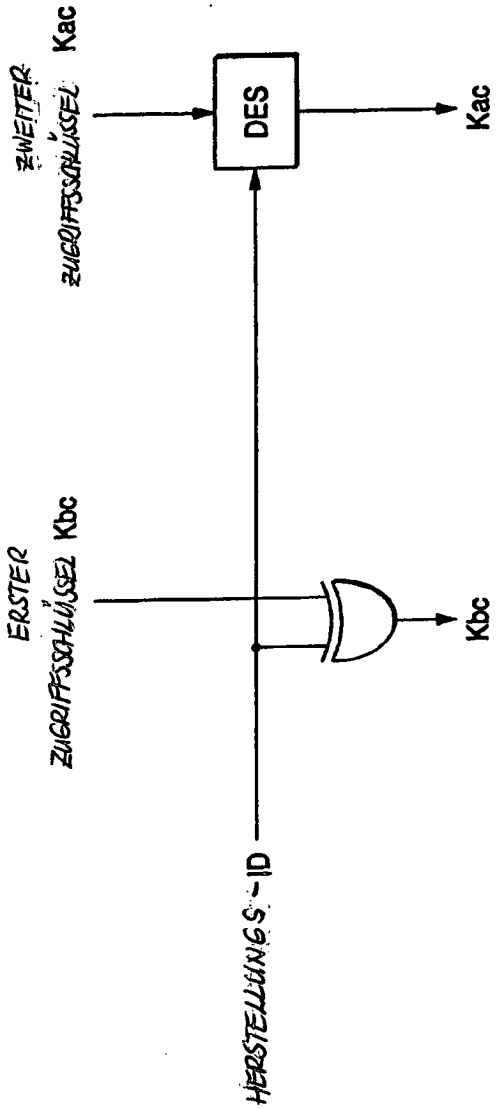

ZWEITER
ZUGRIFFSSCHLÜSSEL
Kac
DES
Kac
ERSTER
ZUGRIFFSSCHLÜSSEL
Kbc
Kbc
HERSTELLUNGS - ID

FIG. 21

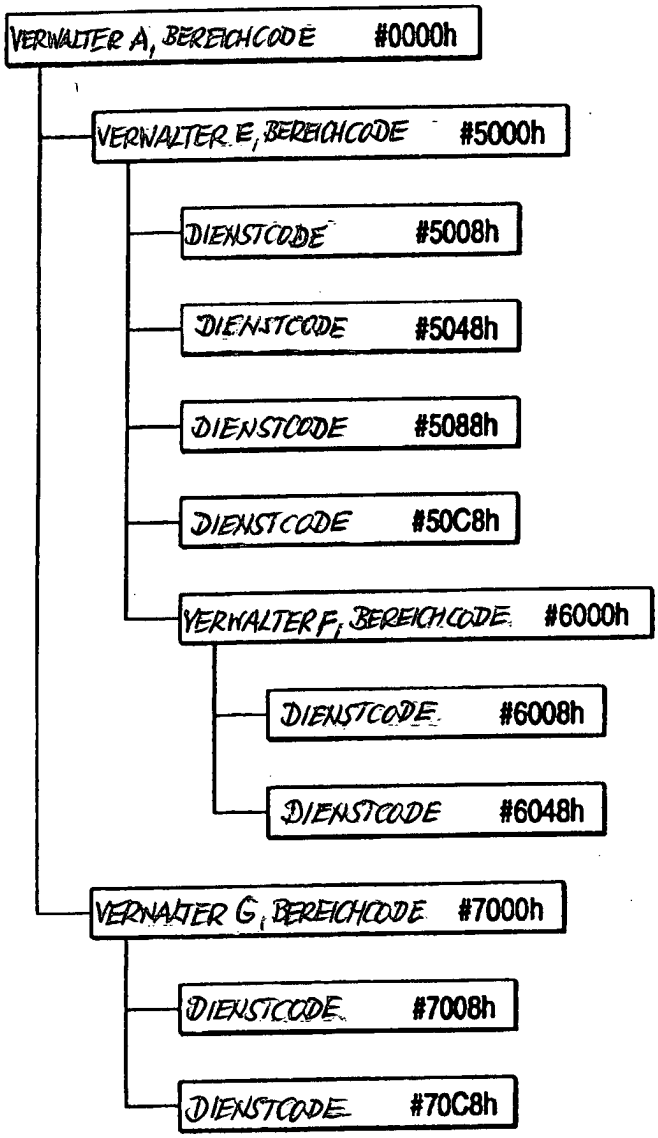

VERWALTER A, BEREICHCODE #0000h
VERWALTER E, BEREICHCODE #5000h
DIENSTCODE #5008h
DIENSTCODE #5048h
DIENSTCODE #5088h
DIENSTCODE #50C8h
VERWALTER F, BEREICHCODE #6000h
DIENSTCODE #6008h
DIENSTCODE #6048h
VERWALTER G, BEREICHCODE #7000h
DIENSTCODE #7008h
DIENSTCODE #70C8h

