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

(10) **DE 698 26 318 T2** 2005.10.13

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 040 456 B1**
(21) Deutsches Aktenzeichen: **698 26 318.9**
(86) PCT-Aktenzeichen: **PCT/US98/27073**
(96) Europäisches Aktenzeichen: **98 964 134.5**
(87) PCT-Veröffentlichungs-Nr.: **WO 99/033033**
(86) PCT-Anmeldetag: **18.12.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **01.07.1999**
(97) Erstveröffentlichung durch das EPA: **04.10.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **15.09.2004**
(47) Veröffentlichungstag im Patentblatt: **13.10.2005**

(51) Int Cl.[7]: **G07F 7/10**

(30) Unionspriorität:
68196 P **19.12.1997** **US**

(84) Benannte Vertragsstaaten:
BE, DE, FR, GB

(73) Patentinhaber:
Visa International Service Association, Foster City, Calif., US

(72) Erfinder:
DAVIS, M., Virgil, Los Altos, US; ROTH, R., Janet, Oakland, US

(74) Vertreter:
Patentanwälte Hauck, Graalfs, Wehnert, Döring, Siemons, Schildberg, 20354 Hamburg

(54) Bezeichnung: **KARTENAKTIVIERUNG AN DER VERTEILUNGSSTELLE**

Beschreibung

Bereich der Erfindung

[0001] Die vorliegende Erfindung bezieht sich im Allgemeinen auf Chipkarten. Spezieller, die vorliegende Erfindung bezieht sich auf eine Technik zur Aktivierung intelligenter Karten an einem Verteilerpunkt oder einige Zeit danach.

Hintergrund der Erfindung

[0002] Chipkarten, die die Fähigkeit haben, einen Wert in einem Speicher auf einer Karte zu speichern, beziehen sich häufig auf "intelligente Zahlkarten". Intelligente Zahlkarten können entweder nach Gebrauch weggeworfen oder wieder aufgeladen werden. Insbesondere intelligente Einwegzahlkarten sind aufgrund der Wertes, den sie haben, anfällig für einen Diebstahl. Sobald eine intelligente Einwegzahlkarte mit Wert geladen worden ist, kann sie für Barzahlungen in vielen Orten benutzt werden; demnach besteht die Besorgnis, dass die Karten gestohlen werden, wenn sie einmal mit Wert geladen worden sind.

[0003] In einem Szenario werden die Karten mit Wert geladen und durch den Kartenlieferanten personalisiert. Sobald sie personalisiert und mit Wert geladen sind, "leben" sie und sind von diesem Zeitpunkt an anfällig für einen Diebstahl. Beispielsweise sind diese Karten anfällig für Diebstahl während des Versandes von dem Lieferanten zur Ausgabe, während sie an einer Ausgabestation gespeichert sind, während sie in einer Kartenausgabemaschine sind, oder zu jeder anderen Zeit bevor die Karten legal an eine Kunden verkauft werden. Falls Karten eher freihändig als an einer Maschine verkauft werden, besteht auch das Risiko, vor dem Verkauf gestohlen zu werden. Bisherige Techniken, den Kartendiebstahl zu bekämpfen, sind sowohl teuer als auch zeitaufwendig.

[0004] Viele Kartenlieferanten und Kartenausgaben verlassen sich auf Versicherungen, um die Kosten von gestohlenen Karten abzudecken. Diese zusätzliche Versicherung gegen Kartendiebstahl kann teuer sein und sind Kosten, auf die ein Kartenaussteller lieber verzichten würde. Um die Karten direkt vor Kartendiebstahl zu schützen, sind physikalische Sicherheitstechniken benutzt worden, um die geladenen intelligenten Zahlkarten vor Diebstahl zu schützen. Zum Beispiel könnten geladene Karten in gepanzerten Lastkraftwagen, in abgeschlossenen Tresoren, etc. während ihres Weges von dem Kartenlieferanten zu einer Ausgabe und schließlich zu einem legitimen Kunden transportiert werden. Die Kosten, die mit diesem sicheren Transport und dieser sicheren Lagerung verbunden sind, können ziemlich hoch sein. Die Tatsache, dass relativ wenige Kartenhersteller existieren, führt zu einem weiteren Anwachsen dieser Kosten. Daher müssen geladene Karten oft über lange Distanzen (nach Übersee, über Kontinente), transportiert werden bevor sie eine Endregion für die Verteilung erreichen. Außer den direkten Kosten für die Sicherheitsausrüstung, die für den Transport dieser Karten benötigt werden, entstehen auch Kosten, die mit den Arbeitskräften verbunden sind, die benötigt werden, um diese Karten während des Transports oder der Lagerung zu schützen.

[0005] Obgleich geladene intelligente Zahlkarten freihändig von einer Person anstatt an einer Kartenausgabemaschine verkauft werden können, kann die Kontrolle und der Lagerbestand der Ausgabe mit dem freihändigen Verkauf auch ziemlich teuer sein. Von einer Maschine verkaufte Karten würden sauberer erscheinen und würden die einfachere Lösung darstellen, obwohl teurer, werden sichere Maschinen für intelligente Zahlkarten benötigt, die schon mit Wert geladen sind. Zudem ist eine Kartenausgabemaschine, die hunderte von intelligenten Zahlkarten aufnimmt, eine Verlockung für Diebe, da jede Karte hunderte von Dollars an Wert haben kann. In bestimmten Ländern werden intelligente Zahlkarten für den Gebrauch in Telefonen öffentlich auf der Straße in Maschinen verkauft, die besonders anfällig für Diebstahl sind.

[0006] Ein System für die Ausgabe intelligenter Zahlkarten ist in der WO-A-9101538 offenbart. Hier wird eine Karte in einem behinderten Zustand ausgegeben, und die Karte zeigt an, dass ein Überprüfungscode benutzt werden könnte, die intelligente Zahlkarte zu aktivieren. Die dadurch ausgegebene Karte ist besonders für den Betrieb verschiedener Verkaufsautomaten geeignet, die Pooltabellen enthalten.

[0007] Demnach ist eine Technik wünschenswert, die nicht nur hilft, den Diebstahl intelligenter Zahlkarten zu verhindern, sondern für eine Ausgabe den Verlust minimiert, sollte eine Karte gestohlen werden. Es ist außerdem wünschenswert, für eine solche Technik die Kosten zu reduzieren, die mit der Sicherheit intelligenter Zahlkarten verbunden ist.

Zusammenfassung der Erfindung

[0008] Um das Vorhergehende zu erreichen, und in Übereinstimmung mit dem Zweck der vorliegenden Erfindung werden ein System und eine Methode, die durch den Gegenstand der Ansprüche 1 und 11 festgelegt werden, für die sichere Aktivierung intelligenter Zahlkarten an einem Verteilerpunkt an Kunden offenbart, die eine größere Sicherheit für intelligente Zahlkarten liefert und die Kosten reduziert, die mit dem Schutz dieser Zahlkarten verbunden ist.

[0009] In einer Ausführung der Erfindung, hat jede

Karte einen Standardbenutzermodus und einen Sicherheitsbenutzermodus. In dem Standardbenutzermodus wird die Karte aktiviert und ist gebrauchsfertig. In dem Sicherheitsbenutzermodus ist die Karte nicht aktiv und kann nicht in einem Zahlungsterminal benutzt werden, um einen Einkauf zu tätigen. Die Karten werden von einem Kartenlieferanten entweder in dem Standardbenutzermodus oder in dem Sicherheitsbenutzermodus personalisiert. Falls die Karte von dem Kartenlieferanten in dem Sicherheitsbenutzermodus verschickt wird, kann die Karte nicht benutzt werden, bis sie in einer Kartenausgabemaschine sofort vor ihrem Verkauf an einen kaufenden Kunden aktiviert wird. Vorteilhafterweise können die Karten nicht benutzt werden und kein Werteverlust tritt ein, falls die Karten während irgendeines Punktes in dem Transport verloren gehen oder gestohlen werden, bevor sie aktiviert werden.

[0010] In einer besonderen Ausführung der Erfindung, muss der Karte, bevor sie aktiviert wird, ein Sicherheitscode vorgelegt werden. Vorteilhafterweise wird der Sicherheitscode auf sichere Art und Weise durch eine Kartenausgabemaschine oder andere Vorrichtungen nur unter Berechtigung durch eine Ausgabe vor dem Kartenverkauf an einen Kunden erzeugt. Es wird vermutet, dass die Kostenersparnis pro Karte durch Anwendung dieser Technik zwischen $0.05 und $0.75 pro Karte liegen.

[0011] In einer weiteren Ausführung der Erfindung wird ein Aktivierungskontrollzähler (ACC) in einem Aktivierungssicherheitsanwendungsmodul (ASAM) in der Kartenausgabemaschine gespeichert. Der Aktivierungskontrollzähler wird bei jedem Aktivierungsversuch der Karte dekrementiert, erfolgreich oder nicht. Der Aktivierungskontrollzähler begrenzt durch Beschränkung der Versuche, die Karte zu aktivieren, dem Betrug und dem Diebstahl ausgesetzt zu sein.

[0012] In einer weiteren Ausführung werden die Aktivierungssicherheitsanwendungsmodule in dem Feld (d.h. in den Kartenausgabemaschinen) gewartet, um von dem Erfordernis abzusehen, ein Aktivierungssicherheitsanwendungsmodul an einen zentralen Ort für die Wartung zurückzuschicken oder einen Computer zu einer Ausgabemaschine zurückzubringen. Ein Feldsicherheitsmodul (FSAM) wird an dem Aktivierungssteuerungscomputer erzeugt und ist in der Lage, eine begrenzte Zahl von Aktivierungssicherheitsanwendungsmodulen zu aktualisieren. Vorzugsweise wird in einem Kontrollsicherheitsmodul (CSAM), in dem Feldsicherheitsmodul und in dem Aktivierungssicherheitsanwendungsmodul eine Hierarchie von Schlüsseln benutzt, um die Sicherheit zu gewährleisten.

Kurze Beschreibung der Zeichnungen

[0013] Die Erfindung, zusammen mit weiteren bevorzugten Ausführungsformen, können unter Bezugnahme der folgenden Beschreibung in Verbindung mit den begleitenden Zeichnungen am besten verstanden werden, in denen

[0014] Fig. 1 symbolisch ein Aktivierungssystem für intelligente Zahlkarten gemäß einer Ausführung der Erfindung veranschaulicht.

[0015] Fig. 2 ein Beispiel von Inhalten eines Speichers einer intelligenten Zahlkarte veranschaulicht, der brauchbar für eine Realisierung einer Ausführung der vorliegenden Erfindung ist.

[0016] Fig. 3 ein Ablaufschema ist, welches beschreibt, wie eine Karte gemäß einer Ausführung der vorliegenden Erfindung erzeugt wird.

[0017] Fig. 4 eine Anordnung für die Erzeugung eines Aktivierungssicherheitsanwendungsmoduls (ASAM) veranschaulicht.

[0018] Fig. 5 ein Ablaufschema ist, das eine Technik der Erzeugung eines Aktivierungssicherheitsanwendungsmoduls beschreibt.

[0019] Fig. 6 ein Ablaufschema ist, das eine Technik der Wartungsdurchführung eines Aktivierungssicherheitsanwendungsmoduls ist.

[0020] Fig. 7 detaillierter eine Kartenausgabemaschine veranschaulicht.

[0021] die Fig. 8A und Fig. 8B Ablaufschemata sind, die einen Prozess beschreiben, durch den eine Karte in einer Maschine, die ein Aktivierungssicherheitsanwendungsmodul benutzt, aktiviert wird.

[0022] Fig. 9 ein Szenario veranschaulicht, in dem eine Karte aktiviert wird, die ein entferntes Aktivierungssicherheitsanwendungsmodul verwendet.

[0023] Fig. 10 ein Szenario veranschaulicht, in dem eine Feldwartung an einem Aktivierungssicherheitsanwendungsmodul durchgeführt wird.

[0024] Fig. 11 eine Schlüsselhierarchie veranschaulicht, durch die die Feldsicherheitsmodule eine Wartung an einem Teil sämtlicher Aktivierungssicherheitsanwendungsmodule in dem Feld durchführen.

[0025] Fig. 12 eine mögliche Sicherheitsausführung präsentiert, die die Information veranschaulicht, die in einem Aktivierungssteuerungscomputer (AM) und in einem Kontrollsicherheitsmodul enthalten sind.

[0026] die Fig. 13 und Fig. 14 ein Computersystem veranschaulichen, das geeignet ist, die Ausführungen der vorliegenden Erfindung zu realisieren.

Detaillierte Beschreibung der Erfindung

Hintergrund von intelligenten Karten

[0027] Die vorliegende Erfindung ist anwendbar auf Chipkarten. Auch werden sie IC-Karten, Karten mit integrierter Schaltung, Speicherkarten, Prozessorkarten genannt. Eine Chipkarte ist typischerweise eine kreditkartengroße Plastikkarte, die eine oder mehrere integrierte Halbleiterschaltungen enthält. Eine Chipkarte kann mit Kassenterminals, Geldautomaten oder Kartenlesern, die in einen Computer integriert sind, an Telefone, Verkaufsautomaten oder mit vielfältigen anderen Vorrichtungen koppeln. Die Chipkarten können mit verschiedenen Arten von Funktionsfähigkeiten programmiert sein, wie beispielsweise Zahlkartenverwendung (eine „Intelligente Zahlkarte), Kredit- oder Guthabenverwendung, Treueverwendung, Kartenhalterinformation usw. Obwohl eine Plastikkarte gegenwärtig das auserwählte Medium für Chipkarten ist, ist daran zu denken, dass Chipkarten in einem kleineren Format realisiert werden, an einer Schlüsselkette befestigt werden oder klein wie ein Chipmodul sein können. Eine Chipkarte kann auch als Teil eines PDA-Computers, eines Telefons realisiert sein oder eine andere Form annehmen. Die untere Beschreibung liefert ein Beispiel möglicher Elemente von Chipkarten, obgleich die vorliegende Erfindung auf einen weiten Bereich von Chipkartentypen anwendbar ist, und speziell auf intelligente Zahlkarten.

[0028] Eine Chipkarte kann einen Mikroprozessor, einen Arbeitsspeicher, einen Festspeicher, einen nichtflüchtigen Speicher, ein Verschlüsselungsmodul (oder arithmetische Einheit) und eine Kartenleser- (oder Terminal-) Schnittstelle enthalten. Andere Merkmale können vorhanden sein wie beispielsweise optische Speicher, elektrisch löschbare programmierbare Flash Festspeicher, ferroelektrische Arbeitsspeicher, Zeitgeber, Zufallszahlengenerator, Unterbrechungsgenerator, Steuerlogik, Ladungspumpe, Stromanschlüsse und Schnittstellenkontakte, die die Kommunikation der Karte mit der Außenwelt erlauben. Natürlich kann eine Chipkarte auf viele Arten realisiert sein, und braucht nicht notwendig einen Mikroprozessor oder andere Merkmale enthalten.

[0029] Der Mikroprozessor ist jede geeignete zentrale Verarbeitungseinheit für die Ausführung von Befehlen und die Kontrolle der Vorrichtung. Arbeitsspeicher dienen als vorübergehende Speicher für berechnete Ergebnisse und als Stapelspeicher. Festspeicher speichern das Betriebssystem, feste Daten, Standard-Routinen, Verweistabellen und andere dauerhafte Informationen. Nichtflüchtige Speicher (wie beispielsweise EPROM oder EEPROM) dienen dazu, Information zu speichern, die nicht verloren sein muss, wenn die Karte von der Energiequelle getrennt ist, die aber auch abänderbar sein muss, um Daten speziell auf individuelle Karten auszulegen, oder sich eventuell während der Kartenlebensdauer ändern. Diese Informationen enthalten eine Kartenidentifikationsnummer, eine persönliche Identifikationsnummer, Berechtigungsstufen, Barguthaben, Kredithöchstgrenzen und andere Informationen, die mit der Zeit nötig sein könnten. Ein Verschlüsselungsmodul ist ein optionaler technischer Baustein, der für die Durchführung verschiedener Verschlüsselungsalgorithmen benutzt wird. Natürlich kann die Durchführung der Verschlüsselung auch in Software durchgeführt werden. Applied Cryptography, Bruce Schneier, John Wiley & Sons, Inc., 1996 diskutieren geeignete Verschlüsselungsalgorithmen und wird hiermit als Referenz aufgenommen.

[0030] Die Kartenleseschnittstelle enthält die Software und Hardware, die notwendig für die Kommunikation mit der Außenwelt sind. Ein breites Spektrum von Schnittstellen ist möglich. Beispielsweise könnte die Schnittstelle eine Kontaktschnittstelle, eine nahegekoppelte Schnittstelle, eine ferngekoppelte Schnittstelle oder verschiedene andere Schnittstelle bereitstellen. Mit einer Kontaktschnittstelle werden Signale von einem integrierten Schaltkreis zu einer Zahl von metallischen Kontakten auf der Außenseite der Karte geleitet, welche in physikalischem Kontakt mit ähnlichen Kontakten einer Kartenlesevorrichtung kommen. Eine Chipkarte kann einen herkömmlichen Magnetstreifen enthalten, um Kompatibilität mit herkömmlichen Kartenlesevorrichtungen und Anwendungen zur Verfügung zu stellen, und kann selbst auch eine Kopie der Magnetstreifeninformation in dem integrierten Schaltkreis für Kompatibilität liefern.

[0031] Verschiedene mechanische und elektrische Eigenschaften einer Chipkarte und Aspekte ihrer Wechselwirkung mit einer Kartenlesevorrichtung werden in Smart Card Handbook, W. Rankl and W. Effing, John Wiley & Sons, Ltd., 1997 beschrieben, und durch die folgenden Beschreibungen definiert, die hier alle als Referenzen aufgenommen werden: Visa Integrated Circuit Card Specification, Visa International Service Association, 1996; EMV Integrated Circuit Card Specification for Payment Systems, EMV Integrated Circuit Terminal Specification for Payment Systems, EMV Integrated Circuit Card Application Specification for Payment Systems, Visa International, Mastercard, Europay, 1996, und International Standard; Identification Cards-Integrated Circuit(s) Cards with Contacts, Parts 1-6, International Standards Organization 1987-1995.

Systemüberblick

[0032] Fig. 1 veranschaulicht symbolisch ein Aktivierungssystem **10** intelligenter Zahlkarten gemäß einer Ausführungsform der Erfindung. In dem System eingeschlossen sind eine Ausgabe **20**, ein Kartenlieferant **22** und eine Kartenausgabemaschine **24**. Eine

intelligente Zahlkarte **30** wird schließlich durch Anwendung eines Ausgabeaktivierungsschlüssels **40** aktiviert und dem Kunden **26** mittels der Kartenausgabemaschine **24** ausgegeben.

[0033] Die Ausgabe **20** erhält Karten von dem Kartenlieferanten **22** und gibt diese Karten dann dem Kunden aus. Die Ausgabe **20** kann jedes geeignete Ausgabeobjekt wie eine Bank, eine Finanzinstitution, eine Dienstleistungsgesellschaft, ein Händler, oder andere Organisationen, oder sogar ein Bevollmächtigter, der für die Ausgabe handelt, sein.

[0034] Der Kartenlieferant **22** kann jeder geeignete Lieferant von intelligenten Zahlkarten sein. Ein Kartenlieferant kann jeder aus dem breiten Spektrum der Kartenhersteller wie Gemplus, Schlumberger, Bull, G&D, etc sein. Abhängig von der Karte führt der Lieferant häufig die Karteninitialisierung und vielleicht die Personalisierung der Karte aus.

[0035] Die Kartenausgabemaschine **24** kann jede geeignete Vorrichtung sein, die für die Aufnahme intelligenter Zahlkarten und die Ausgabe der Karten an Kunden eingerichtet ist. Eine Ausführungsform der Erfindung wird benutzt, um die Karten, während sie in der Maschine sind, zu aktivieren. Beispielsweise ist eine Kartenausgabemaschine (CDM) **24** jede in der Technik bekannte geeignete Kartenausgabemaschine wie sie von G&D und Schlumberger hergestellt werden. Solche Ausgabemaschinen verkaufen automatisch intelligente Zahlkarten von verschiedenartigen Werteinheiten an Kunden, die Geld in die Maschine einzahlen. Intelligente Zahlkarten können an einer Kartenausgabemaschine bar, mit einer Kreditkarte, mit einer Kundenkarte oder einer anderen geeigneten Zahlungsmittel eingekauft werden. Ausgabemaschinen sind auch imstande, durch Gebrauch geeigneter Kommunikationsnetzwerke on-line zu gehen, um Kapital zu prüfen, den Kreditverkehr durchzuführen, ein Konto zu belasten, etc.

[0036] Die Funktionen der Kartenausgabemaschine **24** können auch von einem Kassierer, der ein Kartenterminal benutzt, ausgeführt werden. In diesem Szenario, kauft der Kunde **26** eine intelligente Zahlkarte eher von dem Kassierer als von der automatischen Maschine. Gegen Bezahlung des Kunden führt der Kassierer die gekaufte intelligente Zahlkarte in das Kartenterminal, die Karte wird durch Anwendung einer Ausführungsform der vorliegenden Erfindung aktiviert, und die Karte wird darauf von dem Kassierer an den Kunden ausgehändigt. Die Kartenausgabemaschine **24** kann auch die Form eines vergrößerten POS Terminals oder einer personalisierten Batch-Maschine haben. Eine Kartenausgabemaschine **24** kann auch mit einer anderen Vorrichtung als mit einem Bankautomaten in Verbindung gebracht werden. Zusätzlich zur Fähigkeit, intelligente Zahlkarten zu aktivieren und auszugeben, kann die Kartenausgabemaschine **24** auch andere Funktionen enthalten, wie die Fähigkeit wieder aufladbare Karten zu laden und Waren zu verkaufen.

[0037] Es wird auch beabsichtigt, dass die Funktionen der Kartenausgabemaschine **24** in verschiedene Teile zerlegt werden. Eine einfache Ausgabemaschine oder andere Hilfsmittel können verwendet werden, um die nicht aktivierten Karten an den Kunden auszugeben, der die Karte, um eine aktivierte Karte zu haben, zu einem anderen Kartenterminal bringt. Zum Beispiel kann ein Kunde eine nicht aktivierte intelligente Zahlkarte durch Kauf aus einer Maschine erhalten, durch Verteilung seitens einer Bank oder eines Händlers oder durch eine Postsendung. Der Kunde kann dann die nicht aktivierte Karte in einen Kartenleser einführen, der an einem Personalcomputer angebracht ist, der dann die Aktivierung der Karte durch Anwendung einer Ausführungsform der Erfindung über das Internet oder ein anderes Nachrichtennetz ausführt. Der Kunde kann die Karte vorausbezahlt haben, oder die Karte kann nur durch entsprechende Zahlung durch den Kunden über das Internet aktiviert werden. Ein Kunde kann auch eine nicht aktivierte Karte, die anderswoher erhalten wird, zu einer Kartenausgabemaschine bringen, die dann imstande ist, die Karte zu aktivieren.

