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

(10) **DE 699 36 347 T2** 2008.02.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 097 589 B1**
(21) Deutsches Aktenzeichen: **699 36 347.0**
(86) PCT-Aktenzeichen: **PCT/US99/16188**
(96) Europäisches Aktenzeichen: **99 938 754.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/004717**
(86) PCT-Anmeldetag: **15.07.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **27.01.2000**
(97) Erstveröffentlichung durch das EPA: **09.05.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **20.06.2007**
(47) Veröffentlichungstag im Patentblatt: **28.02.2008**

(51) Int Cl.[8]: ***H04N 7/16*** (2006.01)

(30) Unionspriorität:
93223 P **17.07.1998** **US**

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

(73) Patentinhaber:
Thomson Licensing, Boulogne-Billancourt, FR

(74) Vertreter:
Roßmanith, M., Dipl.-Phys. Dr.rer.nat., Pat.-Anw., 30974 Wennigsen

(72) Erfinder:
ESKICIOGLU, Ahmet Mursit, Indianapolis, IN 46250, US; BEYERS, William Wesley, Carmel, IN 46032, US; HEREDIA, Edwin Arturo, Indianapolis, IN 46250, US; IZZAT, Izzat Hekmat, Carmel, IN 46033, US; NIJIM, Yousef Wasef, Indianapolis, IN 46250, US

(54) Bezeichnung: **SYSTEM MIT BEDINGTEM ZUGANG FÜR DIGITALEN FERNSEHRUNDFUNK**

Beschreibung

Gebiet der Erfindung

[0001] Diese Erfindung betrifft ein System, das verwendet werden kann, um Zugangsberechtigung zu mehreren Sendeanstalten durch eine einzelne Einrichtung für Unterhaltungselektronik bereitzustellen, wie beispielsweise ein Zusatzempfangsgerät (Set-Top-Box) oder ein digitales Fernsehgerät. Jede Einrichtung ist in der Lage, gesendete oder übertragene digitale Ströme von einer Vielfalt von Sendequellen zu empfangen.

Hintergrund der Erfindung

[0002] Heutige NTSC-Fernsehgeräte empfangen Rundfunkdienste von einer Vielfalt von Dienstleistern (siehe Fig. 1). Die meisten Fernsehempfänger **12** sind in der Lage, unverwürfelte Informationen oder Programme direkt von Rundfunk- **22**, Satelliten- **26** und Kabelnetzen **24** zu empfangen. Herkömmlicherweise erfordern Kabelnetze **24**, die verwürfelte oder verschlüsselte Programme bereitstellen, üblicherweise eine separate selbständige Einrichtung **16a** (z.B. ein Zusatzempfangsgerät), um das Programm zu entwürfeln oder zu entschlüsseln. Auf ähnliche Weise stellen digitale Satellitensysteme üblicherweise verwürfelte oder verschlüsselte Programme bereit, die auch die Verwendung eines separaten Zusatzempfangsgeräts **16b** erfordern. Diese Zusatzempfangsgeräte können eine entfernbare intelligente Karte **18a**, **18b** verwenden, welche die notwendigen Entschlüsselungsalgorithmen und Schlüssel enthält. Die Dokumente EP-A-0 626 793 und „Functional model of a conditional access system", EBU Review Technical, Nr. 266, 21.12.1995, Seiten 64 bis 77, XP 000 55 94 50, ISSN 0251-0936, offenbaren Zugangsberechtigungssysteme mit intelligenten Karten. Typischerweise ist ein separates Zusatzempfangsgerät für jeden Dienstleister erforderlich.

[0003] In naher Zukunft können digitale Fernsehrundfunkdienste **5** bis **20** lokale Kanäle umfassen, von denen jeder bis zu 10 gleichzeitige Programme senden kann, wobei einige dieser Programme Programme mit Bezahlung pro Sendung sind. Es kann sein, dass ein Benutzer eine Mischung von Diensten von zahlreichen verschiedenen Dienstleistern haben möchte. Zum Beispiel könnte ein Benutzer alle Basketballspiele der Universität Indiana von dem lokalen Kanal **4** kaufen wollen und alle Notre Dame Football-Spiele von Kanal **13** kaufen und alle Indianapolis Colts Spiele von Kanal **8** kaufen. Wenn jeder dieser Dienste einzigartig verwürfelt wäre, müsste der Benutzer es auf sich nehmen, mehrere intelligente Karten für Zugangsberechtigung zu kaufen und die Karten auszutauschen, sobald der Benutzer durch die Kanäle surft.