FIG. 22

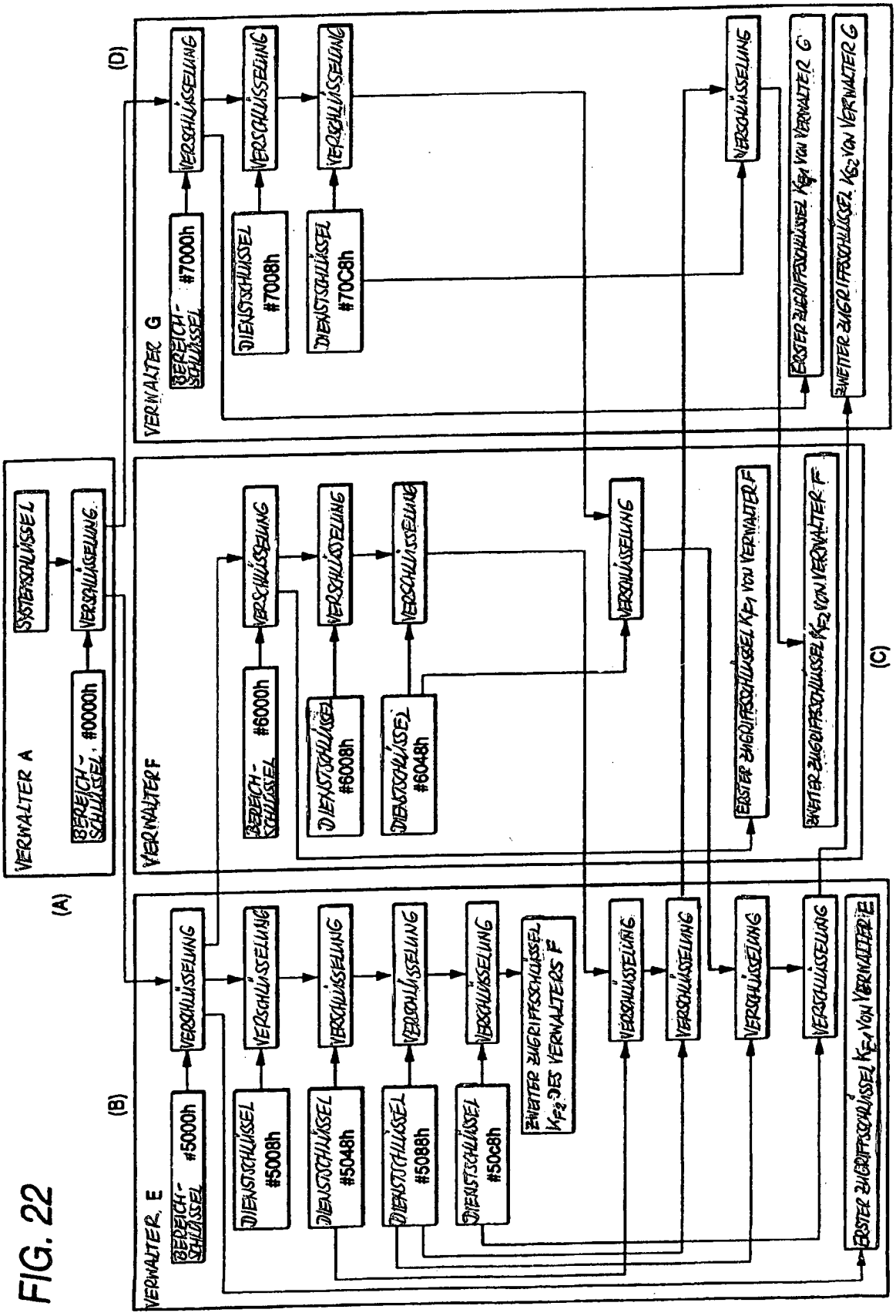

VERWALTER A
SYSTEMSCHLÜSSEL
VERSCHLÜSSELUNG
BEREICH-SCHLÜSSEL #00000h
(A)
VERWALTER F
BEREICH-SCHLÜSSEL #6000h
VERSCHLÜSSELUNG
DIENSTSCHLÜSSEL #6008h
DIENSTSCHLÜSSEL #6048h
ERSTER ZUGRIFFSSCHLÜSSEL K_{F1} VON VERWALTER F
ZWEITER ZUGRIFFSSCHLÜSSEL K_{F2} VON VERWALTER F
(C)
VERWALTER G
BEREICH-SCHLÜSSEL #7000h
DIENSTSCHLÜSSEL #7008h
DIENSTSCHLÜSSEL #70C8h
ERSTER ZUGRIFFSSCHLÜSSEL K_{G1} VON VERWALTER G
ZWEITER ZUGRIFFSSCHLÜSSEL K_{G2} VON VERWALTER G
(D)
VERWALTER E
BEREICH-SCHLÜSSEL #5000h
DIENSTSCHLÜSSEL #5008h
DIENSTSCHLÜSSEL #5048h
DIENSTSCHLÜSSEL #5088h
DIENSTSCHLÜSSEL #50C8h
ZWEITER ZUGRIFFSSCHLÜSSEL K_{E2} DES VERWALTERS F
ERSTER ZUGRIFFSSCHLÜSSEL K_{E1} VON VERWALTER E
(B)