[0038] Wenn die die intelligente Zahlkarte **30** durch einen Kartenliefereranten **22** produziert wird, wird die intelligente Zahlkarte **30** nicht aktiviert, auch wenn sie mit Wert geladen sein kann. (Natürlich kann der Kartenlieferant **22** auch Karten produzieren, die aktiviert sind). In Verbindung mit einem Ausgabeaktivierungsschlüssel **40**, produziert der Kartenlieferant **22** einen Sicherheitscode, der auf der intelligenten Zahlkarte **30** gespeichert ist. Der Ausgabeaktivierungsschlüssel **40** wird auch zur Kartenausgabemaschine **24** weitergeleitet. Die intelligente Zahlkarte **30** kann dann zur Ausgabe **20** transportiert werden, gespeichert und schließlich innerhalb der Kartenausgabemaschine **24** aufgenommen werden, ohne wesentliches Risiko des Diebstahls, da die Karte nicht aktiviert ist und für eine Einkauf nicht genutzt werden kann. Wenn der Kunde mit der Kartenausgabemaschine **24** interagiert, um eine intelligente Zahlkarte **30** zu kaufen, wird der Ausgabeaktivierungsschlüssel **40** innerhalb der Kartenausgabemaschine **24** benutzt, um den Sicherheitscode zu reproduzieren und die intelligente Zahlkarte **30** zu aktivieren, so dass der Wert, der darauf geladen ist, für den Gebrauch zugänglich ist. Die intelligente Zahlkarte **30** wird dann an den Kunden **26** gegen Bezahlung ausgehändigt.

[0039] Die intelligente Zahlkarte **30** ist jede geeignete intelligente Karte, die imstande ist, Werte zu speichern. Vorzugsweise ist die intelligente Zahlkarte **30** eine Speicherkarte, obgleich die intelligente Zahlkarte auch eine Prozessorkarte sein kann, die zusätzlich zum Speicher für das Speichern von Werten andere

Funktionen haben kann. In einer speziellen Ausführung der Erfindung ist die intelligente Zahlkarte **30** eine intelligente Einwegzahlkarte. Andere Details für eine spezielle Ausführung der Erfindung werden in "Visa International CAD/Service Payment Terminal Specification", erhältlich von Visa International, Foster City, California, zur Verfügung gestellt.

[0040] Die unteren Ausführungen beschreiben durch Anwendung spezieller verschlüsselter Algorithmen spezielle Sicherheitsrealisierungen. Im Allgemeinen kann jede geeignete Verschlüsselungstechnik, die den Sicherheitsbedürfnissen entspricht, für die Erzeugung von Schlüsseln und die Verschlüsselung von geheimen Informationen benutzt werden. Die unteren Angaben dienen als ein Beispiel.

Kartenspeicherbeispiel

[0041] Fig. 2 veranschaulicht ein Beispiel eines Speichers **50** für die intelligente Zahlkarte, der brauchbar für eine Realisierung einer Ausführung der vorliegenden Erfindung ist. Der Speicher **50** ist repräsentativ für die möglichen Inhalte des Speichers **50**, die gezeigten Inhalte können in anderen Zuständen und Formen gezeigt werden während sie die vorliegende Erfindung noch umfassen. Andere Hardwarerealisierungen und Implementierungen, die Software benutzen, sind für den Speicher auch möglich. In diesem Beispiel werden verschiedene Flags, Codes, Versionen, etc., benutzt, um den Kartenmodus für einen sicheren Transport zu kontrollieren. Andere sichere Techniken und der Gebrauch von Schlüsseln können auch benutzt werden, um den Wert auf einer Karte zu schützen, währen sie transportiert und gespeichert wird.

[0042] Für Speicherkarten sind ISO Byte H1 60 und ISO Byte H2 62 Standardinformationsbytes, die für die Erkennung des Kartentyps benutzt werden. Zum Beispiel können die Bytes **60** und **62** benutzt werden, um die intelligente Zahlkarte zu erkennen, da sie besondere Chips hat. Für Prozessoren und andere Karten sind diese ISO Bytes nicht erforderlich. Ein Ausgabeidentifikator **64** erkennt die Ausgabe der Karte. Ausschließlich ein Lieferantenindentifikator **68** erkennt den Kartenlieferanten. Eine Kartenseriennummer **69** ist eine Kartenidentifikationsnummer für die Karte. Ein Fehlerzähler **70** ist ein Zähler, der zählt, wie oft eine Karte zum Vergleich mit einem Sicherheitscode vorgelegt wird. In einer Ausführung ist nur eine spezielle Anzahl von Versuchen erlaubt, der Karte den Sicherheitscode vorzulegen. Wenn diese Versuche erschöpft sind, wird die Karte nicht länger einen Sicherheitscode für den Vergleich akzeptieren. Dieses Merkmal hindert einen gewissenlosen Einzelnen vor dem wiederholten Versuch, den Sicherheitscode der Karte durch Anwendung automatischer Hilfsmittel wie ein Computerprogramm zu knacken.

[0043] Der Kartensicherheitscode **72** ist jeder geeigneter Code, der auf der Karte gespeichert ist und die Karte vor einer Aktivierung, außer durch eine berechtigte Person, schützt. Wenn eine berechtigte Person der Karte den korrekten Sicherheitscode, der mit dem Kartensicherheitscode **72** des Speichers **50** übereinstimmt, vorlegt, dann kann die Karte aktiviert werden. Der Kartensicherheitscode **72** kann jeden geeigneten Wert und jedes Format haben. Beispielsweise kann der Code ein vordefinierter konstanter Wert sein, der für alle Karten der gleiche ist, oder ein Wert, der von spezifischen Kartendaten abgeleitet wird, die einen eindeutigen Wert pro Karte erzeugen. Die Sicherheitscodeversion **74** ist ein Wert, der dem Ausgabeaktivierungsschlüssel **40** durch die Ausgabe **20** zugewiesen ist. Dieses Datenelement wird dem Kartenlieferanten **22** durch die Ausgabe **20** zusammen mit dem Ausgabeaktivierungsschlüssel **40** zur Verfügung gestellt, um es bei der Erzeugung von Kartensicherheitscodes anzuwenden. Die Sicherheitscodeversion **74** gibt eine spezielle Version für den Ausgabeaktivierungsschlüssel **40** an und ist nützlich, wenn mehr als eine Version eines Aktivierungsschlüssels innerhalb des Systems in Gebrauch ist. Zum Beispiel kann die Ausgabe **20** durch Anwendung eines neuen Aktivierungsschlüssels starten, Karten jedoch, die auf dem älteren Aktivierungsschlüssel basieren, können noch innerhalb des Systems sein, um darauf zu warten, ausgegeben zu werden. In diesem Szenario ist die Sicherheitscodeversion **74** für Unterscheidung zwischen mehreren verschiedenen Aktivierungsschlüsseln nützlich, der der geeignete Schlüssel für den Gebrauch mit der intelligenten Zahlkarte **30** ist.

[0044] Der Ausgabeflag **76** zeigt an, ob Daten innerhalb des Speichers **50** modifiziert werden können. Ist anfangs 0 gesetzt ("Ausgabemodus" angezeigt), ist der Kartenlieferant **22** frei, Daten in den Speicher zu schreiben. Der Ausgabemodus kann für eine sicheren Transport einer Karte von einem Chiphersteller zu einem Kartenhersteller (falls nötig) benutzt werden. Sobald der Ausgabeflag **76** auf 1 gesetzt wird, können verschiedene Bereiche innerhalb des Speichers nicht länger modifiziert werden. Zum Beispiel können der Kartensicherheitscode **72** und die Sicherheitscodeversion **74** nicht modifiziert werden, sobald der Ausgabeflag **76** auf 1 gesetzt worden ist. Der Sicherheitsflag **78** zeigt einen Kartenmodus an. In diesem Beispiel, wenn der Sicherheitsflag **78** auf 0 gesetzt ist, ist die Karte in dem Standardbenutzermodus und kann für den Einkauf gebraucht werden. Wenn der Sicherheitsflag **78** auf 1 gesetzt ist, ist die Karte in dem Sicherheitsbenutzermodus und sein Wert kann nicht benutzt werden. Der Bereich **80** wird für die Speicherung des Wertes auf der intelligenten Zahlkarte **30** gebraucht. Andere Bereiche **82** können für andere Verwendungszwecke gebraucht werden wie zum Beispiel für die zusätzliche Personalisierung von Daten, andere Codes, einen Authentifizierungs-

schlüssel, einen Antwortzähler und andere Daten und Flags.

[0045] In einer spezifischen Ausführung der Erfindung kann die Karte die folgenden Modi enthalten. In dem Ausgabemodus wird der Zugang zum Speicher durch einen 4-Byte Transportcode gesichert. Wie oben diskutiert, schützt, während er im Sicherheitsbenutzermodus ist, ein 4-Byte Sicherheitscode den Speicher, und ein 2-Byte Zugangscode (Benutzercode) schützt den Speicher, während er in dem Standardbenutzermodus ist. Zugang zu speziellen bereichen ist nur erlaubt, nachdem der Chip den Code, der vorgelegt wird, verifiziert hat. Zum Beispiel während des Ausgabemodus wird der Sicherheitscode als Verschlüsselungstransportcode benutzt, und der Zugang ist nur zum Fehlerzähler und zu ausgewählten Datenbereichen erlaubt. Während des Sicherheitsbenutzermodus ist der Ausgabeflag eingestellt und eine weitere Programmierung der Kartenidentifikationsbereichen ist nicht erlaubt. Im normalen Gebrauch, wenn die Karte im Standardbenutzermodus ist (Ausgabe- und Sicherheitsflagseinstellungen), muss der Benutzercode vorgelegt sein, bevor der Wert auf der Karte dekrementiert werden kann. Abhängig vom Modus sind verschiedene Bereiche des Speichers vorzugsweise entweder im Festspeicher, im programmierbaren Speicher oder im elektrisch löschbaren Speicher. Beispielsweise ist während des Ausgabemodus die Personalisierung der Daten programmierbar fest gespeichert, aber fest gespeichert in anderen Modi. Vorzugsweise sind die Ausgabe und die Sicherheitsflags programmierbar festgespeichert in sämtlichen Modi.

[0046] Wenn die vorliegende Erfindung mit vorausbezahlten Zahlungsanwendungen gebraucht wird, funktioniert die Speicherkarte gut. In einer Ausführung enthält die die Speicherkarte eine Kontrolleinheit (die eine Schnittstelle zu den Kartenkontakten zur Verfügung stellt), verschiedene Flags, eine Speicherzugangskontrolleinheit (die einen Fehlerzähler, einen Sicherheitscode und einen Benutzercode enthält), eine Authentifizierungseinheit (die einen Authentifizierungsschlüssel und einen Antwortzähler enthält), eine Speichereinheit (mit einem elektrisch löschbaren programmierbaren Festspeicher, einem Benutzerspeicher und einem Löschzähler), und eine Programmierungseinheit. Die Authentifizierungseinheit ist eine Hochsicherheitsverschlüsselungseinheit, die eine Authentifizierung mit Abfrage und Antwort erlaubt, und ein Einzelschlüssel.

Kartenproduktionsablaufschema

[0047] Fig. 3 ist ein Ablaufschema, das beschreibt, wie eine Karte gemäß einer Ausführung der Erfindung hergestellt wird. Die Herstellung von mehreren Karten würde dieselbe Vorgehensweise benutzen. In Schritt **102** bettet ein Kartenhersteller einen Chip in die intelligente Karte ein. Ein solcher Fachmann wird zu würdigen wissen, dass dieser Schritt durch jeden geeigneten Kartenhersteller durch Gebrauch verschiedener Chips und auf unterschiedliche Weise durchgeführt werden kann. Beispielsweise ist jeder Chip, der in die intelligente Karte eingebettet wird, jeder geeignete integrierte Schaltkreis und ist vorzugsweise ein Speicherchip. Beispiele für Chips, die benutzt werden können, sind solche, die von Siemens hergestellt werden. Am besten enthält der integrierte Chip zumindest die Kartenspeicherübersicht **50** der Fig. 2.

[0048] Schritt **104** initialisiert und personalisiert die Karte. Im Gegensatz zu einer Kreditkarte, die für ein spezielles Individuum personalisiert wird, wird eine intelligente Zahlkarte typischerweise durch Hinzufügung von Grafiken zur Karte personalisiert. Auch werden verschiedene Datenbereiche in dem Speicher **50** der Karte initialisiert. Beispielsweise werden die bereiche **60** und **62** initialisiert, um den Typen des Chips auf der Karte zu identifizieren, der Bereich **64** wird mit dem Ausgabeidentifikator initialisiert, ein Lieferantenidentifikator wird auf den Bereich **68** geschrieben, ein Fehlerzähler **70** wird auf 0 initialisiert. Vorzugsweise wird das Sicherheitsflag an diesem Punkt auf 1 gesetzt, um anzuzeigen, dass die Karte im Sicherheitsbenutzermodus ist und nicht bis zur Aktivierung benutzt wird. Diese Merkmal hindert einen Dieb eine Karte zu benutzen, die gestohlen worden ist. Zusätzlich speichert der Kartenlieferant den speziellen Wert in die Region **80**, der der intelligenten Zahlkarte zugeordnet ist.

[0049] An diesem Punkt kann der Kartensicherheitscode **72** auf der Karte installiert werden, um nur einem autorisierten Beteiligten zu erlauben, die Karte zu aktivieren. Die Erzeugung eines Sicherheitscodes, sein spezieller Wert und seine Installation auf der Karte kann auf vielfältige Art und Weise durchgeführt werden. Beispielsweise liefern die folgende Schritte eine Technik zur Erzeugung und Installation eines Sicherheitscodes.

[0050] In Schritt **106** erzeugt die Ausgabe einen Ausgabeaktivierungsschlüssel **40**. Obwohl der Schlüssel durch jeden Beteiligten erzeugt werden kann, erlaubt die Erzeugung des Schlüssels durch die Ausgabe, dass die Ausgabe überwachen kann, welche Beteiligte Zugang zum Schlüssel haben und welche Karten durch Anwendung des Schlüssels aktiviert werden können. Der Ausgabeaktivierungsschlüssel **40** kann jeder geeignete Verschlüsselungsschlüssel sein, der brauchbar für die Erzeugung eines Sicherheitscodes ist. Beispielsweise ist der Ausgabeaktivierungsschlüssel **40** ein Datenverschlüsselungsstandardschlüssel (DES) mit doppelter Länge. Auch wird zu dieser Zeit eine Versionsnummer des Schlüssels durch die Ausgabe erzeugt. Obwohl jede Zahl von Aktivierungsschlüsseln durch eine Ausgabe

erzeugt werden kann, wird ein Aktivierungsschlüssel durch einen Kartenlieferanten erzeugt. In einer anderen Ausführungsform der Erfindung, wird ein Aktivierungsschlüssel für jeden Stapel der Karten erzeugt, die durch einen Kartenlieferanten erzeugt werden. In Schritt **108** liefert die Ausgabe den Aktivierungsschlüssel und seine Versionsnummer an den Kartenlieferanten.

[0051] In Schritt **110** erzeugt der Kartenlieferant einen Sicherheitscode für die Karte durch Anwendung des Aktivierungsschlüssels und der Versionsnummer, die von der Ausgabe erhalten werden. Ein Sicherheitscode kann auf vielfältige Art und Weise aus dem Aktivierungsschlüssel erzeugt werden. Jegliche Daten können mit dem Schlüssel durch Anwendung jedes geeigneten Verschlüsselungsalgorithmus unter jedem geeigneten Verschlüsselungsverfahren kombiniert werden, um den Sicherheitscode zu produzieren. Außerdem kann der Sicherheitscode für alle Karten von der Ausgabe derselbe sein, kann derselbe für alle Karten sein, die von einem speziellen Lieferanten erhalten worden sind, kann sich lediglich von Stapeln von Karten von einem speziellen Lieferanten unterscheiden, oder kann sogar ein eindeutiger Wert für jede Karte sein, die von einem Kartenlieferanten erzeugt wird. Beispielsweise benutzt eine spezielle Ausführungsform der vorliegenden Erfindung das folgende Formular für die Erzeugung eines eindeutigen Sicherheitscodes für jede erzeugte intelligente Zahlkarte. Die ersten Datenelemente **60**-**69** des Speichers **50** einer intelligenten Zahlkarte werden in einem Dreier-DES-Algorithmus in einem Elektronikcodebuch (ECB) -Modus durch Anwendung eines Ausgabeaktivierungsschlüssels verschlüsselt. Die vier signifikantesten Bytes aus dem Ergebnis dieser Verschlüsselung werden aufbewahrt und als Sicherheitscode für die Karte benutzt. Nach dieser Art und Weise wird ein Sicherheitscode einzig für die Karte erzeugt. Natürlich kann der Sicherheitscode aus anderen Informationen auf der Karte erzeugt werden und/oder andere Schlüssel benutzen.

[0052] In Schritt **112** wird dieser neue erzeugte Sicherheitscode auf der Karte in dem Datenbereich **72** des Speichers **50** installiert. Zusätzlich wird die Aktivierungsschlüsselversionsnummer, die von der Ausgabe erhalten wird, auch als Sicherheitscodeversion **74** in dem Speicher **50** gespeichert. Eine Hardwarerealisierung der intelligenten Zahlkarte verhindert den Wechsel der Karte von dem Sicherheitsbenutzermodus zu dem Standardbenutzermodus, sofern der Sicherheitscode nicht der Karte vorgelegt wird. Auf diese Art und Weise kann die Karte, bis ein autorisierter Einzelner in der Lage ist, der Karte den Sicherheitscode zu erzeugen und zu liefern, nicht benutzt werden. Diese Sicherheitsmaßnahme kann auch in Software für Karten durchgeführt werden, die diese Fähigkeit haben.

[0053] In Schritt **114** wird das Ausgabeflag **76** auf einen Wert 1 festgelegt, um anzuzeigen, dass sensitive Daten in dem Speicher **50** der Karte nicht länger modifiziert werden können. Trotz der Hardwarerealisierung, verhindert das Festlegen diese Flags die spätere Modifikation sensitiver Daten auf der Karte wie des Kartensicherheitscodes **72**, der Version **74** etc. Eine Softwarerealisierung kann auch benutzt werden, um das Flag **76** zu überwachen. Daten, die für Gebrauch der Karte verändert werden müssen, wie der Wert **80**, können noch modifiziert werden. An diesem Punkt ist die intelligente Zahlkarte mit Wert gespeichert worden, die einem Bargeldbetrag entspricht, jedoch ist die Karte noch nicht aktiviert worden. Deshalb kann sie sicher zur Ausgabe transportiert und gelagert werden. In Schritt **116** werden die Karten, die von dem Kartenlieferanten produziert werden, der Ausgabe übergeben, um sie an die Kunden zu verteilen.

[0054] Eine intelligente Zahlkarte kann durch Anwendung vielfältiger Techniken realisiert werden, um einen Zugang zum Wert auf der Karte zu schützen oder sonst zu verhindern. Eine Kartenauthentifizierung des Terminals kann verlangt werden bevor der Wert dekrementiert werden kann. In einigen Situationen ist eine Authentifizierung nicht erforderlich. Bei normalem Gebrauch, wenn die Authentifizierung erforderlich ist, wird der intelligenten Zahlkarte ein Kartenzugangscode (oder Benutzercode) beschafft, um den Wert auf der Karte zu dekrementirren (i.e. die Karte zu benutzen). In einer Ausführungsform der Erfindung wird festverdrahtete Logik der integrierten Schaltung auf der Karte benutzt, um diese Funktion durchzuführen. Festverdrahtete Logik auf der Karte nimmt den Kartenzugangscode an, verifiziert, dass er korrekt ist und erlaubt dann den Zugriff auf den Wert auf der Karte. Solche festverdrahtete Logik, die einen Kartenzugriffscode bearbeitet ist in der Technik wohlbekannt. Software in einer Karte kann auch benutzt werden, um einen Benutzercode zu verifizieren. Für Prozessorkarten ist es auch möglich, dass dieser Schritt der Authentifizierung durch Anwendung von Verschlüsselungssignaturen anstatt eines Benutzercodes durchgeführt wird.

[0055] In einer Ausführungsform der vorliegenden Erfindung, kann der Wert nicht dekrementiert werden, falls die Karte im Sicherheitsbenutzercode ist (d.h., falls das Sicherheitsflag **78** festgelegt wird). Die Karte muss im Standardbenutzercode sein (d.h., rückgesetzter Sicherheitsflag **78**), bevor der Wert dekrementiert werden kann. In anderen Worten, das Sicherheitsflag **76** muss zuruckgesetzt sein, um die Karte in den Standardbenutzercode zu bringen, bevor dem Kartenzugriffscode erlaubt werden kann, den Wert auf der Karte zu dekrementieren. Obwohl in dieser Ausführungsform die obige Funktionalität als Hardware auf dem integrierten Schaltkreis realisiert wird, könnte diese Funktionalität auch als Software realisiert werden. Zum Beispiel Software, die in dem

Speicher einer Speicherkarte oder in einer Prozessorkarte enthalten ist, kann auch diese Funktionen durchführen, um zu bestimmen, ob eine Karte im Sicherheitsbenutzermodus ist, und dann einen Kartenzugriffscode erhalten und vergleichen.

[0056] Der Fachmann wird in der Lage sein, diese Funktionalitäten durch Anwendung vielfältiger Typen von Software auf vielen Typen von integrierten Schaltkreisen zu realisieren. Diese Funktionalität könnte auch außerhalb der Karte in einem Kartenterminal oder Computer in Kommunikation mit der Karte implementiert werden. In diesem Szenario würde Software außerhalb der Karte die Funktionen "vergleichen, setzen, zurücksetzen, Zugriff erlauben, etc.", durchführen und würde bestimmen, ob es angebracht ist, den Zugriff auf den Wert auf der Karte zu erlauben.

Erzeugung und Wartung des Aktivierungssicherheitsanwendungsmoduls

[0057] Fig. 4 veranschaulicht eine Anordnung **200** zur Erzeugung eines Aktivierungssicherheitsanwendungsmodul (ASAM). Ein Aktivierungssicherheitsanwendungsmodul wird von einer Kartenausgabemaschine benutzt, um die Karten auf sichere Art und Weise zu aktivieren. Die Erzeugung des Aktivierungssicherheitsanwendungsmoduls benutzt einen in Fig. 5 beschriebenen Prozess, der das Aktivierungssicherheitsanwendungsmodul initialisiert und personalisiert. Die Anordnung **200** veranschaulicht eine Aktivierungssteuerungscomputer **202** unter Kontrolle eines Benutzers **204**, der sowohl mit dem Kontrollsicherheitsmodul (CSAM) **206** als auch mit einem Aktivierungssicherheitsanwendungsmodul (ASAM) **208** in Kommunikation ist.

[0058] Der Aktivierungssteuerungscomputer **202** kann jede geeignete Kontrollvorrichtung sein, die so eingerichtet ist, dass sie das Aktivierungssicherheitsanwendungsmodul **208** sicher initialisiert und personalisiert. Beispielsweise wird der die Aktivierungssteuerungscomputer **202** als Anwendungssoftware implementiert, die auf einem Personalcomputer oder einer anderen Haupteinrichtung läuft. Alternativ kann der Aktivierungssteuerungscomputer **202** auf einem Laptop zwecks Tragfähigkeit realisiert sein, oder sogar in einer Kartenausgabemaschine oder in einer anderen Aktivierungsvorrichtung, die dem Benutzer **204** erlauben würde, die Erzeugung und Wartung eines Aktivierungssicherheitsanwendungsmoduls **208** von einer entfernten Lage durch Anwendung kommunikativer Verbindung zu erzeugen und/oder durchzuführen.