Zusammenfassung der Erfindung

[0004] Die vorliegende Erfindung besteht teilweise aus der Erkenntnis des beschriebenen Problems und teilweise daraus, eine Lösung für das Problem bereitzustellen. Ein einzelnes Zugangsberechtigungssystem wird bereitgestellt, das in der Lage ist, mit einer Vielzahl von Dienstleistern verwendet zu werden, ohne Sicherheitsmodule zu wechseln. Solch ein globales Zugangsberechtigungssystem wendet das Konzept automatischer Belastung eines Benutzerkontos an, wenn ein Programm gekauft wird, versus Protokollieren von allen Käufen und Übertragen des Protokolls an den Dienstleister zur Abrechnung. Um die gewünschte Flexibilität zu erreichen, wendet das System einen globalen öffentlichen Schlüssel an, der von allen Dienstleistern verwendet wird; dies ist der öffentliche Schlüssel für jede intelligente Karte. Der entsprechende private Schlüssel wird in die intelligente Karte geladen. Es liegt wohl in den Lehren dieser Anmeldung, dass mehr als ein öffentliches/privates Schlüsselpaar verwendet werden kann, um die Auswirkung bei einem Sicherheitseinbruch zu minimieren.

[0005] Ein Ereignis oder Programm, wie es hier beschrieben ist, umfasst eins von dem Folgenden: (1) audio/visuelle Daten wie beispielsweise einen Spielfilm, eine wöchentliche „Fernsehshow" oder eine Dokumentarsendung; (2) Textdaten wie beispielsweise ein elektronisches Magazin, Zeitung oder Wetterberichte; (3) Computersoftware; (4) binäre Daten wie beispielsweise Bilder oder (5) HTML-Daten (z.B. Webseiten). Die Dienstleister umfassen jeden Anbieter, der Ereignisse sendet, zum Beispiel, herkömmliche Fernsehrundfunknetze, Kabelnetze, digitale Satellitennetze, Anbieter einer elektronischen Auflistung von Ereignissen wie beispielsweise Anbieter eines elektronischen Programmführers und in bestimmten Fällen Internetdiensteanbieter.

[0006] Solch ein System kann auf einer Technologie mit öffentlichem Schlüssel basieren. Ein einziger öffentlicher Schlüssel (Nummer) ist für alle Dienstleister verfügbar. Dies ist der öffentliche Schlüssel für jede intelligente Karte. In jeder intelligenten Karte ist ein geheimer privater Schlüssel gespeichert, der Mitteilungen entschlüsseln kann, die durch den öffentlichen Schlüssel verschlüsselt sind. Der Dienstleister sendet eine CA-Berechtigungsmitteilung in dem Übertragungsstrom, der durch den öffentlichen Schlüssel verschlüsselt ist, wel-

che den Namen des Dienstleisters, den Namen, die Zeit und die Kosten des Programms und den Schlüssel enthält, um die Schlüssel zu entschlüsseln, die zum Verwürfeln des Programms verwendet werden. Diese Mitteilung wird durch die intelligente Karte entschlüsselt und die passenden Informationen werden in der intelligenten Karte für jedes gekaufte Ereignis gespeichert. Die intelligente Karte weist einen bestimmten Betrag an Guthaben für Einkäufe auf, der durch die Bank freigegeben worden ist. Solange wie das Limit nicht überschritten wird, können von dem Zuschauer Programme gekauft werden. Zu irgendeiner passenden voreingestellten Zeit verlangt die intelligente Karte einen Telefonanruf zu der CA-Zentrale. Unter Verwendung eines anderen Satzes von öffentlichen und privaten Schlüsseln empfängt die CA-Zentrale, in Zusammenarbeit mit einer Bank, Abrechnungsinformationen von der intelligenten Karte und stellt zusätzliches Guthaben bereit. Die Bank sendet die Informationen und Gutschriften an den entsprechenden Dienstleister.