FIG. 23

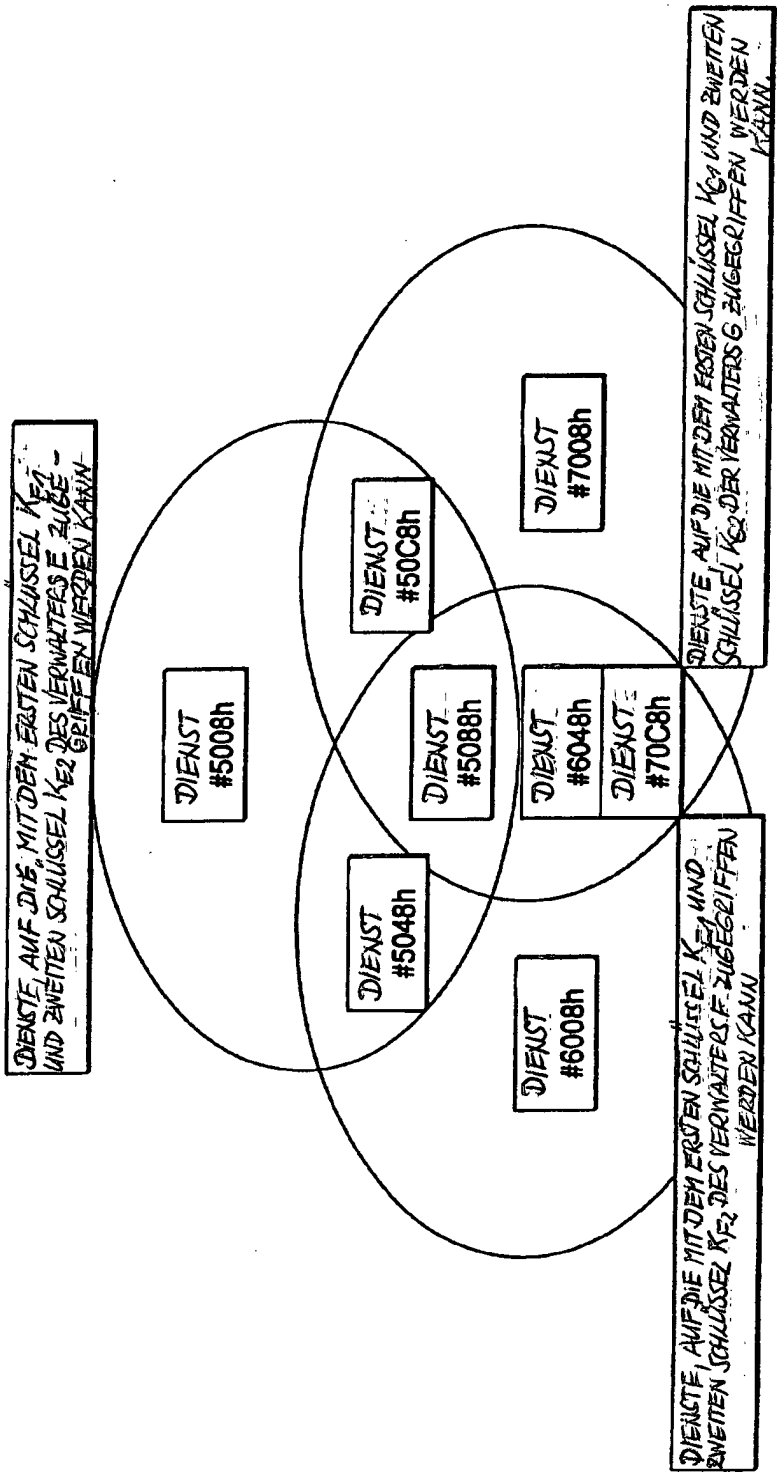

DIENSTE, AUF DIE MIT DEM ERSTEN SCHLÜSSEL K_{E1} UND ZWEITEN SCHLÜSSEL K_{E2} DES VERWALTERS E ZUGE-GRIFFEN WERDEN KANN
DIENSTE, AUF DIE MIT DEM ERSTEN SCHLÜSSEL K_{E1} UND ZWEITEN SCHLÜSSEL K_{F2} DES VERWALTERS F ZUGEGRIFFEN WERDEN KANN
DIENSTE, AUF DIE MIT DEM ERSTEN SCHLÜSSEL K_{G1} UND ZWEITEN SCHLÜSSEL K_{G2} DER VERWALTERS G ZUGEGRIFFEN WERDEN KANN
DIENST #5008h
DIENST #5048h
DIENST #6008h
DIENST #50C8h
DIENST #5088h
DIENST #7008h
DIENST #6048h
DIENST #70C8h