[0059] Das Kontrollsicherheitsmodul **206** ist ein Sicherheitsmodul, das für die Erzeugung des Aktivierungssicherheitsanwendungsmoduls **208** von dem Aktivierungssteuerungscomputer **202** benutzt wird. Das Kontrollsicherheitsmodul **206** kann auf vielfältige Art und Weise implementiert werden, einschließlich als Chipkarte, die auf einem Sicherheitsanwendungsmodul (SAM) basiert, oder als ein Hardwaresicherheitsmodul (HSM). Ein Hardwaresicherheitsmodul (HSM) wird benutzt, um die kryptographische Verarbeitung zu erleichtern. Es speichert typischerweise Geheimschlüssel und Verschlüsselungsalgorithmen, führt kryptographische Funktionen an Geheimdaten aus und erzeugt Sitzungsschlüssel und Signaturen. Wie aus der Technik bekannt, ist ein Hardwaresicherheitsmodul allgemein eine eingriffsichere Vorrichtung, die einen gewissen Grad von physikalischen Sicherheitsmaßnahmen benutzt, um im Innern sensitive Informationen zu schützen. Ein Hardwaresicherheitsmodul kann jedes Sicherheitsmodul sein, das in der Industrie benutzt wird, wie das RACAL HSM Modell RG 7000, oder die Sicherheitsbox, die an einem automatischen Bankautomaten angebracht ist. In alternativen Ausführungsformen, kann das Hardwaresicherheitsmodul **130** auf einer Chipkarte innerhalb eines Kartenlesers, auf einer Reihe von Chipkarten, auf jeden geeigneten Sicherheitscomputer oder als Software realisiert sein.

[0060] Eine Vielfalt von Daten wird durch den Aktivierungssteuerungscomputer **202** für die Erzeugung des Aktivierungssicherheitsanwendungsmoduls **208** verwaltet. Enthalten ist ein Hauptaktivierungsschlüssel **212**, der benutzt wird, um einen Bereichsschlüssel für jedes Aktivierungssicherheitsanwendungsmodul, Benutzerkennwörter **214**, die die Einleitung der Wartung des Aktivierungssicherheitsanwendungsmoduls erlauben, eine Tabelle sämtlicher aktueller Ausgabeaktivierungsschlüssel **216** zusammen mit ihren Identifikationsindizes und eine Tabelle sämtlicher aktiver Aktivierungssicherheitsanwendungsmodule **218**. Jede Eingabe in der Tabelle liefert liefert den Aktivierungssicherheitsanwendungsmodulidentifikator und den gewünschten Maximalwert für den Aktivierungskontrollzähler. Vorzugsweise sind diese Schlüssel und Kennwörter sicher gespeichert. In einer Ausführungsform sind sensitive Schlüssel und Kennwörter in dem Kontrollsicherheitsmodul **206** gespeichert, während in einer anderen Ausführungsform, diese Information in der dem Kontrollsicherheitsmodul **206** zugänglichen Datenbank **210** gespeichert ist und unter einem lokalen Hauptschlüssel (LMK) des Kontrollsicherheitsmodul **206** verschlüsselt ist. Die Datenbank **210** kann sich auch innerhalb des Aktivierungssteuerungscomputers **202** befinden, an entfernter Stelle oder in jedem anderen geeigneten Ort.

[0061] Vorzugsweise hat der Hauptaktivierungsschlüssel **212** eine zugehörige Versionsnummer und wechselt periodisch. Am besten ist der Aktivierungssteuerungscomputer **202** in der Lage, zumindest zwei Hauptaktivierungsschlüssel zu warten. Der Haupaktivierungsschlüssel **212** wird benutzt, um einen Bereichsschlüssel für eine sichere Kommunikati-

on mit dem Aktivierungssicherheitsanwendungsmodul abzuleiten. Basierend auf der Versionsnummer ist ein Wartungsprozess eines Aktivierungssicherheitsanwendungsmodul (wie unten in Fig. 6 beschrieben wird) in der Lage zu bestimmen, ob der Bereichsschlüssel in dem Aktivierungssicherheitsanwendungsmodul ersetzt werden soll. Der Aktivierungssteuerungscomputer **202** hat auch die Fähigkeit, neue Aktivierungsschlüssel, falls erforderlich, zu erzeugen und Schlüssel zu zerstören. In einer Ausführungsform sind es die Datenverschlüsselungsstandardschlüssel von doppelter Länge, die sicher gespeichert werden. Außerdem exportiert vorzugsweise der Aktivierungssteuerungscomputer **202** die Aktivierungsschlüssel auf sichere Art und Weise zu einem Kartenlieferanten.

[0062] Das Aktivierungssicherheitsanwendungsmodul **208** wird aus Kostengründen auf einer Chipkarte implementiert, kann aber auch als Hardwaresicherheitsmodul implementiert sein. Es hat die unten beschriebene Funktionalität.

[0063] Fig. 5 ist ein Ablaufschema, das eine Technik der Erzeugung des Aktivierungssicherheitsanwendungsmoduls **208** beschreibt. Die Erzeugung eines Aktivierungssicherheitsanwendungsmodul bezieht sich auf die Initialisierung und die Personalisierung des Aktivierungssicherheitsanwendungsmoduls. Wenn ein Aktivierungssicherheitsanwendungsmodul erzeugt worden ist, ist es gebrauchsfertig in einer Kartenausgabemaschine, um die Karten, wenn sie verkauft wurden, in der Maschine zu aktivieren.

[0064] In Schritt **252** wird das Aktivierungssicherheitsanwendungsmodul **208** mit jedem Teil der Anwendungssoftware initialisiert, die für seinen Einsatz benötigt werden; vorzugsweise wird die Software in einen elektrisch löschbaren programmierbaren Festspeicher innerhalb des Aktivierungssicherheitsanwendungsmoduls geladen. Zusätzlich werden jegliche Daten und/oder Dateistrukturen, die von dem Aktivierungssicherheitsanwendungsmodul benötigt werden, auch zu dieser Zeit geladen.

[0065] In Schritt **254** wird das Aktivierungssicherheitsanwendungsmodul mit einem Initialisierungsschlüssel geladen. Dieser Initialisierungsschlüssel wird benutzt, um den Bereichsschlüssel zu verschlüsseln, der anschließend in das Aktivierungssicherheitsanwendungsmodul geladen wird. Der Initialisierungsschlüssel kann durch Anwendung jeder geeigneten Technik geladen werden und benutzt irgendeinen Verschlüsselungsverfahren. In einer gängigen bevorzugten Ausführung wird ein Datenverschlüsselungsstandardschlüssel benutzt. Obwohl sich der Initialisierungsschlüssel für jedes Aktivierungssicherheitsanwendungsmodul für eine Ausgabe unterscheiden kann, benutzen sämtliche Aktivierungssicherheitsanwendungsmodule für eine Ausgabe vorzugsweise denselben Initialisierungsschlüssel. In einer speziellen Ausführungsform wird der Initialisierungsschlüssel durch Lieferung mehrerer Datenabschnitte an das Aktivierungssicherheitsanwendungsmodul geladen. Sofort wird innerhalb des Aktivierungssicherheitsanwendungsmoduls bei diesen mehreren Datenabschnitten eine Exclusiv-Oder- Verknüpfung durchgeführt, mit dem Ergebnis, dass der Initialisierungsschlüssel gebildet wird. Der Schlüssel wird dann innerhalb des Aktivierungssicherheitsanwendungsmodul innerhalb eines sicheren Ortes gespeichert. Die Anwendung eines Initialisierungsschlüssels, um den Bereichsschlüssel zu verschlüsseln, erlaubt den Bereichsschlüssel auf sicherer Art und Weise zu übertragen und zu speichern.

[0066] An diesem Punkt ist die Initialisierung komplett und die Personalisierung des Aktivierungssicherheitsanwendungsmoduls kann beginnen. In einer bevorzugten Ausführungsform wird der Benutzer **204** aufgefordert, ein Kennwort an den Aktivierungssteuerungscomputer **202** zu liefern, bevor die Personalisierung beginnen kann. Wenn personalisiert wurde, kann das Aktivierungssicherheitsanwendungsmodul **208** mit Aktivierungsdaten geladen werden, beispielsweise durch Anwendung des In Fig. 7 beschriebenen Prozesses.

[0067] In Schritt **256** wird dem Aktivierungssicherheitsanwendungsmodul **208** ein eindeutiger Identifikator zugeteilt. Vorzugsweise bestimmt der Aktivierungssteuerungscomputer **202** den eindeutigen Identifikator des Aktivierungssicherheitsanwendungsmoduls **208**, der zugeteilt wird und in das Aktivierungssicherheitsanwendungsmodul **208** geladen wird. In Schritt **258** wird dem Aktivierungssicherheitsanwendungsmodul **208** ein maximal erlaubter Wert für seinen Aktivierungsskontrollzähler (ACC) zugeteilt. Der Aktivierungskontrollzähler begrenzt die Zeit, in der das Aktivierungssicherheitsanwendungsmodul **208** versuchen kann, die intelligenten Zahlkarten zu aktivieren. Der Gebrauch des Aktivierungskontrollzählers verhindert skupellose Einzelne, die entweder versuchen, den Sicherheitscode auf einer Karte, die ein Aktivierungssicherheitsanwendungsmodul verwendet, zu knacken, oder illegal eine Kartenausgabemaschine erworben haben und versuchen eine große Anzahl von Karten, die ein einzelnes Aktivierungssicherheitsanwendungsmodul benutzen, zu aktivieren. Dieser maximal erlaubte Wert für den Aktivierungskontrollzähler wird in das Aktivierungssicherheitsanwendungsmodul **208** geladen.

[0068] In Schritt **260** wird auf dem Aktivierungssicherheitsanwendungsmodul **208** ein Bereichsschlüssel installiert. Wie vorher erwähnt, ist der Bereichsschlüssel ein Verschlüsselungsschlüssel der für die sichere Kommunikation zwischen zwei Knoten benutzt wird. In dieser Ausführung erlaubt der Bereichsschlüssel, der auf dem Aktivierungssicherheitsan-

wendungsmodul **208** installiert ist, eine künftige sichere Kommunikation zwischen dem Aktivierungssicherheitsanwendungsmodul **208** und dem Kontrollsicherheitsmodul **206**. Der Bereichsschlüssel kann durch Anwendung vielfältiger Techniken installiert und abgeleitet werden. In einer bevorzugten Ausführung der Erfindung werden die folgenden Schritte verwendet. Der Aktivierungssteuerungscomputer **202** fordert zunächst den Bereichsschlüssel von dem Kontrollsicherheitsmodul **206** an; diese Aufforderung enthält das Benutzerkennwort und den Identifikator des Aktivierungssicherheitsanwendungsmoduls. Bei Überprüfung des Benutzerkennwortes durch das Kontrollsicherheitsmodul **206** erzeugt das Kontrollsicherheitsmodul **206** den Bereichsschlüssel für das Aktivierungssicherheitsanwendungsmodul **208**. Der Bereichsschlüssel wird dann unter dem Initialisierungsschlüssel verschlüsselt und wird als Antwort auf seine Aufforderung zum Aktivierungssteuerungscomputer **202** geliefert. Der Aktivierungssteuerungscomputer **202** sendet dann einen „LADE BEREICHSSCHLÜSSEL" Befehl zum Aktivierungssicherheitsanwendungsmodul **208** zusammen mit dem verschlüsselten Bereichsschlüssel. Das Aktivierungssicherheitsanwendungsmodul **208** entschlüsselt dann den Bereichsschlüssel und ersetzt den Initialisierungsschlüssel durch den Bereichsschlüssel.

[0069] Es wird einsichtig sein, dass der Bereichsschlüssel auf viele Arten abgeleitet werden kann. Um ein Beispiel zu geben, der Bereichsschlüssel ist ein Datenverschlüsselungsstandardschlüssel doppelter Länge, der zwischen dem Aktivierungssicherheitsanwendungsmodul **208** und dem Kontrollsicherheitsmodul **206**, das nur auf das Aktivierungssicherheitsanwendungsmodul **208** beschränkt ist, gemeinsam benutzt wird. Der Bereichsschlüssel kann durch Anwendung des folgenden Algorithmus abgeleitet werden. Ein erster Schlüssel wird durch Verschlüsselung des Identifikators des Aktivierungssicherheitsanwendungsmoduls **208** (mit Nullen aufgefüllt) durch Anwendung des Hauptaktivierungsschlüssels unter einem dreifachen Datenverschlüsselungsstandardschlüssel-Algorithmus erzeugt. Ein zweiter Schlüssel wird durch Verschlüsselung des Einerkomplements des Identifikators des Aktivierungssicherheitsanwendungsmoduls **208** (mit Nullen aufgefüllt) durch Anwendung des Hauptaktivierungsschlüssels unter einem dreifachen Datenverschlüsselungsstandardschlüssel-Algorithmus erzeugt. Der Bereichsschlüssel wird dann durch Verwendung einer Verkettung des ersten und zweiten Schlüssels konstruiert. Wenn das Aktivierungssicherheitsanwendungsmoduls **208** initialisiert und personalisiert (Aktivierungssicherheitsanwendungsmodulerzeugung) worden ist, kann die Wartung des Aktivierungssicherheitsanwendungsmoduls **208** durchgeführt werden.

[0070] Fig. 6 ist ein Ablaufschema, das eine Technik der Durchführung der Wartung des Aktivierungssicherheitsanwendungsmoduls **208** beschreibt. In einer Ausführungsform der Erfindung wird die Wartung des Aktivierungssicherheitsanwendungsmoduls **208** unter der Kontrolle des Aktivierungssteuerungscomputers **202** während der Kommunikation mit dem Kontrollsicherheitsmodul **206** durchgeführt. Die Wartung kann durch Anwendung einer Wählverbindung zwischen der Kartenausgabemaschine, die das Aktivierungssicherheitsanwendungsmodul **208** und den Hauptsteuerungsaktivierungscomputer **202** enthält, oder durch den physikalischen Transport des Aktivierungssicherheitsanwendungsmodusl 208 zum Aktivierungssteuerungscomputer **202** und durch seine Positionierung in einen Kartenleser, der am Ort des Aktivierungssteuerungscomputer **202** angebracht ist, geschehen. Alternativ ist es möglich, einen tragbaren Hauptaktivierungssteuerungscomputer **202** zusammen mit dem Kontrollsicherheitsmodul **206** an die Stelle der Kartenausgabemaschine zu bringen, um die Wartung des Aktivierungssicherheitsanwendungsmodul **208** durchzuführen.

[0071] Das Aktivierungssicherheitsanwendungsmodul **208** enthält Daten, die vorzugsweise von Zeit zu Zeit aktualisiert werden, inklusive: Einen Bereichsschlüssel für die sichere Kommunikation mit dem Aktivierungssteuerungscomputer **202**, einen Satz von Ausgabeaktivierungsschlüsseln, und einen Aktivierungskontrollzähler (ACC). Natürlich, bevor das Aktivierungssicherheitsanwendungsmodul **208** zum ersten Male benutzt wird, wird eine ähnliche der in Fig. 6 beschriebenen Prozedur angewendet, um einen Bereichsschlüssel zu installieren, einen Satz von Ausgabeaktivierungsschlüsseln zu installieren und den Aktivierungskontrollzähler auf einen speziellen Wert einzustellen. Wenn zum Beispiel das Aktivierungssicherheitsanwendungsmodul **208** darauf vorbereitet worden ist, in das Feld gebracht zu werden, können die Prozeduren der Fig. 5 und Fig. 6 durchgeführt werden, um das Aktivierungssicherheitsanwendungsmodul **208** für die Aktivierung der intelligenten Zahlkarten in einer Kartenausgabemaschine zu aktivieren. Wenn das Aktivierungssicherheitsanwendungsmodul **208** in dem Feld benutzt und die Wartung gewünscht wird, kann die Prozedur von Fig. 6 benutzt werden, um diese Wartung durchzuführen.

[0072] In Schritt **270** liefert der Benutzer **204** ein geeignetes Kennwort, um das Auftreten der Wartung des Aktivierungssicherheitsanwendungsmoduls **208** zu erlauben. In Schritt **272** werden Daten von dem Aktivierungssicherheitsanwendungsmodul **208** abgefragt, um die eigentliche Wartung zu erlauben. Diese Daten enthalten den Identifikator des Aktivierungssicherheitsanwendungsmoduls **208**, eine Liste von Ausgabeaktivierungsschlüsseln, den aktuellen Wert des Aktivierungskontrollzählers, seinen maximalen Wert, und die aktuelle Bereichsschlüsselversionsnummer.

[0073] Schritt **274** bestimmt, ob ein neuer Bereichsschlüssel durch Prüfung der aktuellen Bereichsschlüsselversionsnummer, die von dem Aktivierungssicherheitsanwendungsmodul **208** abgefragt wird, erforderlich wird. Falls ein neuer Schlüssel erforderlich wird (oder falls dies die erste Wartung ist), aktualisiert Schritt **276** den Bereichsschlüssel. Schritt **276** kann auf viele Arten durchgeführt werden. In einer speziellen Ausführungsform wird ein Aktualisierungsbefehl zur Ersetzung eines Bereichsschlüssel eines Aktivierungssicherheitsanwendungsmoduls **208** angewendet, der eine neue Bereichsschlüsselversionsnummer, einen neuen Bereichsschlüssel doppelter Länge und einen Bereichsschlüsselprüfwert enthält. Vorzugsweise sind die ganzen Befehlsdaten verschlüsselt. Die Antwort des Aktivierungssicherheitsanwendungsmoduls **208** ist die neue Bereichsschlüsselversionsnummer und der Bereichsschlüsselprüfwert, beide in Klartext. Vorzugsweise wird ein neuer Bereichsschlüssel unter dem alten Bereichsschlüssel verschlüsselt.

[0074] Schritt **278** setzt fest, ob irgendwelche Ausgabeaktivierungsschlüssel veraltet sind und wenn nötig gelöscht werden können. Wenn ja aktualisiert Schritt **280** die Ausgabeschlüssel in dem Aktivierungssicherheitsanwendungsmodul **208**. Schritt **280** kann auf viele Arten durchgeführt werden. In einer speziellen Ausführung wird ein Aktualisierungsbefehl zur Löschung verschiedener Ausgabeaktivierungsschlüssel dem Aktivierungssicherheitsanwendungsmodul **208** bereitgestellt. Dieser Befehl enthält veränderliche Längenlisten von Schlüsselindizes, die anzeigen, welche Schlüssel zu löschen sind.

[0075] Schritt **282** bestimmt, ob neue Ausgabeaktivierungsschlüssel zum Aktivierungssicherheitsanwendungsmodul **208** hinzugefügt werden sollen. Es könnte nötig sein, neue Schlüssel hinzuzufügen, falls die Ausgabe mit neuen Versionen hervorkommt oder falls das Aktivierungssicherheitsanwendungsmodul **208** zum ersten Male gewartet ist. Wenn ja, fügt Schritt **284** einen neuen Ausgabeschlüssel oder Ausgabeschlüssel dem Aktivierungssicherheitsanwendungsmodul **208** hinzu. Schritt **284** kann auf viele Arten durchgeführt werden. In einer speziellen Ausführung wird ein aktualisierter Befehl, einen Ausgabeaktivierungsschlüssel hinzuzufügen, für jeden hinzuzufügenden Schlüssel durchgeführt. Dieser Befehl benutzt einen Block für jeden hinzuzufügenden Schlüssel, der eine neue Ausgabeaktivierungsschlüsselversionsnummer, eine neuer Ausgabeaktivierungsschlüssel doppelter Länge und einen Aktivierungsschlüsselprüfwert enthält. Vorzugsweise sind die ganzen Befehlsdaten verschlüsselt. Die Antwort, die von dem Aktivierungssicherheitsanwendungsmodul **208** empfangen wird ist ein Block für jeden Schlüssel, der erfolgreich hinzugefügt wurde und enthält sowohl die Schlüsselversionsnummer und den Schlüsselprüfwert in Klartext. Vorzugsweise sind die neuen Aktivierungsschlüssel und die verknüpften Informationen unter dem aktuellen Bereichsschlüssel verschlüsselt.

[0076] Schritt **286** bestimmt, ob der Aktivierungskontrollzähler (ACC) aktualisiert werden soll. Bevor zum Beispiel das Aktivierungssicherheitsanwendungsmodul **208** dem Feld freigegeben wird, wird es nötig sein, dass es sein Aktivierungskontrollzählerwertesatz hat. Also falls eine Karteausgabemaschine, die ein Aktivierungssicherheitsanwendungsmodul **208** benutzt, einen großen Teil der Karten aktiviert hat, ist es möglich, dass sein Aktivierungskontrollzählerwert dem maximalen Aktivierungskontrollzählerwert angenähert ist, der für das Aktivierungssicherheitsanwendungsmodul **208** erlaubt ist. Wenn ja könnte es wünschenswert sein, den Aktivierungskontrollzählerwert erneut zu aktualisieren. Vorteilhafterweise kann der Aktivierungskontrollzählerwert auf einen speziellen Wert festgelegt werden, die von der Umgebung abhängt, in der sich die Kartenausgabemaschine befindet. Zum Beispiel ist es für den Innenraum einer schnellen Durchgangsstation, die eine gute Sicherheit hat und eine extrem große Menge geringwertiger Karten verkaufen kann, wünschenswert, den Aktivierungskontrollzählerwert auf eine ziemlich hohe Zahl festzusetzen. Weil die Karten einen geringeren Wert haben und die Maschine in einer sicheren Gegend gelegen ist, ist das Risiko geringer und der Aktivierungskontrollzählerwert kann höher festgesetzt sein. Für eine Kartenausgabemaschine jedoch, die in einer Straße gelegen ist, kann es wünschenswert sein, den Aktivierungskontrollzähler augrund des anwachsenden Risikos des Diebstahls der Maschine auf einen niedrigeren Wert zu setzen.

[0077] Falls der Aktivierungskontrollzähler aktualisiert ist, lädt Schritt **288** einen neuen Aktivierungskontrollzählerwert in das Aktivierungssicherheitsanwendungsmodul **208**. Schritt **288** kann auf viele Arten durchgeführt werden. In einer speziellen Ausführung wird ein aktualisierter Befehl benutzt, um einen neuen Aktivierungskontrollzählerwert zu laden. Dieser Befehl enthält den neuen Aktivierungskontrollzählerwert und den aktuellen Aktivierungskontrollzählerwert. An diesem Punkt ist die Wartung des Aktivierungssicherheitsanwendungsmoduls **208** komplett.

[0078] Die Kommunikation der Befehle und die Antworten zwischen dem Aktivierungssteuerungscomputer (AM) **202** und dem Aktivierungssicherheitsanwendungsmodul **208** kann durch Gebrauch vieler verschiedener Protokolle durchgeführt werden. In einer Ausführung der Erfindung beginnt die Aktualisierung der Schritte **276**, **280**, **284**, **288** mit einem Intitialisierungsaktualisierungsbefehl von dem Aktivierungssteuerungscomputer **202** zum Aktivierungssicherheitsanwendungsmodul **208**. Vorzugsweise sendet dieser Befehl den Identifikator des Kontrollsicherheitsmoduls und empfängt dafür der Reihe nach den

Identifikator des Aktivierungssicherheitsanwendungsmoduls **208**, den aktualisierten Transaktionszähler (NTU) und die Bereichsschlüsselversionsnummer (VKZ).