[0007] Im Allgemeinen definiert die vorliegende Erfindung ein Verfahren zum Bereitstellen von Zugangsberechtigung zu einem eingeschränkten gesendeten oder übertragenen Ereignis. Zuerst werden verschlüsselte Zugangsinformationen empfangen, die dem gesendeten Ereignis zugeordnet sind. Als Nächstes werden die Zugangsinformationen entschlüsselt (oder entwürfelt) und die Kosten für das gesendete Ereignis überprüft, um zu entscheiden, ob sie weniger betragen als eine vorgespeicherte Bargeldreserve. Dann wird das verwürfelte gesendete Ereignis von dem Dienstleister empfangen und es wird entwürfelt.

[0008] Gemäß einem Aspekt der vorliegenden Erfindung umfasst das Verfahren zum Verwalten des Zugangs zu einem eingeschränkten gesendeten oder übertragenen Ereignis von einem einzigen von einer Vielzahl von Dienstleistern das Empfangen einer Vielzahl von Zugangsinformationsmitteilungen, die dem übertragenen Ereignis zugeordnet sind. Wobei jede der Zugangsinformationsmitteilungen unter Verwendung eines verschiedenen öffentlichen Schlüssels verwürfelt ist und Daten umfasst, die den Kosten des übertragenen Ereignisses entsprechen. Danach das Entschlüsseln oder Entwürfeln von einer einzigen der Zugangsinformationsmitteilungen unter Verwendung des vorgespeicherten privaten Schlüssels, der dem Dienstleister zugeordnet ist, und das Überprüfen, dass die Kosten des übertragenen Ereignisses weniger betragen als eine vorgespeicherte Bargeldreserve. Schließlich das Empfangen des verwürfelten übertragenen Ereignisses von einem einzigen der Dienstleister und das Entwürfeln des übertragenen Ereignisses unter Verwendung des Entwürfelungsschlüssels.

[0009] Gemäß einem anderen Aspekt der vorliegenden Erfindung umfasst das Verfahren zum Verwalten des Zugangs zu einem eingeschränkten übertragenen Paket von Ereignissen das Empfangen, über einen direkten Kanal, von digital signierten Zugangsinformationen, die dem Paket von Ereignissen zugeordnet sind und Daten umfassen, die den Kosten des Paketes von Ereignissen entsprechen. Die Signatur auf den Zugangsinformationen wird unter Verwendung eines öffentlichen Schlüssels überprüft; die Kosten des Paketes werden nachgeprüft, um sicherzustellen, dass sie weniger als eine vorgespeicherte Bargeldreserve betragen. Wenn irgendeines der verwürfelten gesendeten Ereignisse, das zu dem Paket gehört, von dem Dienstleister empfangen wird, werden seine Zugangsinformationen entschlüsselt, um den Entwürfelungssschlüssel zu erhalten.

[0010] Gemäß noch einem anderen Aspekt der vorliegenden Erfindung umfasst das Verfahren zum Verwalten des Zugangs zu einem eingeschränkten übertragenen Ereignis das Transferieren, von einer Bank, einer Bargeldreserve auf eine intelligente Karte; das Empfangen eines verschlüsselten Ereignisschlüssels und der Kosten des Ereignisses von einem Dienstleister; das Weiterreichen des Ereignisschlüssels und der Kaufinformationen an die intelligente Karte, welche mit dem digitalen Videogerät gekoppelt ist. Als Nächstes werden die Kosten des Ereignisses überprüft, um zu bestimmen, dass sie weniger als die gespeicherte Bargeldreserve betragen und die Kosten werden einbehalten. Der verschlüsselte Ereignisschlüssel wird entschlüsselt und das verwürfelte Ereignis wird empfangen und danach an die intelligente Karte weitergereicht, wo es unter Verwendung des entschlüsselten Ereignisschlüssels entwürfelt wird. Schließlich wird das entwürfelte Ereignis an das digitale Videogerät transferiert.

[0011] Diese und andere Aspekte der Erfindung werden unter Bezugnahme auf eine bevorzugte Ausführungsform der Erfindung erläutert, die in den beigefügten Zeichnungen gezeigt ist.

Kurze Beschreibung der Zeichnung

[0012] Fig. 1 ist ein Blockdiagramm, das eine Konfiguration vom Stand der Technik zum Zusammenschalten von Einrichtungen für Unterhaltungselektronik mit einer Vielfalt von Dienstleistern darstellt.