FIG. 24

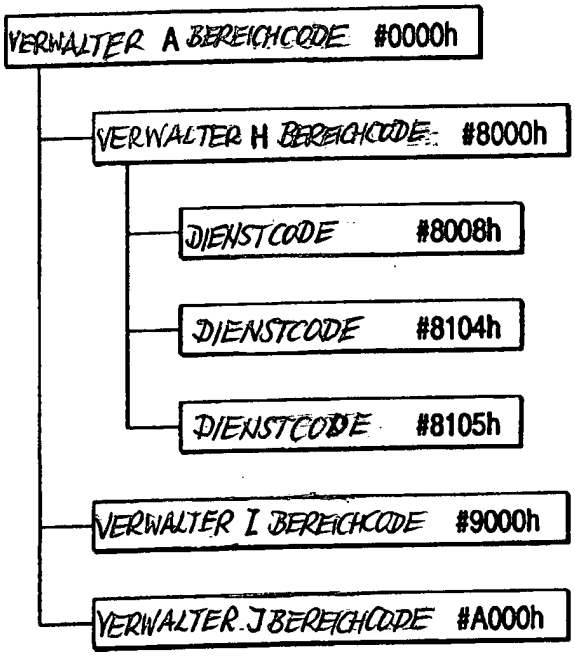
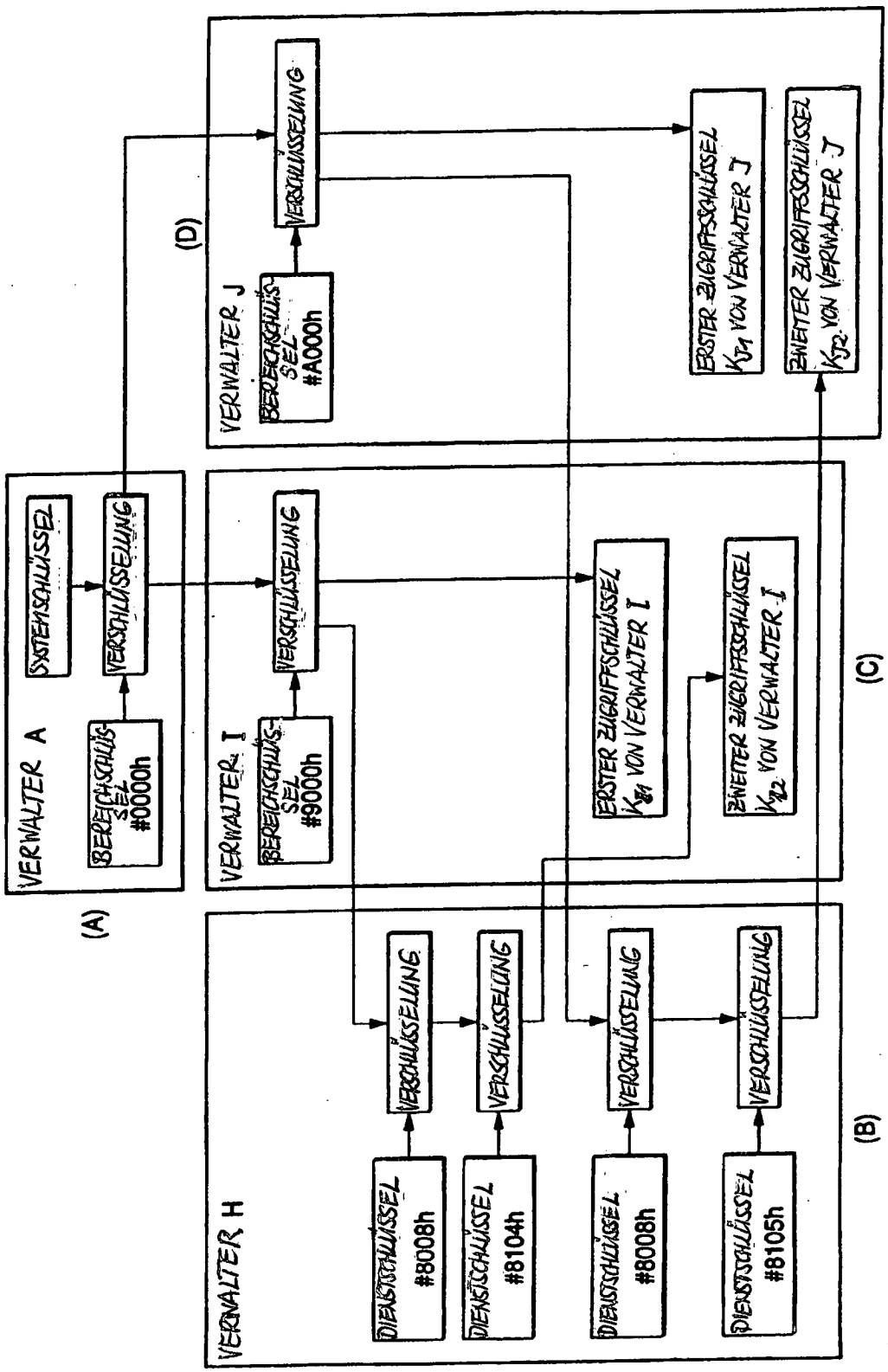

VERWALTER A BEREICHCODE #0000h
VERWALTER H BEREICHCODE #8000h
DIENSTCODE #8008h
DIENSTCODE #8104h
DIENSTCODE #8105h
VERWALTER I BEREICHCODE #9000h
VERWALTER J BEREICHCODE #A000h

FIG. 25


VERWALTER A
SYSTEMSCHLÜSSEL
VERSCHLÜSSELUNG
BEREICHSCHLÜSSEL #0000h
(A)
VERWALTER J
VERSCHLÜSSELUNG
BEREICHSCHLÜSSEL #A000h
(D)
ERSTER ZUGRIFFSSCHLÜSSEL K_{J1} VON VERWALTER J
ZWEITER ZUGRIFFSSCHLÜSSEL K_{J2} VON VERWALTER J
VERWALTER I
VERSCHLÜSSELUNG
BEREICHSCHLÜSSEL #9000h
ERSTER ZUGRIFFSSCHLÜSSEL K_{I1} VON VERWALTER I
ZWEITER ZUGRIFFSSCHLÜSSEL K_{I2} VON VERWALTER I
(C)
VERWALTER H
VERSCHLÜSSELUNG
VERSCHLÜSSELUNG
VERSCHLÜSSELUNG
VERSCHLÜSSELUNG
DIENSTSCHLÜSSEL #8008h
DIENSTSCHLÜSSEL #8104h
DIENSTSCHLÜSSEL #8008h
DIENSTSCHLÜSSEL #8105h
(B)