[0079] Bei der Verarbeitung der Initialisierungsaktualisierungsbefehle, benutzt vorzugsweise das Aktivierungssicherheitsanwendungsmodul **208** den internen aktualisierten Transaktionszähler, um zu verfolgen, wie viele Aktualisierungen angefordert werden. Dieses Merkmal gibt zusätzliche Sicherheit. Der interne Zähler wird für jede angeforderte Aktualisierung inkrementiert; wenn sein maximaler Wert erreicht ist, wird ein Antwortcode, der dieses Faktum anzeigt an den Aktivierungssteuerungscomputer **202** zurückgegeben anstatt die normalen Antwort auf einen Initialisierungsaktualisierungsbefehl. Vorzugsweise wird der interne Aktualisierungstransaktonszähler implementiert, so dass er sich nicht umdreht, wenn er seinen maximalen Wert erreicht.

[0080] Wenn der Aktivierungssteuerungscomputer **202** eine Antwort auf seinen Initialisierungsaktualisierungsbefehl enthält, sendet er einen aktualisierten Befehl (wie oben beschrieben) zusammen mit einem Nachrichtenauthentifizierungsscode (MAC) und empfängt dafür Antwortdaten und einen Beendigungscode von dem Aktivierungssicherheitsanwendungsmodul **208**. Wenn der aktualisierte Befehl von dem Aktivierungssicherheitsanwendungsmodul **208** empfangen wird, kopiert es seinen internen aktualisierten Transaktionszähler für eine dauerhafte Speicherung und verifiziert den Nachrichtenberechtigungscode. Dann führt es die angeforderte Aktualisierung (der Ausgabeschlüssel, des Aktivierungskontrollzählers oder des Bereichsschlüssels) aus und gibt eine Antwort an den Befehl zurück, wie oben beschrieben worden ist. Falls irgendein Fehler während der Verifikation des Nachrichtenberechtigungscodes oder während der Aktualisierung auftritt, wird eine passende Antwort an den Aktivierungssteuerungscomputer **202** zurückgegeben. Wenn der Aktivierungssteuerungscomputer **202** eine Antwort auf seinen aktualisierten Befehl erhalten hat, überprüft er diese erhaltenen Antwortdaten. Jeder Fehler, der während irgendeiner Initialisierungsaktualisierung, eines aktualisierten Befehls oder Überprüfungsbefehle auftritt, endet mit einem Fehlerzustandscode, der festgelegt ist.

[0081] Obwohl die Datensicherheit eines jeden aktualisierten Befehls auf vielfältige Weise geschützt werden kann, wird vorzugsweise ein Nachrichtenauthentifikationscode (MAC) benutzt. Der Nachrichtenauthentifikationsscode wird durch Verwendung des Bereichsschlüssel des Aktivierungssicherheitsanwendungsmoduls erzeugt, der einen Blockverschlüsselungscode benutzt, der sich oft auf ein CBC Modus bezieht. In einer aktuellen bevorzugten Ausführungsform wird die Erzeugung durchgeführt, wie sie in der Referenz „ISO/IEC 9797", zweite Auflage, beschrieben wird, oder sie kann, wie in der Referenz ANSI X9.19, 1996 beschrieben, durchgeführt werden.

[0082] Ebenso können die Daten und Befehle, die die Schlüssel aktualisieren, auf vielfältige Weise verschlüsselt sein. In einer aktuellen bevorzugten Ausführungsform wird die Verschlüsselung durch Anwendung des Datenverschlüsselungsstandardschlüssels in dem Ereignissteuerblockmodus mit einem einfachen Kommunikationsschlüssel durchgeführt, wie in der Referenz „ANSI X3.92" erklärt, obwohl andere Techniken auch benutzt werden können. Der Kommunikationsschlüssel wird durch Anwendung des folgenden Algorithmus von dem Bereichsschlüssel des Aktivierungssicherheitsanwendungsmoduls abgeleitet. Der Kontrollsicherheitsmodulidentifikator, der Aktivierungssicherheitsanwendungsmodulidentifikator und der interne Transaktionsaktualisierungszähler werden zusammen verkettet und durch Anwendung des Bereichsschlüssels unter dem Verschlüsselungsalgorithmus des dreifachen Datenverschlüsselungsstandardschlüssels verschlüsselt, um den Kommunikationsschlüssel zu erhalten. Außerdem ist für jeden Schlüssel, der aktualisiert wird, ein Prüfwert in den verschlüsselten Daten enthalten. Der Prüfwert wird durch Anwendung des dreifachen Datenverschlüsselungsstandardschlüssels berechnet, um einen 8-Byte Block von binären Nullen zu verschlüsseln. Der Prüfwert in Klartext wird an den Aktivierungssteuerungscomputer zurückgegeben, um zu überprüfen, dass die Daten korrekt empfangen und entschlüsselt werden. Kontrollwerte können auch auf andere Arten berechnet werden.

[0083] Wenn das Aktivierungssicherheitsanwendungsmodul **208** das erste Mal richtig gewartet worden ist und in einer Kartenausgabemaschine präsent ist, ist es bereit die Aktivierung der intelligenten Zahlkarten in der Maschine zu beginnen.

Kartenaktivierung

[0084] Fig. 7 veranschaulicht die Kartenausgabemaschine **24** detaillierter. In der Kartenausgabemaschine **24** enthalten sind ein Aktivierungssicherheitsanwendungsmodul **208** und eine Zahl intelligenter Zahlkarten **30**, die für die Aktivierung und die Ausgabe an den Kunden bereit sind. Zur Vereinfachung der Erklärung sind das Aktivierungssicherheitsanwendungsmodul **208** und die intelligente Zahlkarte **30** vergrößert außerhalb der Kartenausgabemaschine **24** gezeigt. Die Kartenausgabemaschine **24** kontrolliert durch Anwendung des Aktivierungssicherheitsanwendungsmoduls **208** den Kartenaktivierungsprozess, um den Ausgabeaktivierungsschlüssel zu speichern und die Kartensicherheitscodes zu berechnen, die notwendig für die Aktivierung intelligenter Zahlkarten ist. In einer typischen Situation erhält ein Kun-

de, der eine Karte an der Kartenausgabemaschine **24** kauft, eine Karte, die von der Maschine ausgegeben wird, wenn die Karte durch Anwendung des Aktivierungssicherheitsanwendungsmodul **208** aktiviert worden ist.

[0085] Die Fig. 8A und Fig. 8B sind Ablaufschemata, die einen Prozeß beschreiben, durch den die intelligente Zahlkarte **30** innerhalb der Kartenausgabemaschine **24** durch Anwendung des Aktivierungssicherheitsanwendungsmodul aktiviert wird. Der Prozess in den Fig. 8A und Fig. 8B wird eingeleitet, sobald ein Kunde einen Einkauf einer intelligenten Zahlkarte aus der Kartenausgabemaschine **24** tätigt. In Schritt **302** liest die Kartenausgabemaschine **24** Kartentypendaten von der intelligenten Zahlkarte **30**. In dieser speziellen Ausführung wird Typeninformation in dem Speicher **50** der intelligenten Zahlkarte **30** gespeichert, nämlich Byte H1 60 und Byte H2 62. Diese Bytes zeigen die Typen von Chips an, die innerhalb der intelligenten Zahlkarte **30** gebraucht werden, und zeigen an, ob diese Karte für die Aktivierung geeignet ist oder nicht. Für einen Prozessor und andere Typen von Karten sind diese Bytes nicht erforderlich; Schritt **302** würde dann nicht erforderlich sein oder eine andere Technik kann benutzt werden, um den Typ des Chips zu bestimmen.

[0086] Basierend auf den Kartentypendaten legt Schritt **304** fest, ob diese Karte geeignet ist, aktiviert zu werden. In dieser speziellen Ausführung legt Schritt **304** fest, ob die intelligente Zahlkarte **30** einen speziellen Typ von Chip eingebettet hat. Wenn ja, zeigt dies an, dass die Karte entweder in einem Sicherheitsbenutzermodus oder in einem Standardbenutzermodus sein kann. Falls die Karte nicht der korrekte Typ ist, dann wird die Karte in Schritt **314** einfach an den Kunden ausgegeben, vorausgesetzt die Bezahlung ist gemacht worden. Eine Karte, die nicht für die Aktivierung geeignet ist, ist wahrscheinlich schon aktiviert und kann auf der Stelle ausgegeben werden.

[0087] Schritt **306** liest zusätzliche relevante Daten von der intelligenten Zahlkarte **30**, die nützlich für die Aktivierung der Karte ist. Die zusätzlichen Daten enthalten den Ausgabeidentifikator, den Kartenlieferantenidentifikator, die Versionsnummer des Ausgabeaktivierungsschlüssels und den Sicherheitsflag. Schritt **308** legt durch Kontrolle des abgefragten Sicherheitsflags fest, ob die Karte in Sicherheitsbenutzermodus ist. Falls die Karte nicht im Sicherheitsbenutzermodus ist, dann ist die Karte schon im Standardbenutzermodus und braucht nicht aktiviert werden. Die Karte wird an an den Kunden in Schritt **314** ausgegeben.

[0088] Falls jedoch die intelligente Zahlkarte im Sicherheitsbenutzermodus ist, dann wird der geeignete Sicherheitscode für die intelligente Zahlkarte **30** vom Aktivierungssicherheitsanwendungsmodul **208** abgefragt. Der Sicherheitscode, der vom Aktivierungsicherheitsanwendungsmodul **208** abgefragt wird, wird benutzt, um die intelligente Zahlkarte **30** zu aktivieren. Der Sicherheitscode kann von dem Aktivierungssicherheitsanwendungsmodul **208** oder anderen geeigneten Sicherheitsvorrichtungen auf viele Arten und Weisen abgefragt werden. Beispielsweise beschreibt Fig. 8B eine Technik für die Abfrage des Sicherheitscode. In Schritt **312** wird der abgefragte Sicherheitscode der Karte **30** vorgelegt, um die Karte zu aktivieren.

[0089] Die Verifizierung durch die intelligente Zahlkarte **30**, das der Sicherheitscode, der ihr vorgelegt wird, der in dem Speicher der Karte vorgelegte ist, kann durch verschiedene Techniken ausgeführt werden. In einer bevorzugten Ausführung der Erfindung wird der Chip, wie oben beschrieben, auf der Karte implementiert, um einen vorgelegten Sicherheitscode mit dem Sicherheitscode zu vergleichen, der schon auf der Karte gespeichert wurde. Die Implementierung dieses Vergleichs als Hardware kann durch Fachleute der Chipimplementierung ausgeführt werden. In anderen Ausführungen kann residente Software auf der intelligenten Zahlkarte **30** den Vergleich und die Aktivierung der Karte ausführen, oder andere Sicherheitsvorrichtungen (wie zum Beispiel das Aktivierungssicherheitsanwendungsmodul **208** oder die Kartenausgabemaschine **24**) kann die Sicherheitscodes vergleichen und die Karte mit Erfolg aktivieren. In einer bevorzugten Ausführung wird durch Anwendung folgenden Vorgehens der Sicherheitscode verifiziert und die Karte aktiviert. Zunächst wird eine Adressenneueinstellung der Karte ausgeführt. Dann wird der Fehlerzähler durch Setzen des nächsten freien Bits in dem Fehlerzähler **70** inkrementiert. Falls zum Beispiel der Fehlerzähler **70** 4 Bits hat, werden nur 4 Versuche erlaubt, die intelligente Zahlkarte **30** zu aktivieren. Dieses Merkmal schützt vor unbefugten Versuchen, durch Anwendung automatischer Mittel die Karte wiederholt zu aktivieren. Dann wird der Sicherheitscode, der von dem Aktivierungssicherheitsanwendungsmodul **208** abgefragt wird, der intelligenten Zahlkarte **30** vorgelegt. Der Sicherheitscode wird am Eingabe-Ausgabe Pin der Karte Bit für Bit vorgelegt. Die Karte vergleicht den empfangenen Sicherheitscode Bit für Bit mit dem, der in ihrem Speicher gespeichert wurde. Falls erfolgreich, löscht der nächste Schritt den Fehlerzähler. Ein erfolgreich gelöschter Fehlerzähler **70** zeigt an, dass der vorgelegte Sicherheitscode durch die intelligente Zahlkarte **30** verifiziert worden ist. Vorzugsweise wird eine Löschoperation auf die Fehlerzählerbits in dem Speicher angewandt. Falls der Sicherheitscode korrekt eingegeben worden ist, ist es erlaubt, den Fehlerzähler zu löschen. Eine erfolgreiche Löschoperation kann als Hinweis einer erfolgreichen Sicherheitscodeverifizierung benutzt werden. Falls der Vergleich nicht erfolgreich war, erlaubt der Chip

nicht, dass der Fehlerzähler gelöscht wird; der Fehlerzähler zeigt dann an, wieviele vergebliche Vergleiche ausprobiert worden sind (bis vier). Dann wird der Sicherheitsflag **78** auf der intelligenten Zahlkarte **30** auf 0 gesetzt, um den regulären Benutzermodus anzuzeigen. Das Setzen des Sicherheitscodes wird nicht möglich sein, es sei denn, der vorgelegte Code ist verifiziert worden.

[0090] An diesem Punkt ist die intelligente Zahlkarte **30** jetzt aktiviert und ist gebrauchsfertig. Schließlich wird der Sicherheitscode auf der intelligenten Zahlkarte **30** gelöscht. Diese Löschung hält einen skrupellosen Beteiligten von einem späteren Lesen des Sicherheitscodes ab. Sobald die Karte aktiviert worden ist, wird die Karte an einen Kunden in Schritt **314** abgegeben. Falls die Aktivierung nicht erfolgreich ist, wird die Karte zurückgewiesen und als unbenutzbar in der Kartenausgabemaschine **24** gekennzeichnet.

[0091] Fig. 8B ist ein Ablaufschema, das eine Technik beschreibt, durch welche Schritt **310** von Fig. 8A ausgeführt werden kann. In Schritt **310** fordert die Kartenausgabemaschine **24** den Sicherheitscode von dem Aktivierungssicherheitsanwendungsmodul **208** an. Das Aktivierungssicherheitsanwendungsmodul **208** verwaltet die Sicherheit für den Aktivierungsprozess. Zusätzlich zur Bereitstellung des Sicherheitsschlüsselverwaltung stellt das Aktivierungssicherheitsanwendungsmodul **208** auch den Aktivierungskontrollzähler (ACC) zur Verfügung, der die Gefährdung durch Betrug und Diebstahl durch Beschränkung der Zahl der Karten, die das Aktivierungssicherheitsanwendungsmodul **208** aktivieren kann, begrenzt.

[0092] Schritt **320** bestimmt, ob der Aktivierungskontrollzähler gleich 0 ist. Wenn ja, zeigt dies an, daß eine maximale Zahl von Karten schon durch das Aktivierungssicherheitsanwendungsmodul **208** aktiviert worden ist und keine weiteren Karten aktiviert werden können. Danach gibt Schritt **322** eine negative Antwort zurück, die anzeigt, dass die intelligente Zahlkarte **30** nicht aktiviert werden wird und Schritt **310** ist fertig. Falls jedoch die maximale Zahl noch nicht erreicht worden ist, dann subtrahiert Schritt **324** 1 von dem Aktivierungskontrollzähler.

[0093] Durch Anwendung der Daten, die zuvor von der intelligenten Zahlkarte **30** gelesen werden, wählt Schritt **326** den geeigneten Ausgabeaktivierungsschlüssel aus, mit dem der Kartensicherheitscode abzuleiten ist. Vorzugsweise wird ein Schlüsselindex, der auf dem Ausgabeindentifikator, dem Kartenlieferantenidentifikator, und der Aktivierungsschlüsselversionsnummer beruht, benutzt, um den geeigneten Aktivierungsschlüssel auszuwählen. Solch ein Index ist nützlich, weil zahlreiche Aktivierungsschlüssel mit einem Aktivierungssicherheitsanwendungsmodul **208** für den Gebrauch erhältlich sein können. Zum Beispiel kann jede Ausgabe einen verschiedenen Aktivierungsschlüssel benutzen und kann sowohl verschiedene Aktivierungsschlüssel für verschiedene Lieferanten als auch verschiedene Schlüssel für verschiedene Stapel von demselben Lieferanten benutzen. Außerdem können verschiedene Versionen eines Aktivierungsschlüssels sein. Wenn ein geeigneter Ausgabeaktivierungsschlüssel ausgewählt worden ist, leitet Schritt **328** den Kartensicherheitscode in derselben Art und Weise ab und benutzt die selbe Information wie in Schritt **110** in Fig. 3. Weil derselbe Aktivierungsschlüssel benutzt wird, zusammen mit derselben Information für die Karte, wird ein identischer Sicherheitscode abgeleitet. Schließlich schickt Schritt **330** diesen abgeleiteten Sicherheitscode zurück zur Kartenausgabemaschine **24** zur Vorlage bei der intelligenten Zahlkarte **30**.

[0094] Andere Ausführungsformen sind durch Anwendung des Aktivierungssicherheitsanwendungsmoduls **208** auch für die Aktivierung der intelligenten Zahlkartekarte **30** geeignet. Beispielsweise kann die intelligente Zahlkarte **30**, während sie noch im Sicherheitsbenutzermodus ist, von einer Maschine ausgegeben werden oder von einem Kunden in Empfang genommen werden. Der Kunde kann später bei einer geeigneten Aktivierungsvorrichtung, die ein Aktivierungssicherheitsanwendungsmodul **208** enthält, die intelligente Zahlkarte **30** vorlegen und die Karte an diesem Punkt aktivieren durch Anwendung eines ähnlichen Prozesses, wie in den Fig. 8A und Fig. 8B gezeigt. Außerdem könnte eine solche Aktivierung an einem Handelsort, Kiosk oder an einer anderen öffentlichen Stelle, wo sich eine Aktivierungsvorrichtung befindet, stattfinden, oder sie könnte durch Gebrauch jeder geeigneten Computervorrichtung mit einer Netzwerkverbindung stattfinden. Zum Beispiel könnte die Funktionalität der Kartenausgabemaschine **24** über das Internet aufgeteilt werden. In diesem Beispiel gibt ein Kunde eine nicht aktivierte Karte in einen Kartenleser, der Zuhause oder im Büro an einem Personalcomputer angebracht ist. Von diesem Ort kommuniziert die intelligente Zahlkarte **30** mittels des Personalcomputers über das Internet mit dem Aktivierungssicherheitsanwendungsmodul **208**, das sich an einem entfernten Ort befindet. Befehle und Kommunikation zwischen der intelligenten Zahlkarte **30** und dem Aktivierungssicherheitsanwendungsmodul **208** können noch in derselben Art und Weise, wie oben beschrieben, ablaufen, abgesehen davon, dass die beiden Vorrichtungen entfernt voneinander sein würden. Andere Szenarien, in denen die intelligente Zahlkarte **30** aktiviert werden könnte, sind auch möglich.

[0095] Fig. 9 veranschaulicht ein Szenario **400**, in dem die intelligente Zahlkarte **30** durch Anwendung eines entfernten Aktivierungssicherheitsanwendungsmoduls **208** aktiviert wird. Das Szenario **400** zeigt einen Benutzercomputer **402** in Kommunikation

mit jeder geeigneten Computervorrichtung **404** über jede geeignete Telekommunikationsverbindung **406** wie das Internet. Mit dem Benutzercomputer **402** in Verbindung wird die intelligente Zahlkarte **30** in Verbindung gebracht, die einer Kartenleservorrichtung vorgelegt wird, die an dem Benutzercomputer **402** angebracht ist. Auf ähnliche Weise und Weise befindet sich das Aktivierungssicherheitsanwendungsmodul **208** entweder in einer Kartenlesevorrichtung, die an der Computervorrichtung **404** befestigt ist, oder es wird in einer Kartenausgabemaschine **24** oder in einer anderen Vorrichtung, die eine ähnliche Funktionalität hat, implementiert.

Feldwartung des Aktivierungssicherheitsanwendungsmoduls

[0096] Fig. 10 veranschaulicht ein Szenario **500**, in welchem eine Feldwartung auf dem Aktivierungssicherheitsanwendungsmodul **208** durchgeführt wird. In dieser Ausführungsform wird das Feldsicherheitsmodul (FSAM) **502** in der Kartenausgabemaschine **24** vorgelegt und ist in der Lage, die Wartung des Aktivierungssicherheitsanwendungsmoduls **208** in dem Feld durchzuführen.

[0097] Die vorigen Ausführungen der Fig. 4 und Fig. 6 veranschaulichen die Wartung des Aktivierungssicherheitsanwendungsmoduls **208**, die durch den Aktivierungssteuerungscomputer **202** unter Kontrolle des Kontrollsicherheitsmoduls **206** durchgeführt wird. Diese Ausführung zieht in Erwägung, dass entweder das Aktivierungssicherheitsanwendungsmodul **208** physikalisch einer Kartenlesevorrichtung, die an dem Aktivierungssteuerungscomputer **202** angebracht ist, vorgelegt wird, oder eine Telekommunikationsverbindung zwischen dem Aktivierungssteuerungsteuerungscomputer **202** und einer Kartenausgabemaschine, in der das Aktivierungssicherheitsanwendungsmodul **208** präsent ist, vorhanden ist. In anderen Szenarien ist es jedoch wünschenswert, das Aktivierungssicherheitsanwendungsmodul **208** in dem Feld ohne die Notwendigkeit einer Telekommunikationsverbindung zurück zum Aktivierungssteuerungsteuerungscomputer **202** oder das Erfordernis, dass das Aktivierungssicherheitsanwendungsmodul **208** physikalisch zurück zum Aktivierungssteuerungscomputer **202** transportiert wird, zu warten. Zum Beispiel können viele Kartenausgabemaschinen nicht die Funktionalität haben, mit dem Aktivierungssteuerungscomputer **202**, um die Wartung des Aktivierungssicherheitsanwendungsmoduls **208** durchzuführen, über eine sichere Verbindung zu kommunizieren und/oder es kann schwierig und teuer sein, das Aktivierungssicherheitsanwendungsmodul **208** zurückzuschicken. Weil eine Kartenausgabemaschine regelmäßig von Wartungstechnikern für die physikalische Wartung aufgesucht werden (zum Entfernen von Bargeld und/oder des Wiederauffüllens intelligenter Zahlkarten), würde es von Vorteil sein, die Wartung des Aktivierungssicherheitsanwendungsmodul zur selben Zeit durchzuführen.

[0098] Zu diesen Zwecken kann ein Feldsicherheitsmodul **502** von einem Wartungstechniker in eine Kartenausgabemaschine **24** geführt werden, wenn es gewartet wird und in einen Kartenlesevorrichtung, die an der Kartenausgabemaschine **24** angebracht ist, eingegeben wird. Der Wartungsprozess des Aktivierungssicherheitsanwendungsmodul **208** wird dann durch einen Code innerhalb des Feldsicherheitsmoduls **502** kontrolliert. Das Feldsicherheitsmodul **502** kann jede geeignete Vorrichtung, ähnlich des Kontrollsicherheitsmoduls **206**, für die Durchführung einer Wartung des Aktivierungssicherheitsanwendungsmoduls sein. Zum Beispiel könnte das Feldsicherheitsmodul **502** ein technischer Sicherheitsbaustein sein, obwohl es vorzugsweise auf einer Chipkarte implementiert ist.

[0099] Aus Sicht des Aktivierungssicherheitsanwendungsmoduls bleibt der Wartungsprozess derselbe. Der Aktivierungssteuerungssteurungscomputer **202** wird jetzt sowohl für die Erzeugung und Wartung des Feldsicherheitsmoduls verantwortlich sein als auch für die Erzeugung des Aktivierungssicherheitsanwendungsmoduls. Mit Ausnahme der unten bemerkten Unterschiede kann die Erzeugung und Wartung eines Feldsicherheitsmoduls auf eine ähnliche Art und Weise wie die zuvor oben in den Fig. 4.6 beschriebenen durchgeführt werden.

[0100] In einer Ausführung unterscheidet sich die Erzeugung und Wartung des Feldsicherheitsmoduls von der Erzeugung und Wartung des Aktivierungssicherheitsanwendungsmoduls. Wenn ein Bereichsschlüssel zunächst geladen oder in einem Feldsicherheitsmodul ersetzt wird, wird das Feldsicherheitsmodul beide, den neuen Bereichsschlüssel und den alten Bereichsschlüssel, beibehalten, um sicherzustellen, dass es durch Anwendung des vorigen Bereichsschlüssels noch mit den Aktivierungssicherheitsanwendungsmodulen kommunizieren kann. Zusätzlich wird jedes Feldsicherheitsmodul einen maximalen Aktivierungskontrollzählerwert und einen aktuellen Aktivierungskontrollzählerwert ähnlich solchen, die von den Aktivierungssicherheitsanwendungsmodulen getragen werden. Jederzeit lädt ein Feldsicherheitsmodul einen neuen Aktivierungskontrollzählerwert in ein Aktivierungssicherheitsanwendungsmodul, es wird seinen eigenen gegenwärtigen Aktivierungskontrollzählerwert um einen entsprechenden Betrag dekrementieren. Wenn sein eigener aktueller Aktivierungskontrollzählerwert 0 ist, kann es nicht länger die Wartung auf den Aktivierungssicherheitsanwendungsmodulen durchführen. Dieses zusätzliche Niveau an Sicherheit begrenzt die Zahl der Karten, den ein Feldsicherheitsmodul erlauben kann, ein Aktivierungssicherheitsanwendungsmodul zu aktivieren.

[0101] Ein Vorteil des Gebrauchs eines Feldsicherheitsmoduls, eine Feldwartung durchzuführen, ist der, das die Funktionalität, die normalerweise durch das Kontrollsicherheitsmodul **206** kontrolliert wird, an verschiedene Feldsicherheitsmodul delegiert werden kann, so dass die Aktivierungssicherheitsanwendungsmodul eine größere Effizienz in dem Feld beibehalten können. Trotzdem ist die Delegation dieser Befugnis mit zusätzlichen Risiken verbunden. Um das Risiko zu vermindern, dass mit der Erlaubnis, die Wartung des Feldes durch die Feldsicherheitsmodul auszuführen, verbunden ist, ist es besser, den Umfang der Wartung, den ein einzelnes Feldsicherheitsmodul durchführen kann, abzugrenzen.

[0102] Beispielsweise veranschaulicht Fig. 11 ein Szenario **600**, in dem die Feldsicherheitsmodul nur in der Lage sind, die Wartung auf Teilmengen aller Aktivierungssicherheitsanwendungsmodule in dem Feld durchzuführen. Das Szenario **600** veranschaulicht das Kontrollsicherheitsmodul **601**, der die erzeugten Feldsicherheitsmodule **602**-**606** hat. Das Feldsicherheitsmodul **602** wird als das betrachtet, auf das die Aktivierungssicherheitsanwendungsmodul **610** zurückgehen und welches für die Wartung jeglicher Aktivierungssicherheitsanwendungsmodule **610** verantwortlich ist. Auf ähnliche Art und Weise sind die Feldsicherheitsmodule **604** und **606** für jede Zahl der Aktivierungssicherheitsanwendungsmodule **612** beziehungsweise **614** verantwortlich.

[0103] In Verbindung mit dem Kontrollsicherheitsmodul **601** stehend ist ein Hauptbereichsschlüssel **620**, der für die Ableitung der Bereichsschlüssel für die Feldsicherheitsmodule und Aktivierungssicherheitsanwendungsmodule benutzt wird. Bei Anwendung eines geeigneten Feldsicherheitsmodulsidentifikators, wird der Hauptbereichsschlüssel **620** benutzt, um die Feldbereichsschlüssel **630** abzuleiten, einen pro Feldsicherheitsmodul. Jeder Feldsicherheitsmodulfeldbereichsschlüssel nacheinander wird verwendet, die Bereichsschlüssel **640** für jedes Aktivierungssicherheitsanwendungsmodul abzuleiten, die auf das Feldsicherheitsmodul zurückgehen. Beispielsweise wird der Aktivierungssicherheitsanwendungsmoduidentifikator jedes Aktivierungssicherheitsanwendungsmoduls **610** in Verbindung mit dem Feldbereichsschlüssel für das Feldsicherheitsmodul **602** benutzt, um den eindeutigen Bereichsschlüssel für jedes Aktivierungssicherheitsanwendungsmodul **610** abzuleiten. Wie zuvor beschrieben, wird dieser Bereichschlüssel für die sichere Kommunikation zwischen einem der Aktivierungssicherheitsanwendungsmodule **610** und dem Feldsicherheitsmodul **602** benutzt. In ähnliche Art und Weise wird der Feldbereichschlüssel für das Feldsicherheitsmodul **602** für die sichere Kommunikation zwischen dem Feldsicherheitsmodul **602** und dem Kontrollsicherheitsmodul **601** gebraucht. Wenn der Aktivierungssteuerungscomputer **202** ein spezielles Aktivierungsanwendungssicherheitsmodul erzeugt, führt er zusätzliche Schritte aus. Zunächst ordnet er ein spezielles Aktivierungssicherheitsanwendungsmodul einem Feldsicherheitsmodul zu. Dann leitet er den Feldsicherheitsmodulbereichsschlüssel ab, und von diesem leitet er den geeigneten Aktivierungsanwendungssicherheitsmodulbereichsschlüssel ab. Auf diese Art delegiert das Kontrollsicherheitsmodul **601** die Befugnis für die Wartung der Aktivierungssicherheitsanwendungsmodule in dem Feld, jedoch für jedes Feldsicherheitsmodul mit einem begrenzten Gültigkeitsbereich.

[0104] Wenn ein Feldsicherheitsmodul nun ein Aktivierungssicherheitsanwendungsmodul in dem Feld innerhalb einer Kartenausgabemaschine wartet, ist es besser, dass eine Kartenausgabemaschine einen Teil der Software enthält, die zuvor auf den Aktivierungssteuerungscomputer **202** implementiert wurde, um die Wartung des Aktivierungssicherheitsanwendungsmoduls zu unterstützen. Alternativ kann ein Feldsicherheitsmodul eine höhere Prozessorkarte sein, die all die Steuerlogik und Software für die Steuerung der Wartung eines Aktivierungssicherheitsanwendungsmoduls enthält.

Sicherheitsausführung

[0105] Fig. 12 stellt eine mögliche Sicherheitsausführung dar, die die Information veranschaulicht, die in dem Aktivierungssteuerungscomputer **202** und dem Kontrollsicherheitsmodul **206** enthalten sind. Szenario **700** veranschaulicht einen Aktivierungssteuerungscomputer **202**, der assoziierte Informationen **701** hat und in Kommunikation mit dem Kontrollsicherheitsmodul **206** steht. Ein lokaler Hauptschlüssel (LMK) **702** ist sicher in dem Kontrollsicherheitsmodul **206** gespeichert, das eine sichere Stelle für diesen wichtigen Schlüssel zur Verfügung stellt. Es wird einsehbar sein, dass das Kontrollsicherheitsmodul **206** ein Sicherheitsmodul oder eine Sicherheitskarte ist, mit denen es notwendig ist, Aktivierungssicherheitsanwendungsmodule und Feldsicherheitsmodule zu erzeugen und zu warten.

[0106] Wie vorausgehend in Fig. 4 erwähnt, kann die Information **701**, die mit dem Aktivierungssteuerungscomputer **202** verknüpft ist, in dem Kontrollsicherheitsmodul **206** oder in einer Sicherheitsdatenbank gespeichert werden, die nur mit Berechtigung von dem Kontrollsicherheitsmodul **206** zugänglich ist, wie zum Beispiel durch Anwendung des lokalen Hauptschlüssels. Benutzerkennwörter **710** sind für Einzelne erforderlich, die den Aktivierungssteuerungscomputer **202** benutzen möchten, um die Erzeugung und Wartung durchzuführen. Aktivierungsschlüssel **712** sind in Verbindung mit einem Aktivierungsschlüsselindex **714** gespeichert, der als Indices den Ausgabeidentifikator, den Kartenlieferantenidentifikator und die Aktivierungsschlüsselversionsnum-

mer enthält. Hauptbereichsableitungsschlüssel **716** werden benutzt, um Feldbereichsschlüssel für jede Anzahl von Feldsicherheitsmodulen abzuleiten. Es können mehrere oder nur ein Hauptbereichsschlüssel vorhanden sein. Ein Aktivierungssicherheitsanwendungsmodulverzeichnis **718** enthält eine Liste sämtlicher aktiver Anwendungssicherheitsanwendungsmodule zusammen mit jedem Aktivierungssicherheitsanwendungsmodulidentifikator, seinem maximalen erlaubten Aktivierungskontollzählerwert, und seinen assoziierten Stammfeldsicherheitsanwendungsmodulen. Auf diese Weise hat der Aktivierungssteuerungscomputer **202** alle ihm zur Verfügung stehenden relevanten Informationen für die Erzeugung und Wartung der Aktivierungssicherheitsanwendungsmodule und der Feldsicherheitsmodule.

Computersystemausführung

[0107] Die Fig. 13 und Fig. 14 veranschaulichen ein Computersystem **900**, das geeignet für die Realisierung der Ausführungen der vorliegenden Erfindung ist. Die Fig. 13 zeigt eine mögliche physikalische Ausbildung des Computersystems. Natürlich kann das Computersystem viele physikalische Ausbildungen haben, die von einer integrierten Schaltung, einer gedruckten Schaltung und einem kleinen Handgerät bis zu einem riesigen Supercomputer reichen. Das Computersystem **900** enthält einen Monitor **902**, einen Bildschirm **904**, ein Gehäuse **906**, ein Plattenlaufwerk **908**, eine Tastatur **910** und eine Maus **912**. Eine Wechselplatte **914** ist ein maschinenlesbares Medium, das benutzt wird, um Daten zum und von dem Computersystem **900** zu übertragen.

[0108] Die Fig. 14 ist ein Beispiel eines Blockschemas für ein Computersystem **900**. Einem Systembus **920** ist ein breites Spektrum von Untersystemen angeschlossen. Prozessoren) **922** (die auch Zentraleinheiten, oder CPU's bezeichnet werden) sind mit Speichervorrichtungen gekoppelt, die einen Speicher **924** enthalten. Der Speicher **924** enthält einen Arbeitsspeicher (RAM) und einen Festspeicher (ROM). Es ist in der Technik wohlbekannt, dass der Festspeicher dazu dient, Daten und Befehle unidirektional zur Zentraleinheit zu übertragen und der Arbeitsspeicher wird typischerweise benutzt, um Daten und Befehle bidirektional zu übertragen. Beide Typen der Speicher können jede geeignete der oben beschriebenen maschinenlesbaren Medien enthalten. Eine Speicherplatte **926** ist auch bidirektional mit der Zentraleinheit **922** verbunden; sie stellt zusätzliche Datenspeicherkapazität zur Verfügung und kann auch jede der oben beschriebenen maschinenlesbaren Medien enthalten. Die Speicherplatte **926** kann benutzt werden, um Programme, Daten und dergleichen zu speichern und ist typischerweise ein Sekundärspeichermedium (beispielsweise ein Plattenspeicher), das langsamer als ein Primärspeicher ist. Es wird einsehbar sein, dass die Informationen, die auf der Festplatte **926** gehalten werden, in geeigneten Fällen als virtuelle Speicher in den Speicher **924** in Standardweise integriert ist. Die Wechselplatte **914** kann jede Form der oben beschriebenen maschinenlesbaren Medien annehmen.

[0109] Die Zentraleinheit **922** ist mit einer Auswahl von Ein- und Ausgabegeräten wie dem Bildschirm **904**, der Tastatur **910**, der Maus **912** und dem Lautsprecher **930** verbunden. Im allgemeinen können Ein- und Ausgabegeräte sein: Optische Anzeigen, Trackbälle, Mäuse, Tastaturen, Mikrophone, Berührungsbildschirme, Wandlerkartenleser, Magnetbandleser oder Lochstreifenleser, Tabletts, Pens, Spracherkennungseinrichtungen und Handschriftenerkennungseinrichtungen, biometrische Lesegeräte, oder andere Computer. Fakultativ kann die Zentraleinheit **922** mit anderen Computern oder Kommunikationsnetzen, die eine Netzwerk-Schnittstelle **940** benutzen, verbunden sein. Mit einer solchen Netzwerk-Schnittstelle wird beabsichtigt, dass die Zentraleinheit Informationen vom Netzwerk erhalten kann, oder Informationen an das Netzwerk im Verlauf der Ausführung der oben beschriebenen Verfahrenschritte ausgeben kann. Außerdem können Verfahrensausführungen der vorliegenden Erfindung ausschließlich nur in der Zentraleinheit **922** oder über ein Netwerk wie beispielsweise das Internet in Verbindung mit einer separaten Zentraleinheit, die einen Teil der Informationsverarbeitung gemeinsam nutzen, ausgeführt werden.

[0110] Außerdem beziehen sich weiter Ausführungen der vorliegenden Erfindung auf Rechnerspeicherprodukte mit maschinenlesbaren Datenträgern, die einen Rechnercode für die Durchführung von verschiedenen rechnerimplementierten Programmschritten haben. Der Datenträger- und Computercode können speziell für die Zwecke der vorliegenden Erfindung entworfen und konstruiert sein, oder wohlbekannt sein und solchen zur Verfügung stehen, die Fachwissen in Computersoftware haben. Beispiele von maschinenlesbaren Datenträgern beziehen ein, ohne sie darauf zu begrenzen: magnetische Datenträger, beispielsweise magnetische Festplatten, Floppy-Disk, und Magnetbänder, optische Datenträger wie CD-ROM's und holographische Vorrichtungen; magnetooptische Datenträger wie optische Disketten; und Hardware-Vorrichtungen, die speziell für die Speicherung und ausführung von Programmcodes ausgelegt sind, wie beispielsweise anwendungsspezfische Schaltkreise (ASIC-Schaltkreise), programmierbare Logikbausteine (PLD's) und Festspeicher (ROM) und Speicher mit wahlfreiem Zugriff (RAM). Beispiele für einen Computercode enthalten Maschinencode, wie beispielsweise von einem Compiler erstellt, und Dateien die einen höherwertigen Code enthalten, die von einem Computer durch Anwendung eines Interpretierers ausgeführt werden.

[0111] Obwohl die vorhergehende Erfindung in einigen Details zum Zwecke der Klarheit und des Verständnisses beschrieben worden ist, ist es offensichtlich, dass spezielle Änderungen und Modifikationen innerhalb des Schutzbereichs der hinzugefügten Patentansprüche praktiziert werden können. Zum Beispiel kann der Aktivierungsschlüssel direkt oder in Kombination mit anderen Codes und/oder Verschlüsselungscodes benutzt werden, um einen Sicherheitsode für die Karte bereitzustellen. Jedes Rechtsobjekt kann die Funktionen des Lieferanten oder der Ausgabe erfüllen. Auch kann die Kartenausgabemaschine Teil einer großen Maschine bilden, oder kann funktionell auf ein Rechnerverbund aufgeteilt werden. Zusätzlich kann jede geeignete Chipkarte, die in einen Sicherheitscode versetzt werden kann, benutzt werden. Ein Sicherheitscode kann durch ein Aktivierungssicherheitsanwendungsmodul während der Aktivierung erzeugt werden oder durch eine andere sichere Hardware-Vorrichtung, oder auch in Software. Es kann sogar ein manuell eingegebener Sicherheitscode erlaubt sein, um die Karte zu aktivieren. Demnach sollten die beschriebenen Ausführungen nur als erläuternde oder nicht als beschränkende aufgefasst werden, und die Erfindung sollte nicht auf die darin gegebenen Details begrenzt werden, sondern durch die folgenden Ansprüche bestimmt werden.

Patentansprüche

1. Ein System für die sichere Aktivierung intelligenter Zahlkarten (**30**) an einem Verteilerpunkt, folgendes aufweisend:
eine Kartenausgabemaschine (**24**) für die Aufnahme intelligenter Zahlkarten (**30**), wobei jede intelligente Zahlkarte (**30**) einen gespeicherten Wert (**80**) und einen Kartensicherheitscode (**72**) speichert, der Kartensicherheitscode ist so eingerichtet ist, dass ein unbefugter Zugriff auf den gespeicherten Wert auf der intelligenten Zahlkarte (**30**) verhindert ist, und
ein Aktivierungssicherheitsanwendungsmodul (**208**) zum Empfangen eines Ausgabeaktivierungsschlüssels (**40**) und zur Erzeugung eines abgeleiteten Kartensicherheitscodes, wobei das Aktivierungssicherheitsanwendungsmodul ein Verschlüsselungsmodul enthält, welches den abgeleiteten Kartensicherheitscode von dem Ausgabeaktivierungsschlüssel (**40**) ableitet,
und die Kartenausgabemaschine (**24**) eingerichtet ist, um den abgeleiteten Kartensicherheitscode von dem Aktivierungssicherheitsanwendungsmodul (**208**) zur Vorlage an die intelligente Zahlkarte abzufragen, bei einer Übereinstimmung des abgeleiteten Kartensicherheitscodes mit dem gespeicherten Kartensicherheitscode (**72**) wird die intelligente Zahlkarte aktiviert.

2. System nach Anspruch 1, dadurch gekennzeichnet, dass jede intelligente Zahlkarte weiterhin eine für die Zahlkarte eindeutige Information (**69**) enthält und das Verschlüsselungsmodul des Aktivierungssicherheitsanwendungsmoduls eingerichtet ist, um den abgeleiteten Kartensicherheitscode aus dem Ausgabeaktivierungsschlüssel (**40**) und der eindeutigen Information (**69**) abzuleiten.

3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Kartenausgabemaschine (**24**) das Aktivierungssicherheitsanwendungsmodul (**208**) enthält und das System weiterhin folgendes aufweist:
eine Ausgabe (**20**) von intelligenten Zahlkarten, wobei die Ausgabe einen geheimen Ausgabeaktivierungsschlüssel erzeugt, und
einen Kartenlieferanten (**22**), der den geheimen Ausgabeaktivierungsschlüssel von der Ausgabe (**20**) erhält, wobei der Kartenlieferant (**22**) basierend auf dem geheimen Ausgabeaktivierungsschlüssel eine Vielzahl von Ausgabekartensicherheitscodes ableitet,
und der Kartenlieferant (**22**) die intelligenten Zahlkarten (**30**) in einem Stapel liefert, der gespeicherte Kartensicherheitscode (**72**) auf jeder intelligenten Zahlkarte des Stapels ein von dem Sicherheitsausgabeaktivierungsschlüssel abgeleiteter Ausgabekartensicherheitscode ist, sich jede intelligente Zahlkarte weiterhin in einem Sicherheitsmodus befindet, so dass der auf jeder intelligenten Zahlkarte gespeicherte Wert für den Gebrauch unzugänglich ist, und
die Kartenausgabemaschine (**24**) so eingerichtet ist, dass das Aktivierungssicherheitsanwendungsmodul einen der Kartensicherheitscodes abfragt und dem Kartensicherheitscode einer gegebenen intelligenten Zahlkarte anbietet, wodurch die gegebene intelligente Zahlkarte aus dem Sicherheitsmodus genommen wird und zum Gebrauch zur Verfügung steht, sobald der angebotene Sicherheitscode mit dem gespeicherten Kartensicherheitscode (**72**) übereinstimmt.

4. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass
eine Datenbank (**210**) einen für die Aktivierung der intelligenten Zahlkarten notwendigen Hauptaktivierungsschlüssel (**212**) sicher speichert, wobei das Aktivierungssicherheitsanwendungsmodul (**208**) so eingerichtet ist, dass der Hauptaktivierungsschlüssel sicher speicherbar ist und das Verschlüsselungsmodul durch Anwendung des Hauptaktivierungsschlüssel den abgeleiteten Kartensicherheitscode ableitet, und
ein Kontrollsicherheitsmodul (**206**), das sicheren Zugriff auf den Hauptaktivierungsschlüssel (**212**) hat, und das
ein Aktivierungssteuerungscomputer (**202**) mit der Datenbank (**210**), dem Kontrollsicherheitsmodul (**206**) und dem Aktivierungssicherheitsanwendungsmodul (**208**) in Verbindung steht, wobei der Aktivierungssteuerungscomputer (**202**) eingerichtet ist, um den Hauptaktivierungsschlüssel (**212**) aus der Datenbank (**210**) über das Kontrollsicherheitsmodul (**206**) zu dem Aktivierungssicherheitsanwendungsmodul

(**208**) zu übertragen, wodurch das Aktivierungssicherheitsanwendungsmodul (**208**) imstande ist, die abgeleiteten Kartensicherheitscodes durch Anwendung des Hauptaktivierungsschlüssels (**212**) zu erzeugen.

5. System nach Anspruch 4, dadurch gekennzeichnet, dass das Aktivierungssicherheitsmodul (**208**) weiterhin einen Aktivierungskontrollzähler aufweist, der die Zahl der intelligenten Zahlkarten begrenzt, die das Aktivierungssicherheitsmodul aktivieren kann.

6. System nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass das Aktivierungssicherheitsanwendungsmodul (**208**) weiterhin einen Bereichsschlüssel (**640**) aufweist, der die sichere Kommunikation zwischen dem Aktivierungssicherheitsanwendungsmodul (**208**) und dem Kontrollsicherheitsmodul ermöglicht.

7. System nach Anspruch 1 bis 3, dadurch gekennzeichnet, dass das System folgendes aufweist:
ein Feldsicherheitsmodul (**502**), das einen Feldaktivierungsschlüssel (**630**) speichert, der notwendig für die Aktivierung der intelligenten Zahlkarten (**30**) ist,
wobei das Aktivierungssicherheitsanwendungsmodul (**208**) eingerichtet ist, um den Feldaktivierungsschlüssel (**630**) sicher zu speichern und das Verschlüsselungsmodul eingerichtet ist, um die abgeleiteten Kartensicherheitscodes von dem Feldaktivierungsschlüssel abzuleiten, und
die Kartenausgabemaschine eingerichtet ist, um den Feldaktivierungsschlüssel von dem Feldsicherheitsmodul (**502**) dem Aktivierungssicherheitsanwendungsmodul (**208**) zu übertragen, wodurch das Aktivierungssicherheitsanwendungsmodul (**208**) imstande ist, die abgeleiteten Kartensicherheitscodes durch Anwendung des Aktivierungsschlüssels zu erzeugen.

8. System nach Anspruch 7, dadurch gekennzeichnet, dass das Aktivierungssicherheitsanwendungsmodul weiterhin einen Aktivierungskontrollzähler aufweist, der die Zahl der intelligenten Zahlkarten begrenzt, die das Aktivierungssicherheitsanwendungsmodul (**208**) aktivieren kann, wobei das Feldsicherheitsmodul einen neuen Maximumwert zur Erneuerung des Aktivierungskontrollzählers des Aktivierungssicherheitsmodul enthält.

9. System nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass das System folgendes aufweist:
einen Kontrollsicherheitsmodul (**601**), das einen Hauptbereichsschlüssel (**620**) besitzt,
eine Vielzahl von Feldsicherheitsmodulen (**602**,**604**,**606**), wobei das Kontrollsicherheitsmodul (**601**) mit den Feldsicherheitsmodulen durch Anwendung der Feldbereichschlüssel (**630**), die von dem Hauptbereichsschlüssel (**620**) abgeleitet sind, in Verbindung steht, und
eine Vielzahl von Sätzen von Aktivierungssicherheitsanwendungsmodulen (**610**,**612**,**614**), wobei jeder Satz der Aktivierungssicherheitsanwendungsmodulen durch Anwendung eines Bereichsschlüssels (**640**), der von einem der Feldbereichsschlüsseln (**630**) abgeleitet ist, mit einem der Feldsicherheitsmodulen (**602**,**604**,**606**) in Verbindung steht.

10. System nach Anspruch 7 bis 9, dadurch gekennzeichnet, dass das oder jedes Feldsicherheitsmodul eine Chipkarte oder ein Hardwaresicherheitsmodul ist.

11. Verfahren zur sicheren Aktivierung intelligenter Zahlkarten (**30**), die in einer Kartenaufnahmevorrichtung enthalten sind, mit folgenden Schritten:
Feststellen, ob eine gegebene intelligente Zahlkarte (**30**) sich in einem Sicherheitsmodus befindet (Schritt **308**), wobei die intelligente Zahlkarte einen gespeicherten Kartensicherheitscode aufweist;
Ableiten eines abgeleiteten Kartensicherheitscode durch Anwendung eines Aktivierungssicherheitsanwendungsmoduls (**208**) und eines Ausgabeaktivierungsschlüssels (Schritt **310**);
Anbieten des abgeleiteten Kartensicherheitscode der intelligenten Zahlkarte (Schritt **312**); Aktivieren der intelligenten Zahlkarte, so dass der Wert auf der intelligenten Zahlkarte für den Gebrauch verfügbar ist, wenn der abgeleitete Kartensicherheitscode mit dem gespeicherten Kartensicherheitscode übereinstimmt, und
Ausgabe der intelligenten Zahlkarten aus der Kartenaufnahmevorrichtung (Schritt **314**).

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass
eine eindeutige Information von der intelligenten Zahlkarte gelesen wird und
durch Gebrauch der eindeutigen Information und des Ausgabeaktivierungsschlüssels der abgeleitete Kartensicherheitscode abgeleitet wird.

13. Verfahren nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass festgestellt wird, ob ein Aktivierungskontrollzähler des Aktivierungssicherheitsanwendungsmodul (**208**) eine Grenze erreicht hat (Schritt **320**), wobei bei Feststellung, dass die Grenze erreicht wurde, durch den Aktivierungskontrollzähler das Verfahren zur Aktivierung der intelligenten Zahlkarte abgebrochen wird (Schritt **322**).

14. Verfahren nach einem der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass an einem Verteiler eine intelligente Zahlkarte, die einen gespeicherten Wert hat, erzeugt wird (Schritt **102**);
ein Ausgabeaktivierungsschlüssel von einem Ausgabeelement erhalten wird (Schritt **106**);
durch Anwendung des erhaltenen Ausgabeaktivierungsschlüssels ein Sicherheitscode für die intelli-

gente Zahlkarte erzeugt wird (Schritt **110**); der erzeugte Sicherheitscode auf der intelligenten Zahlkarte installiert wird (Schritt **112**);
die intelligente Zahlkarte in einen Sicherheitsmodus gebracht wird, so dass der gespeicherte Wert nicht zur Verfügung steht;
die intelligente Zahlkarte zum Ausgabeelement geliefert wird (Schritt **116**), wodurch die intelligente Zahlkarte auf sichere Art und Weise geliefert wird, da der gespeicherte Wert nicht verfügbar ist.

15. Verfahren gemäß Anspruch 14, dadurch gekennzeichnet, dass die Erzeugung des Sicherheitscodes weiterhin das Lesen der eindeutigen Information von der intelligenten Zahlkarte und das Ableiten des Sicherheitscodes durch Anwendung

16. Verfahren nach einem der Ansprüche 11 bis 15, dadurch gekennzeichnet, dass
ein Aktivierungssteuerungscomputer (**202**) in Verbindung mit einem Kontrollsicherheitsmodul (**206**) und dem Aktivierungssicherheitsanwendungsmodul (**208**) gebracht wird;
durch Anwendung des Kontrollsicherheitsmoduls (**206**) ein Hauptaktivierungsschlüssel (**212**) aus der Datenbank (**210**) wiederaufgefunden wird, wobei der Hauptaktivierungsschlüssel (**212**) notwendig für die Aktivierung der intelligenten Zahlkarten ist;
Verschlüsselungssoftware in das Aktivierungssicherheitsanwendungsmodul (**208**) geladen wird, um dem Aktivierungssicherheitsanwendungsmodul die Erzeugung des Kartensicherheitscodes unter Anwendung des Hauptaktivierungsschlüssels zu ermöglichen; und
der wiederaufgefundene Aktivierungsschlüssel zum Aktivierungssicherheitsanwendungsmodul (**208**) übertragen wird, wodurch das unter Anwendung des Hauptaktivierungsschlüssels zu erzeugen.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass ein Maximumwert für den Aktivierungskontrollzähler in das Aktivierungssicherheitsanwendungsmodul (**208**) geladen wird, wobei der Aktivierungskontrollzähler die Anzahl der intelligenten Zahlkarten begrenzt, die das Aktivierungssicherheitsanwendungsmodul aktivieren kann.

18. Verfahren nach Anspruch 16 oder 17, dadurch gekennzeichnet, dass zusätzlich ein Bereichsschlüssel in das Aktivierungssicherheitsanwendungsmodul (**208**) geladen wird, wobei der Bereichsschlüssel die sichere Kommunikation zwischen dem Aktivierungssicherheitsanwendungsmodul und dem Kontrollsicherheitsmodul ermöglicht.

19. Verfahren nach einem der Ansprüche 11 bis 18, dadurch gekennzeichnet, dass zusätzlich
eine Vielzahl der intelligenten Zahlkarten in einer Kartenausgabemaschine (**24**) plaziert wird, wobei die intelligenten Zahlkarten jeweils einen Kartensicherheitscode erfordern, bevor ihr Wert zugänglich ist,
ein Feldsicherheitsmodul (**502**) in Verbindung mit dem Aktivierungssicherheitsanwendungsmodul (**208**) der Kartenausgabemaschine (**24**) gebracht wird, wobei das Feldsicherheitsmodul einen Feldaktivierungsschlüssel aufweist, der notwendig für die Aktivierung der intelligenten Zahlkarten ist, der Feldaktivierungsschlüssel von dem Feldsicherheitsmodul (**502**) wiedergewonnen wird und
der wiedergewonnene Feldaktivierungsschlüssel zum Aktivierungssicherheitsanwendungsmodul (**208**) übertragen wird, wodurch das Aktivierungssicherheitsanwendungsmodul (**208**) nun imstande ist, durch Anwendung des Feldaktivierungsschlüssel die Kartensicherheitscodes zu erzeugen.

20. Verfahren nach Anspruch 19, dadurch gekennzeichnet, dass ein neuer Maximumwert für einen Aktivierungskontrollzähler von dem Feldsicherheitsmodul abgerufen wird und der Aktivierungskontrollzähler des Aktivierungssicherheitsanwendungsmodul (**208**) durch Anwendung des abgerufenen neuen Maximumwerts zurückgestellt wird, wobei der Aktivierungskontrollzähler die Anzahl der intelligenten Zahlkarten, die das Aktivierungssicherheitsanwendungsmodul (**208**) aktivieren kann, begrenzt.

21. Verfahren nach einem der Ansprüche 11 bis 20, dadurch gekennzeichnet, dass
eine Verbindung über ein Kommunikationsnetz zwischen dem Aktivierungssteuerungscomputer (**202**), der ein Kontrollsicherheitsmodul (**206**) aufweist, und der Kartenausgabemaschine (**24**) eingeleitet wird, wobei die Kartenausgabemaschine das Aktivierungssicherheitsanwendungsmodul (**208**) enthält und eine Vielzahl der intelligenten Zahlkarten (**30**), die, bevor ihr Wert zugänglich ist, einen Kartensicherheitscode (**72**) erfordern,
das Kontrollsicherheitsmodul (**206**) in Verbindung mit dem Aktivierungssicherheitsanwendungsmodul (**208**) der Kartenausgabemaschine gebracht wird, wobei das Kontrollsicherheitsmodul (**206**) einen Kontrollaktivierungsschlüssel enthält, der notwendig für die Aktivierung der intelligenten Zahlkarten ist,
der Kontrollaktivierungsschlüssel von dem Kontrollsicherheitsmodul (**206**) abgerufen wird und
der abgerufene Kontrollaktivierungsschlüssel zum Aktivierungssicherheitsanwendungsmodul (**208**) über ein Kommunikationsnetz übertragen wird, wodurch das Aktivierungssicherheitsanwendungsmodul (**208**) nun imstande ist, durch Anwendung des Kontrollaktivierungsschlüssels die Kartensicherheitscodes zu erzeugen.

Es folgen 14 Blatt Zeichnungen

Anhängende Zeichnungen

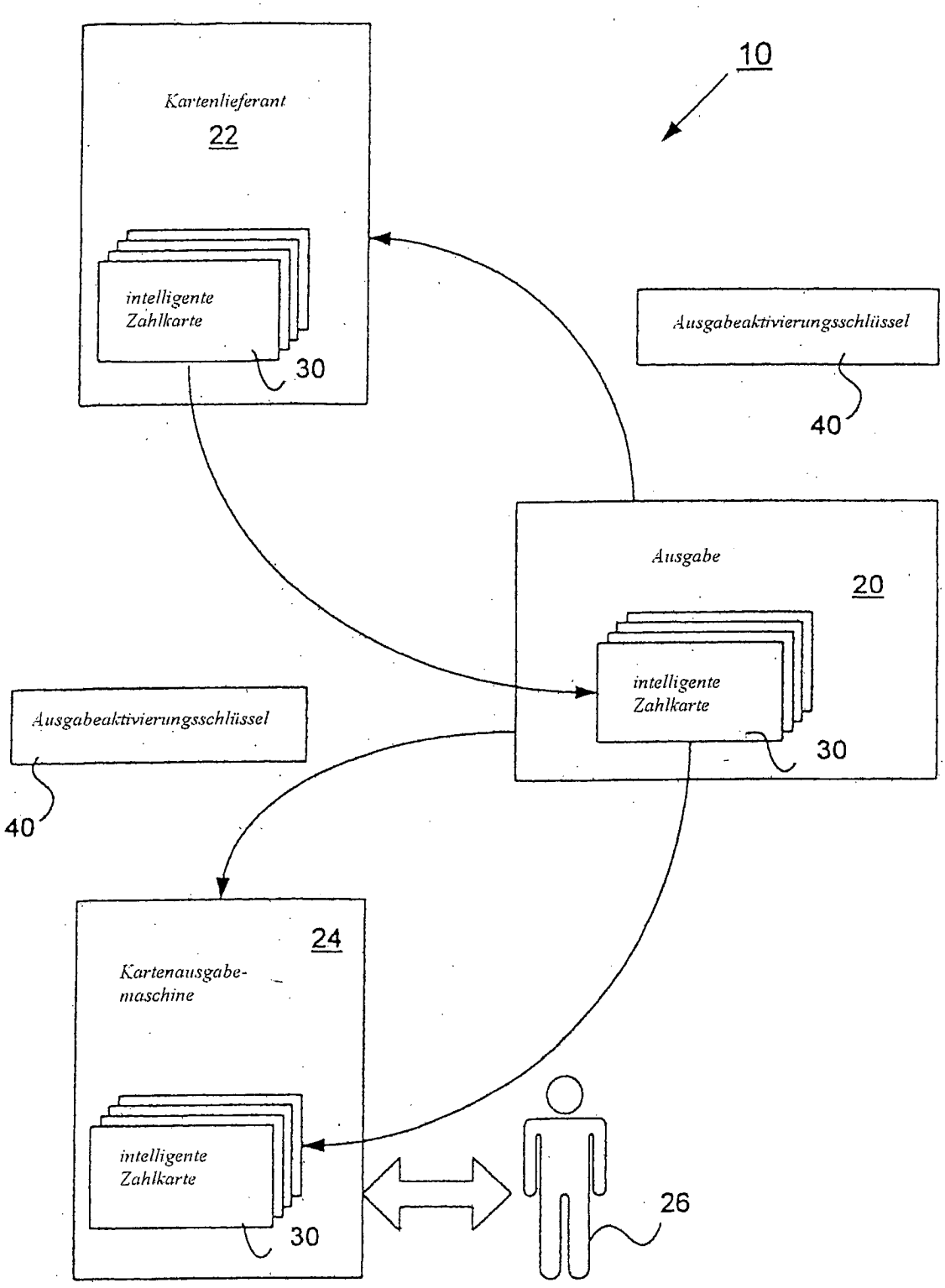


FIG. 1

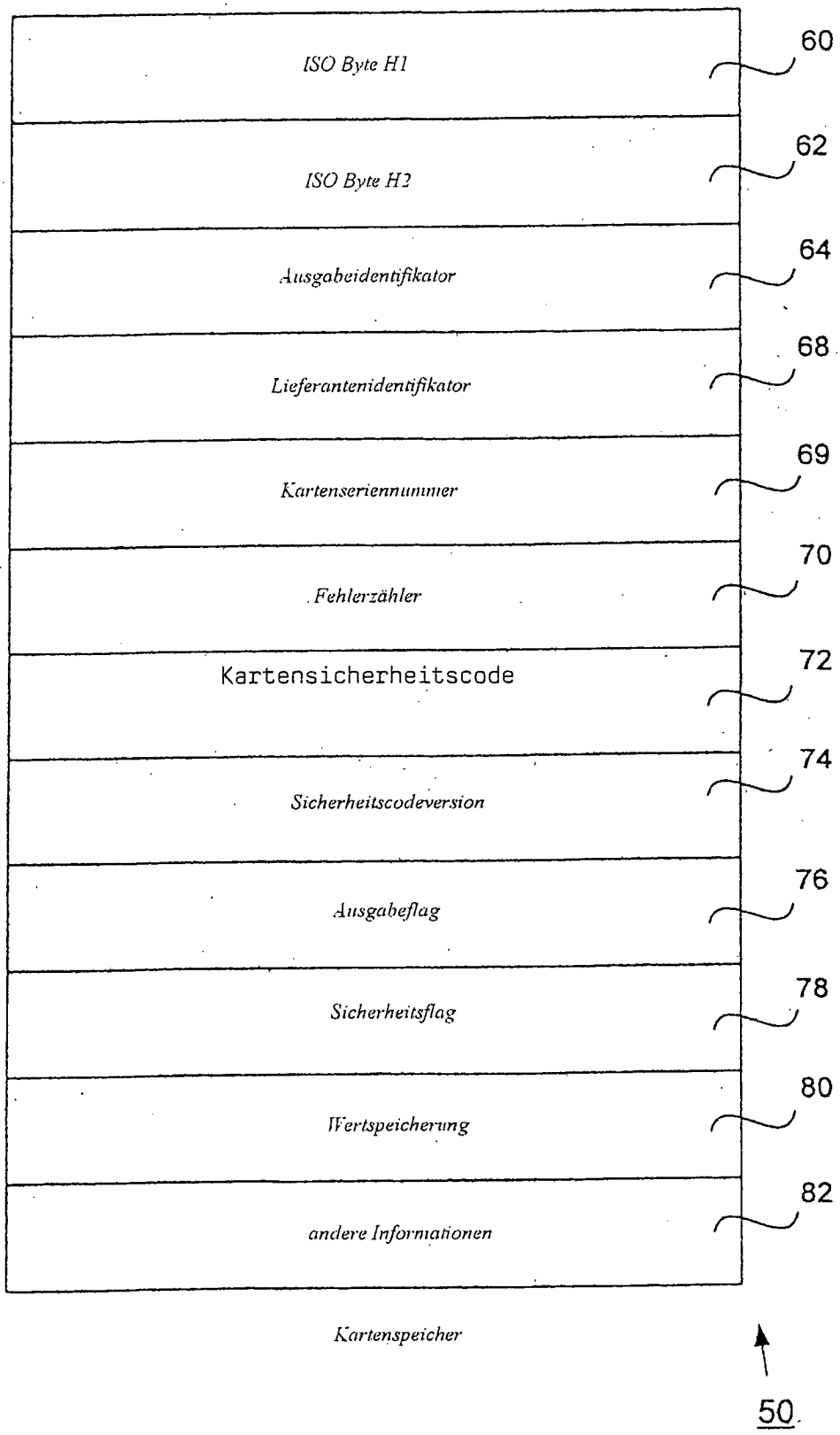

ISO Byte H1
60
ISO Byte H2
62
Ausgabeidentifikator
64
Lieferantenidentifikator
68
Kartenseriennummer
69
Fehlerzähler
70
Kartensicherheitscode
72
Sicherheitscodeversion
74
Ausgabeflag
76
Sicherheitsflag
78
Wertspeicherung
80
andere Informationen
82
Kartenspeicher
50

FIG. 2

FIG. 3

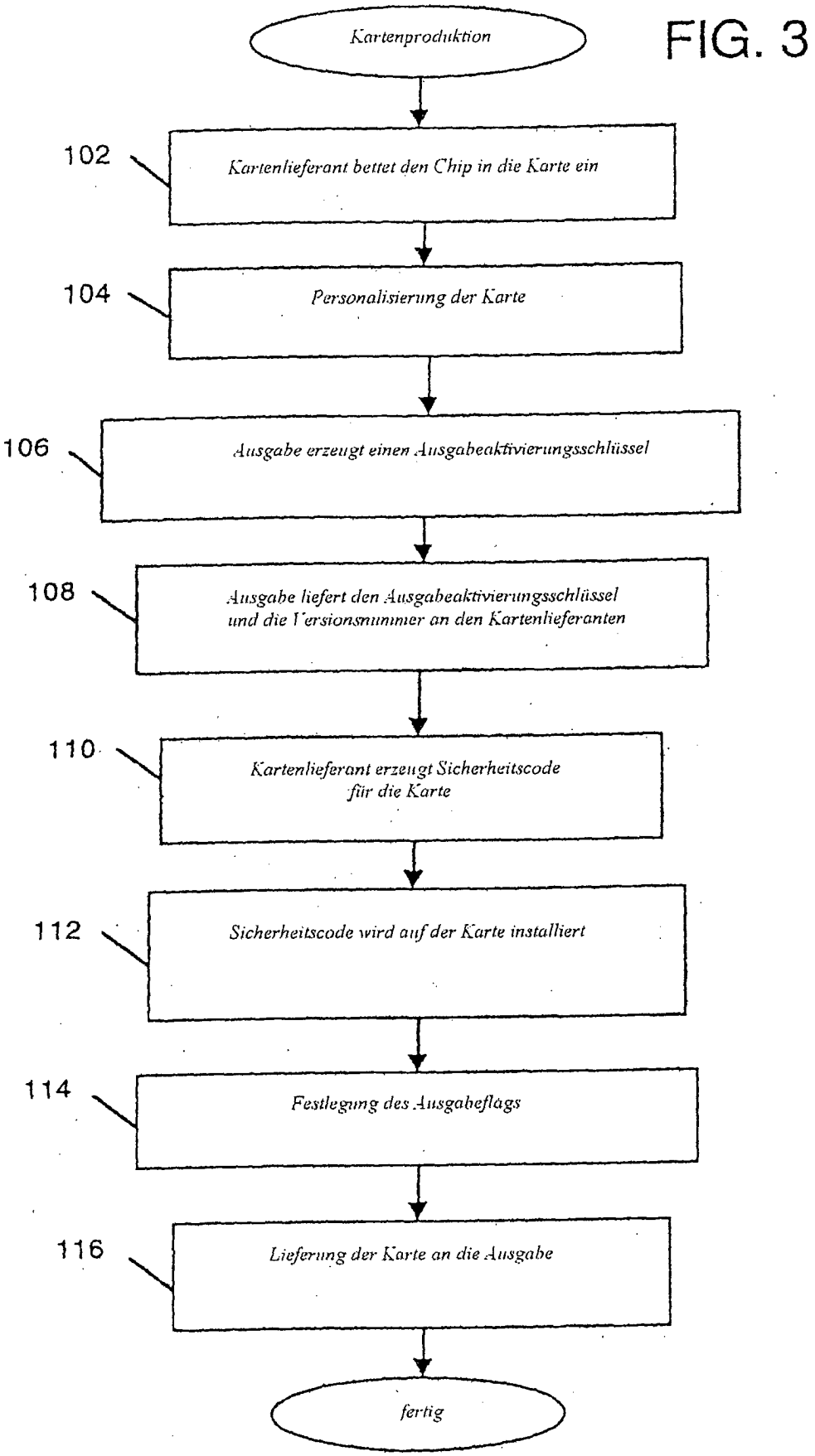
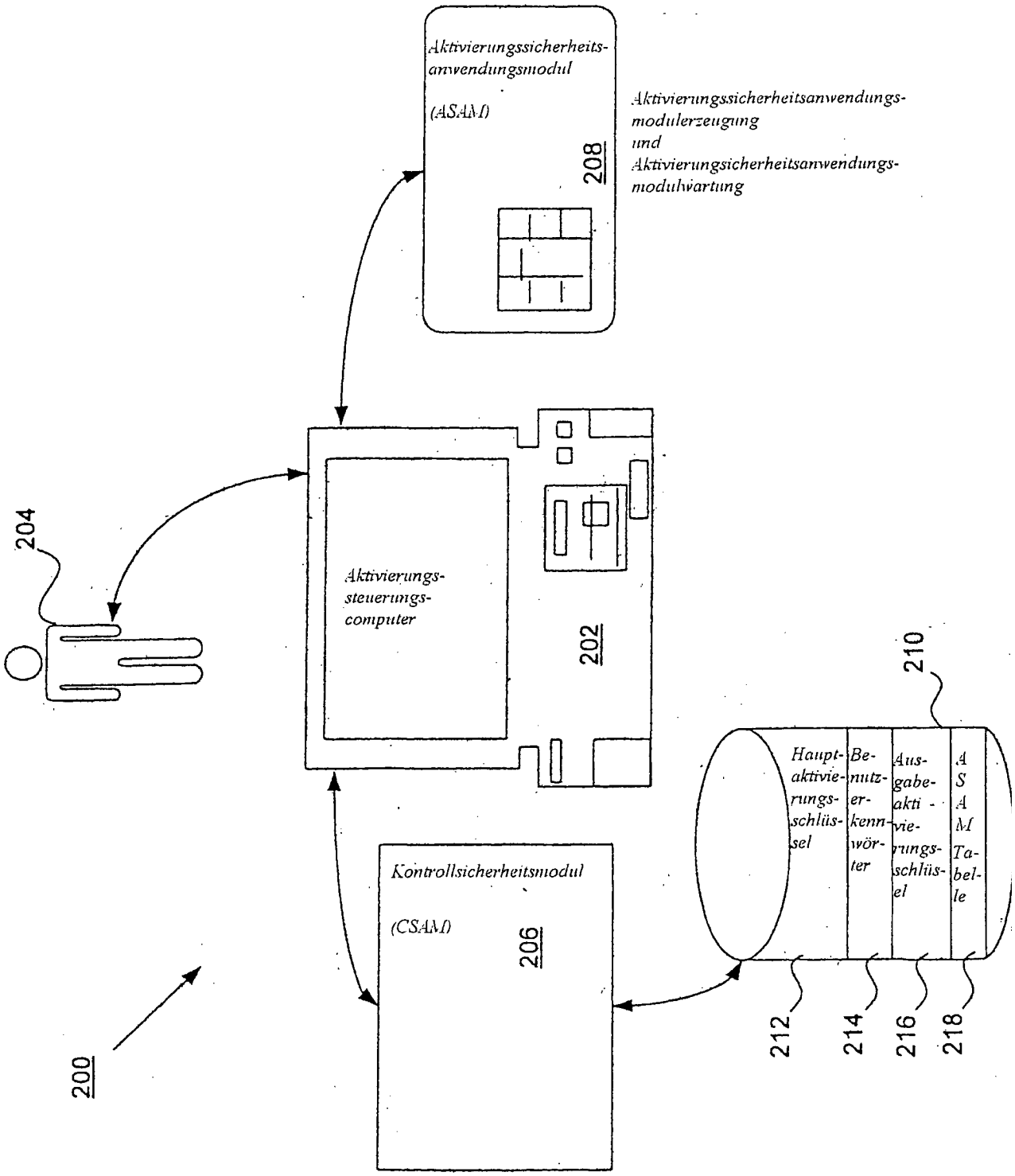

Kartenproduktion
102
Kartenlieferant bettet den Chip in die Karte ein
104
Personalisierung der Karte
106
Ausgabe erzeugt einen Ausgabeaktivierungsschlüssel
108
Ausgabe liefert den Ausgabeaktivierungsschlüssel und die Versionsnummer an den Kartenlieferanten
110
Kartenlieferant erzeugt Sicherheitscode für die Karte
112
Sicherheitscode wird auf der Karte installiert
114
Festlegung des Ausgabeflags
116
Lieferung der Karte an die Ausgabe
fertig

FIG. 4


Aktivierungssicherheits-
anwendungsmodul
(ASAM)
208
Aktivierungssicherheitsanwendungs-
modulerzeugung
und
Aktivierungsicherheitsanwendungs-
modulwartung
204
Aktivierungs-
steuerungs-
computer
202
210
Haupt-
aktivie-
rungs-
schlüs-
sel
Be-
nutz-
er-
kenn-
wör-
ter
Aus-
gabe-
akti -
vie-
rungs-
schlüs-
sel
A
S
A
M
Ta-
bel-
le
Kontrollsicherheitsmodul
(CSAM)
206
200
212
214
216
218

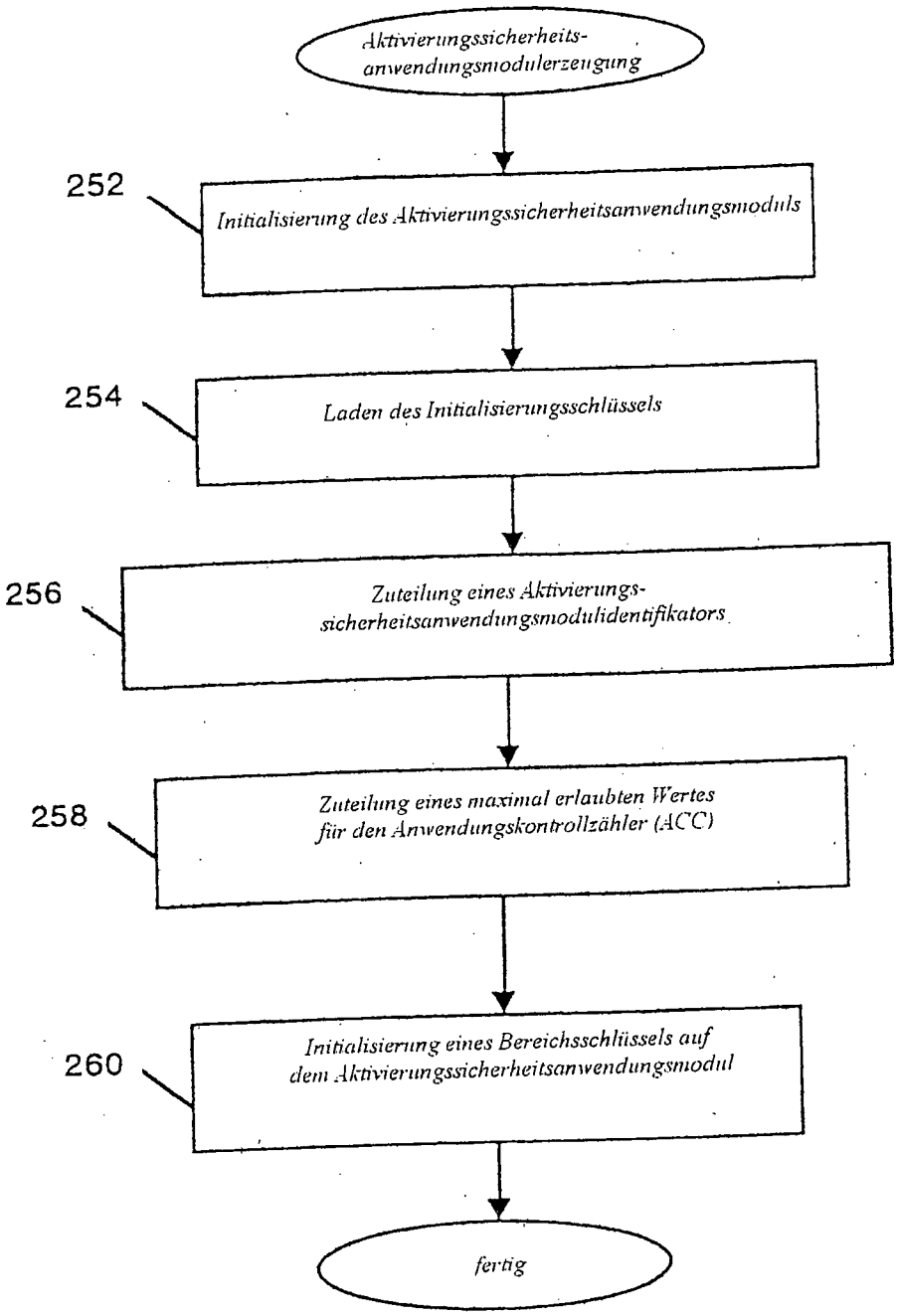

Aktivierungssicherheits-
anwendungsmodulerzeugung
252
Initialisierung des Aktivierungssicherheitsanwendungsmoduls
254
Laden des Initialisierungsschlüssels
256
Zuteilung eines Aktivierungs-
sicherheitsanwendungsmodulidentifikators
258
Zuteilung eines maximal erlaubten Wertes
für den Anwendungskontrollzähler (ACC)
260
Initialisierung eines Bereichsschlüssels auf
dem Aktivierungssicherheitsanwendungsmodul
fertig

FIG. 5

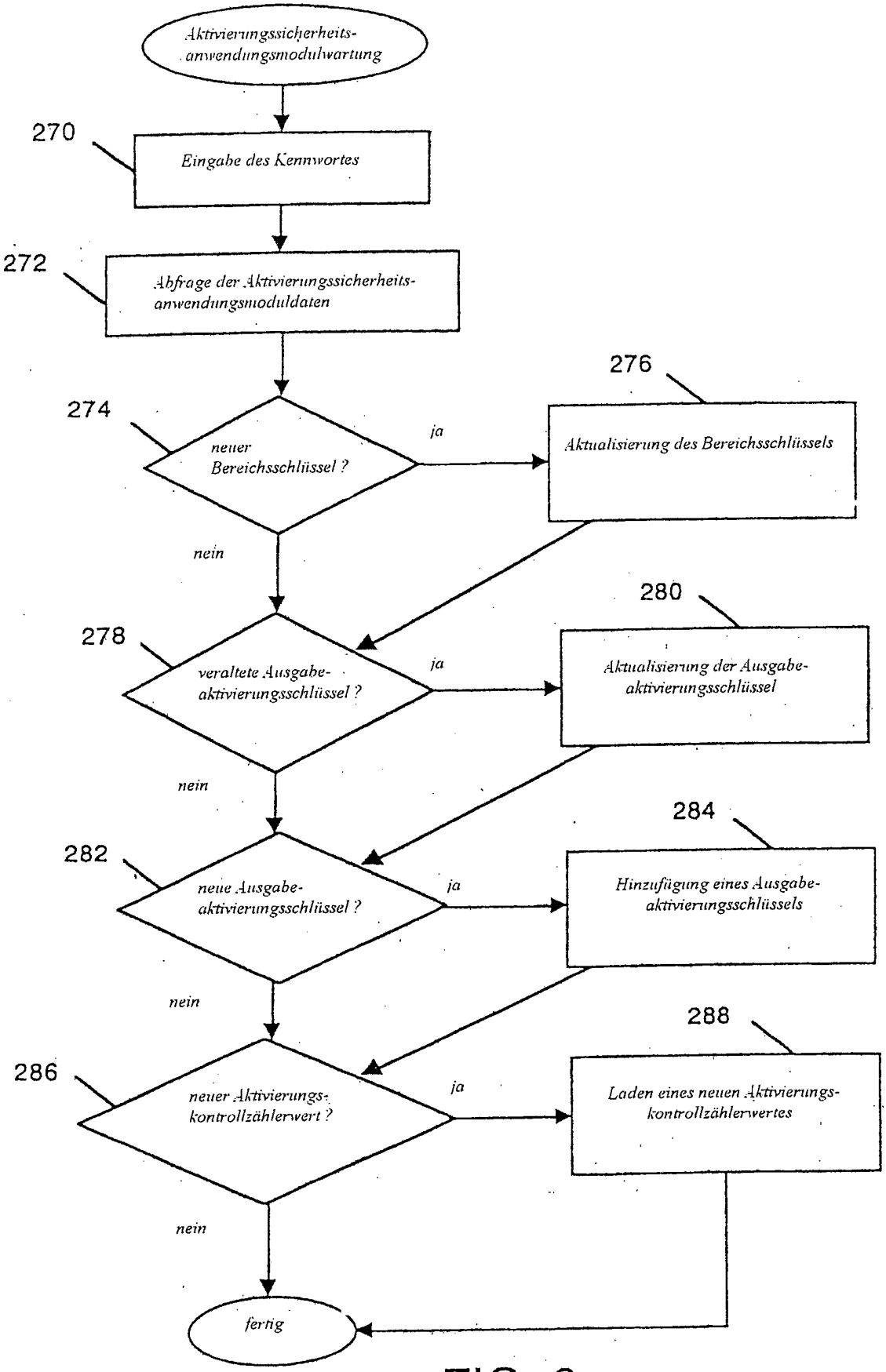

Aktivierungssicherheits-anwendungsmodulwartung
270
Eingabe des Kennwortes
272
Abfrage der Aktivierungssicherheits-anwendungsmoduldaten
274
neuer Bereichsschlüssel ?
ja
276
Aktualisierung des Bereichsschlüssels
nein
278
veraltete Ausgabe-aktivierungsschlüssel ?
ja
280
Aktualisierung der Ausgabe-aktivierungsschlüssel
nein
282
neue Ausgabe-aktivierungsschlüssel ?
ja
284
Hinzufügung eines Ausgabe-aktivierungsschlüssels
nein
286
neuer Aktivierungs-kontrollzählerwert ?
ja
288
Laden eines neuen Aktivierungs-kontrollzählerwertes
nein
fertig

FIG. 6

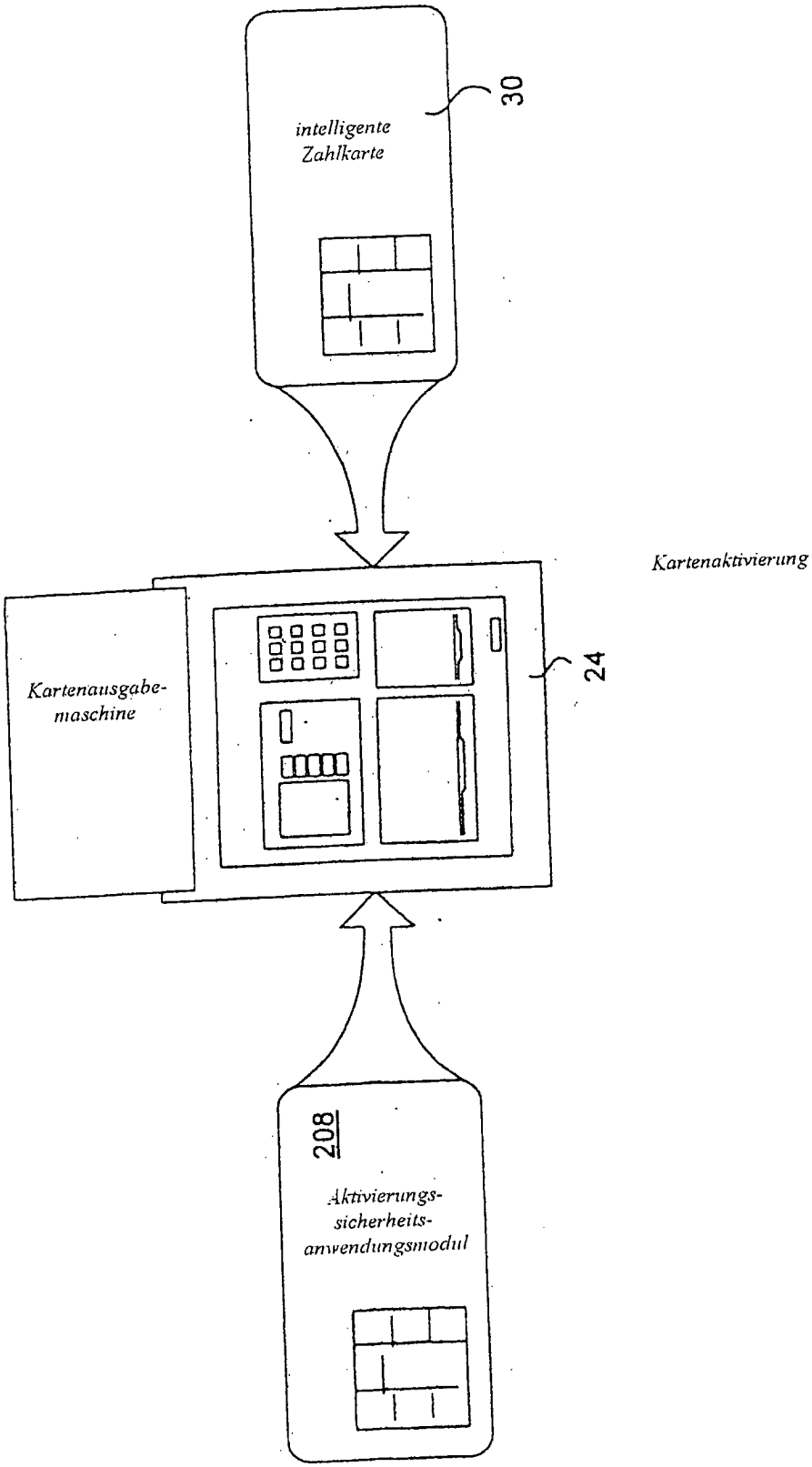

intelligente Zahlkarte
30
Kartenaktivierung
Kartenausgabe-maschine
24
208
Aktivierungs-sicherheits-anwendungsmodul

FIG. 7

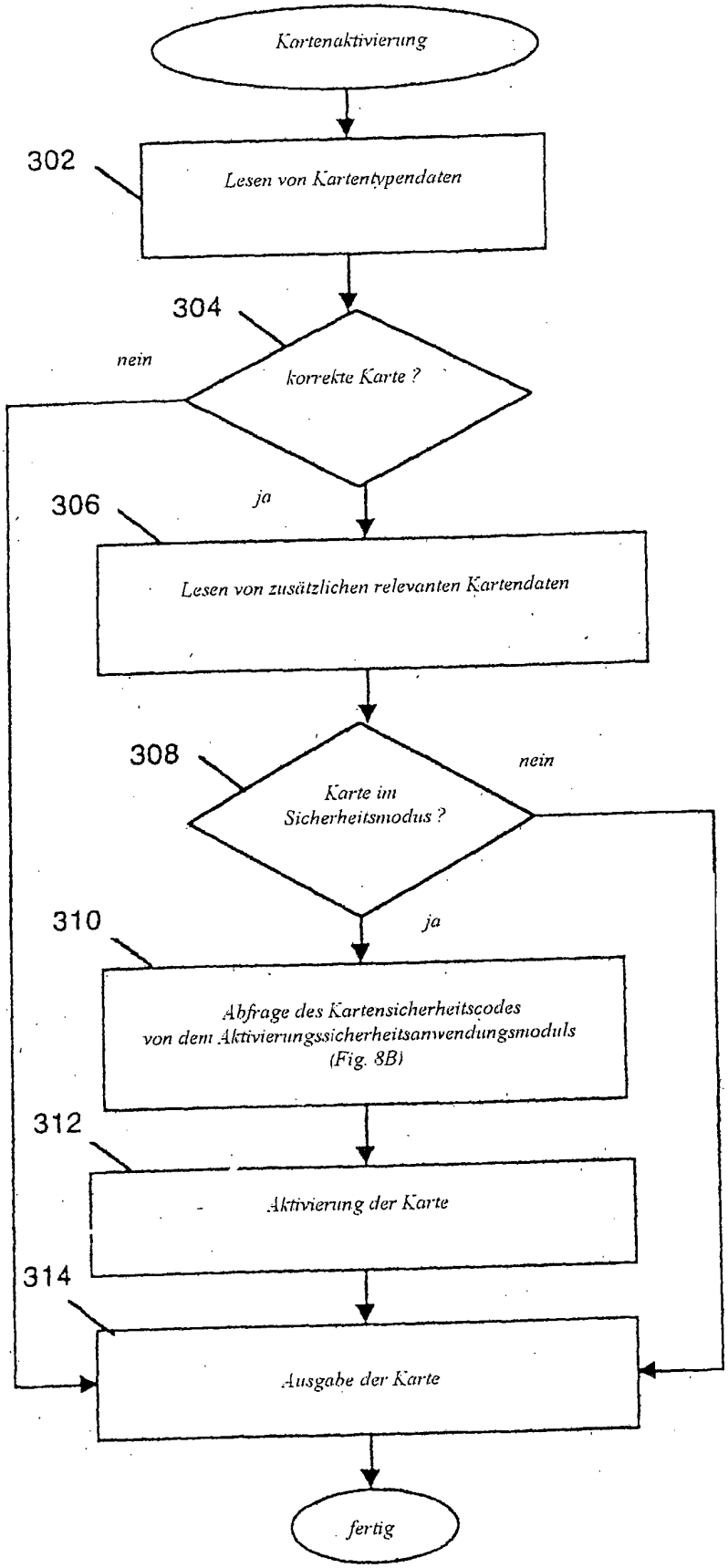

Kartenaktivierung
302
Lesen von Kartentypendaten
304
nein
korrekte Karte ?
ja
306
Lesen von zusätzlichen relevanten Kartendaten
308
nein
Karte im Sicherheitsmodus ?
ja
310
Abfrage des Kartensicherheitscodes von dem Aktivierungssicherheitsanwendungsmoduls (Fig. 8B)
312
Aktivierung der Karte
314
Ausgabe der Karte
fertig

FIG. 8A

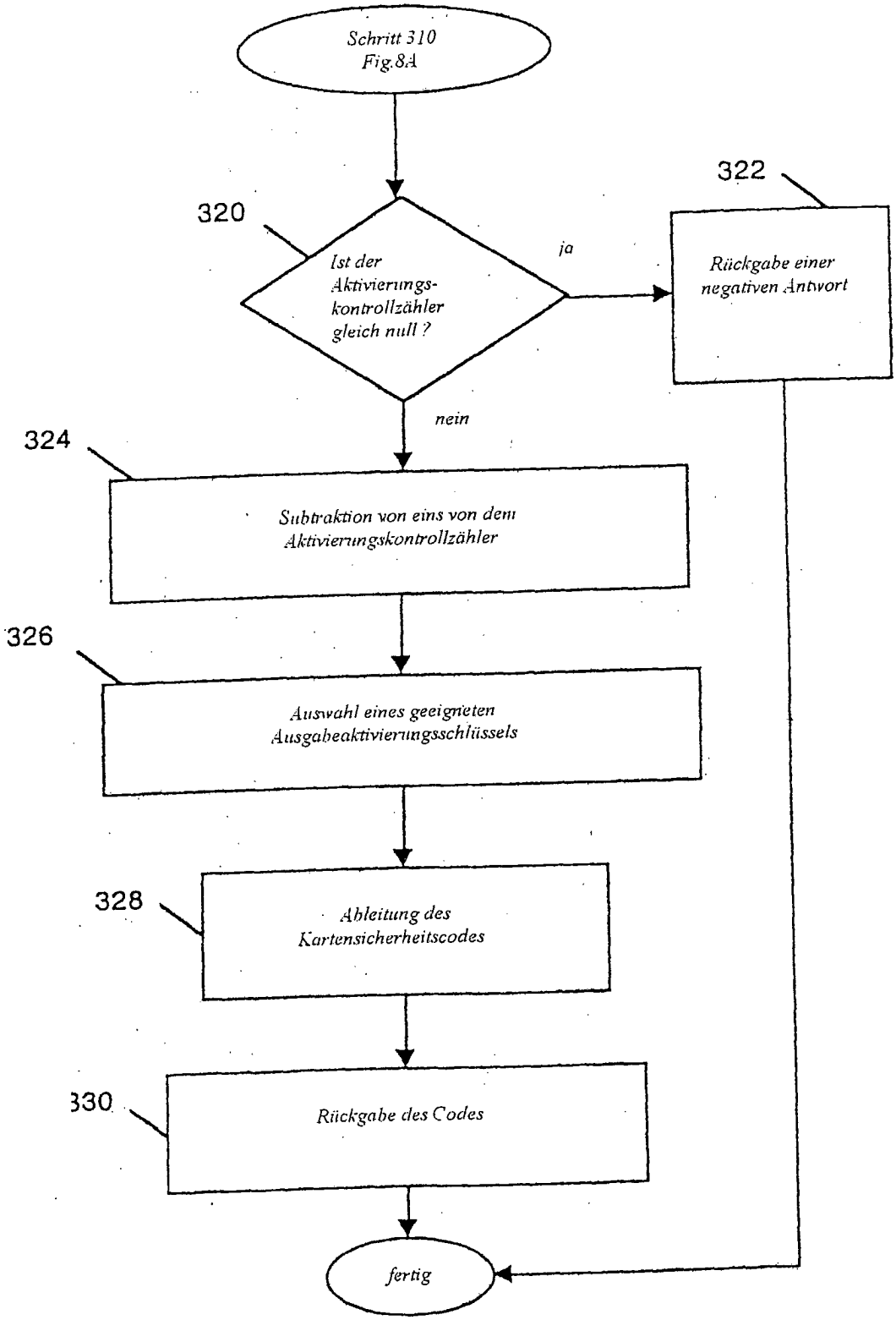

Schritt 310
Fig.8A
320
Ist der Aktivierungs-kontrollzähler gleich null ?
ja
322
Rückgabe einer negativen Antwort
nein
324
Subtraktion von eins von dem Aktivierungskontrollzähler
326
Auswahl eines geeigneten Ausgabeaktivierungsschlüssels
328
Ableitung des Kartensicherheitscodes
330
Rückgabe des Codes
fertig

FIG. 8B

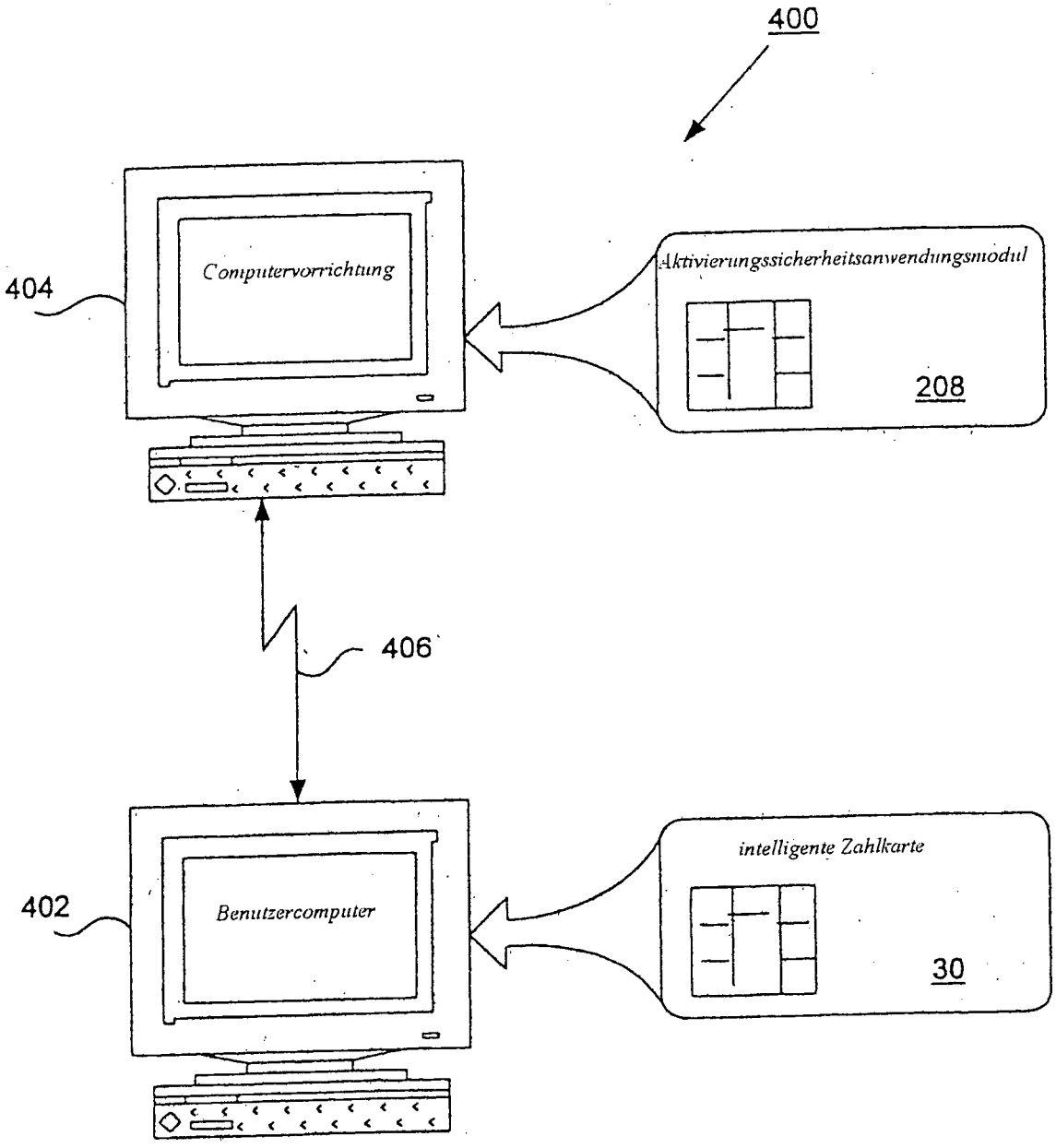

400
404
Computervorrichtung
Aktivierungssicherheitsanwendungsmodul
208
406
402
Benutzercomputer
intelligente Zahlkarte
30

FIG. 9

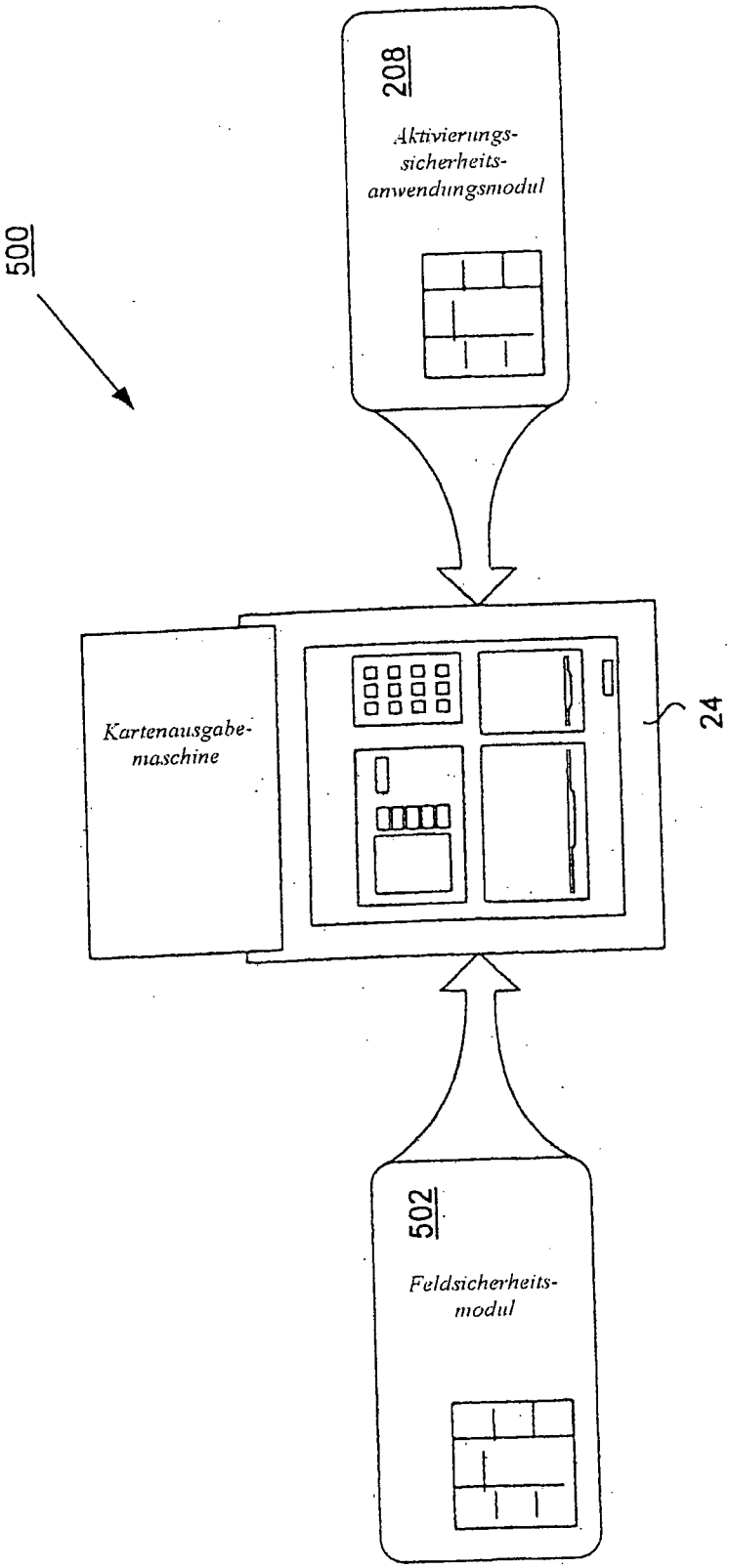

500
208
Aktivierungs-
sicherheits-
anwendungsmodul
Feldwartung des
Aktivierungssicherheits-
anwendungsmoduls
Kartenausgabe-
maschine
24
502
Feldsicherheits-
modul

FIG. 10

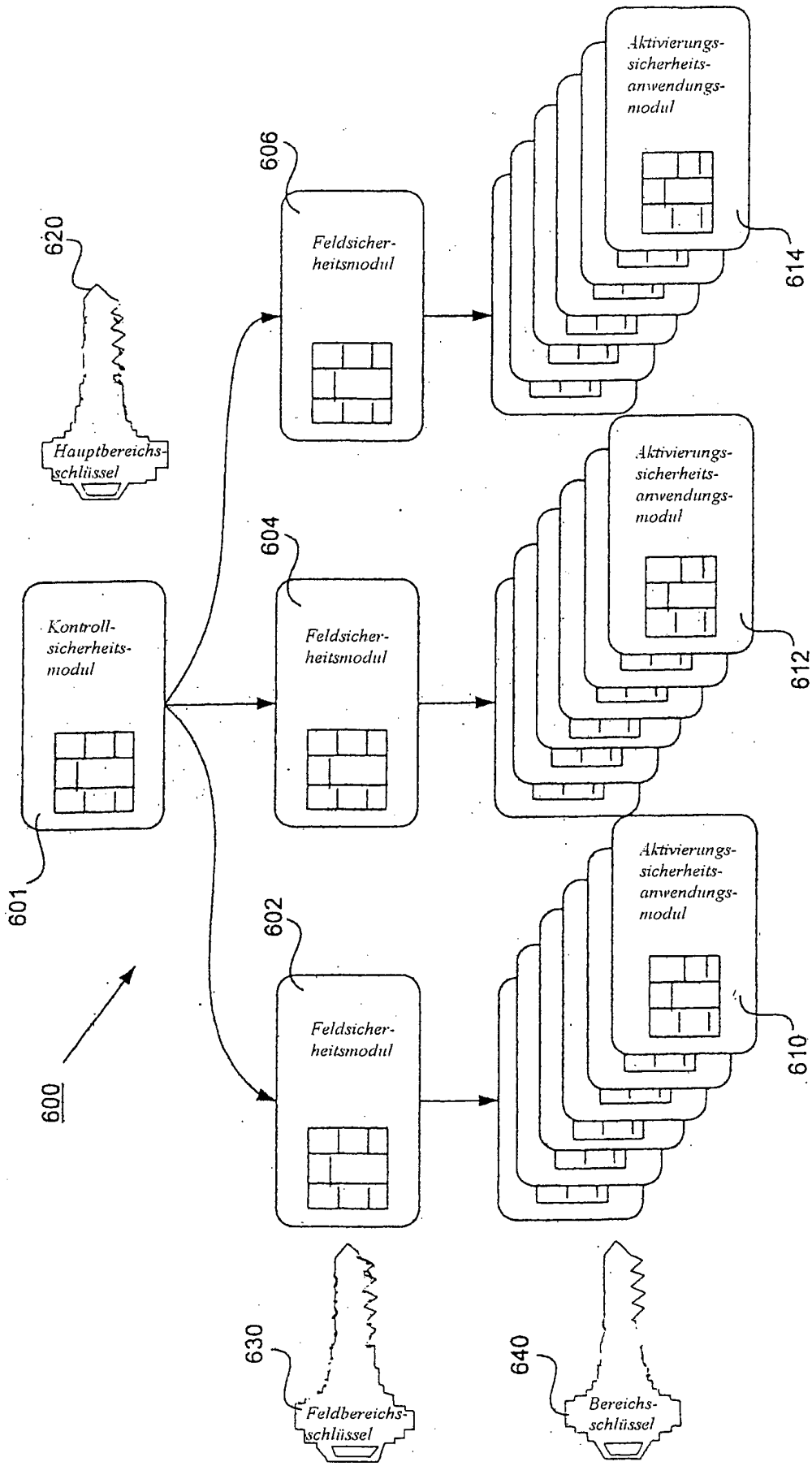

Aktivierungs-sicherheits-anwendungs-modul
606
Feldsicher-heitsmodul
620
614
Hauptbereichs-schlüssel
Aktivierungs-sicherheits-anwendungs-modul
Feldsicherheits-modulschlüssel-hierarchie
604
Kontroll-sicherheits-modul
Feldsicher-heitsmodul
612
601
Aktivierungs-sicherheits-anwendungs-modul
602
Feldsicher-heitsmodul
610
600
630
640
Feldbereichs-schlüssel
Bereichs-schlüssel

FIG. 11

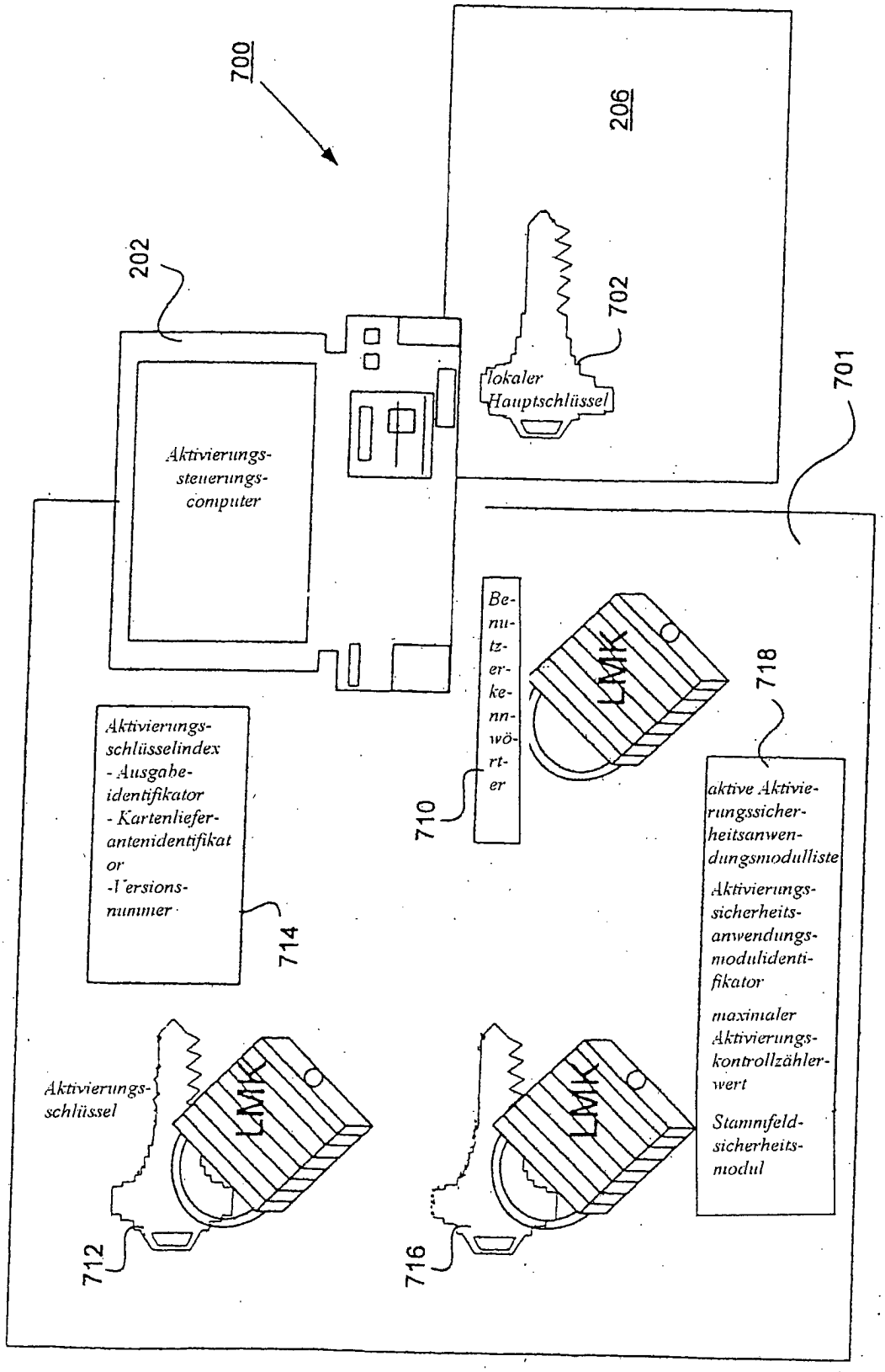

700
206
202
702
lokaler Hauptschlüssel
701
Aktivierungs-steuerungs-computer
Benutzerkennwörter
710
LMK
718
Aktivierungsschlüsselindex
- Ausgabeidentifikator
- Kartenlieferantenidentifikator
-Versionsnummer
714
aktive Aktivierungssicherheitsanwendungsmodulliste
Aktivierungssicherheitsanwendungsmodulidentifikator
maximaler Aktivierungskontrollzählerwert
Stammfeldsicherheitsmodul
Aktivierungsschlüssel
LMK
712
LMK
716

FIG. 12

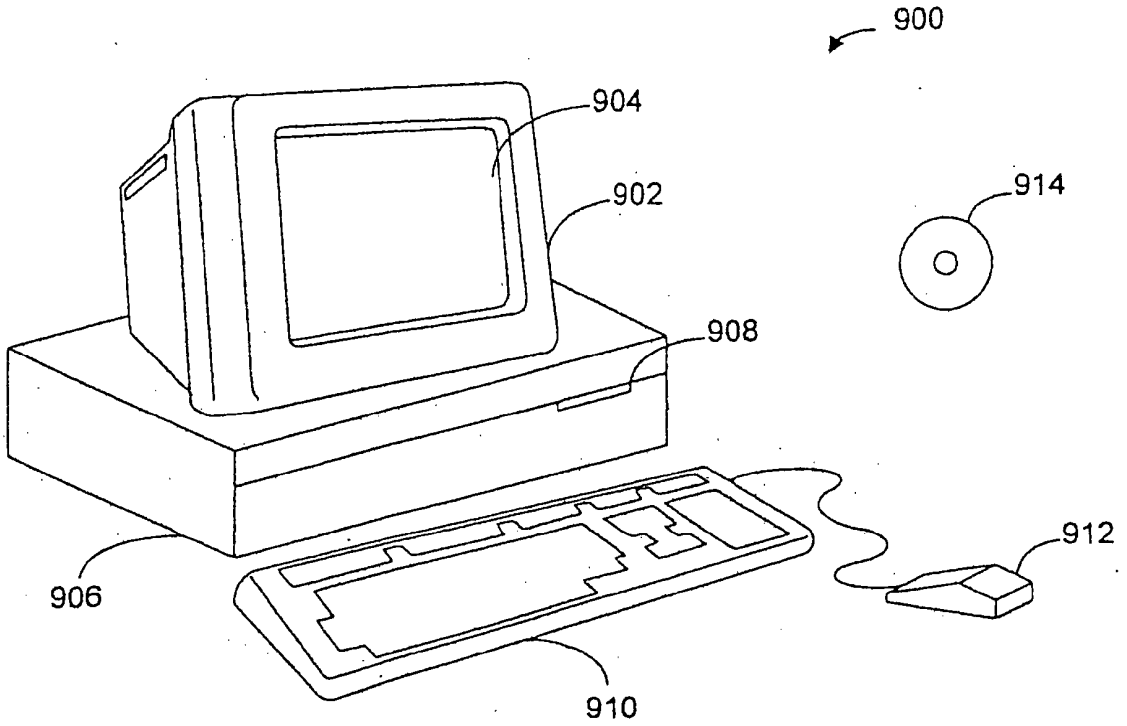

900
904
902
914
908
912
906
910

FIG. 13

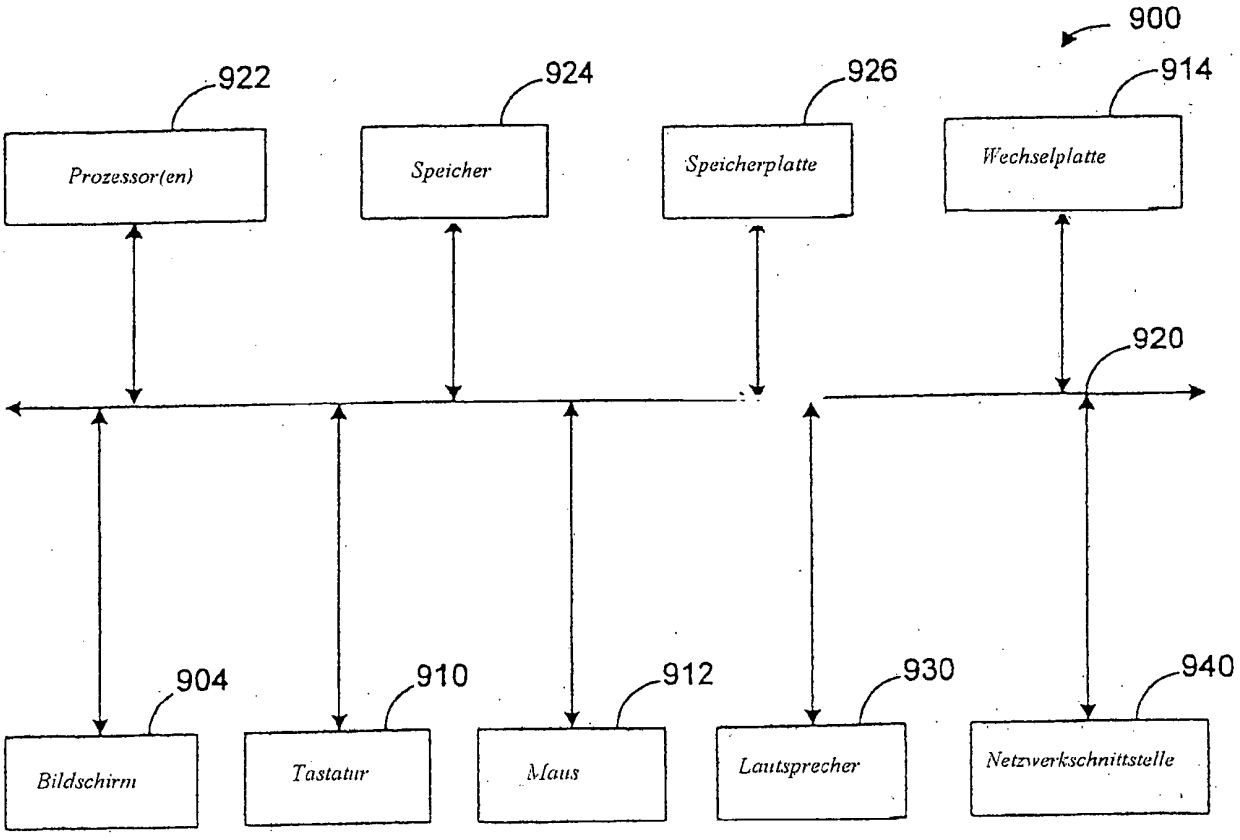

900
922
924
926
914
Prozessor(en)
Speicher
Speicherplatte
Wechselplatte
920
904
910
912
930
940
Bildschirm
Tastatur
Maus
Lautsprecher
Netzwerkschnittstelle

FIG. 14