[0013] Fig. 2 ist ein Blockdiagramm, das eine Architektur zum Bilden einer Schnittstelle zwischen einem allgemeinen digitalen Fernsehgerät und einer Vielzahl von terrestrischen Sendeanstalten darstellt; und

[0014] Fig. 3 ist ein Blockdiagramm einer beispielhaften Implementierung eines Systems zum Verwalten des Zugangs zu einer Einrichtung gemäß der Erfindung.

Ausführliche Beschreibung der Zeichnung

[0015] Die vorliegende Erfindung stellt ein Zugangsberechtigungssystem bereit, welches verwendet werden kann, um Dienste von einer einzigen von einer Vielzahl von Quellen zu erhalten. Wenn das Zugangsberechtigungssystem in einem digitalen Fernsehgerät (DTV) oder einem Zusatzempfangsgerät oder dergleichen implementiert ist, ermöglicht es einem Benutzer, von mehr als einem einzigen Dienstleister verwürfelte Ereignisse zu empfangen, ohne die Zugangsberechtigungsmodule oder intelligenten Karten auszutauschen. Als Alternative kann die Funktionalität der intelligenten Karte innerhalb des DTV eingebettet sein. Solch ein Zugangsberechtigungssystem kann als eine Gebührenbrücke für den Zugang zu Diensten agieren, wodurch für den Hersteller des DTV ein Mechanismus ermöglicht wird, auf der Grundlage der Nutzung seines DTV Gebühren zu kassieren. Auf ähnliche Weise kann diese Erfindung in einem Zusatzempfangsgerät (STB, Set-Top-Box) implementiert sein; zur Vereinfachung richtet sich die nachstehende Beschreibung der Erfindung auf eine Implementierung unter Verwendung eines digitalen Fernsehgeräts und einer damit gekoppelten intelligenten Karte.

[0016] In Fig. 2 veranschaulicht das System **30** die allgemeine Architektur für das Verwalten von Zugang zu einem digitalen Fernsehgerät (DTV) **40a**, **40b**. Zur Vereinfachung ist die nachfolgende Beschreibung auf ein einzelnes DTV **40A** beschränkt. Ähnliche Elementzahlen definieren dasselbe Funktionselement. Die intelligente Karte (SC) **42a** ist in ein (nicht gezeigtes) Kartenlesegerät von DTV **40a** eingesteckt oder damit gekoppelt; der Bus **45** verbindet DTV **40a** und SC **42a** miteinander, wodurch der Transfer von Daten zwischen ihnen ermöglicht wird. Solche intelligenten Karten umfassen zum Beispiel ISO 7816 Karten, die dem National Renewable Security Standard (NRSS) Teil A entsprechen, oder PCMCIA-Karten, die dem NRSS Teil B entsprechen. Dieses erfindungsgemäße Konzept ist nicht auf intelligente Karten an sich beschränkt, sondern kann auch bei Zugangsberechtigungsmodulen eingesetzt werden. Wenn solch eine intelligente Karte mit einem Lesegerät für intelligente Karten gekoppelt wird, kann, in konzeptioneller Hinsicht, die Funktionalität der intelligenten Karte als Bestandteil der Funktionalität des digitalen Fernsehgeräts betrachtet werden, wodurch die „Grenzen" aufgehoben werden, die durch den physischen Kartenkörper der intelligenten Karte geschaffen werden.

[0017] DTV **40a** kann Dienste von einer Vielzahl von Dienstleistern (SP) empfangen, wie beispielsweise Rundfunkfernseh-SP **50** und **52**, einem Kabelfernsehen (nicht gezeigt), und einem Satellitensystem (nicht gezeigt). Diese Erfindung ist vorteilhaft bei terrestrischem Senden. Zertifikatsautorität (CA) **75** ist mit keinem, weder den Dienstleistern noch dem DTV **40a**, direkt verbunden, aber gibt digitale Zertifikate und öffentliche und private Schlüsselpaare aus, welche, wie nachstehend erläutert, verwendet werden. Es liegt in dem Umfang dieser Erfindung, dass die Rolle der Zertifikatsautorität **75** in Zusammenarbeit mit dem Hersteller des DTV **40a** durch die Dienstleister dargestellt werden kann. Die Abrechnungszentrale **70** wird verwendet, um die Benutzerkonten zu verwalten; aktualisierte Informationen werden bereitgestellt, sobald die Benutzer Vorkehrungen treffen, zusätzliche Dienste zu kaufen, und sobald diese Dienste verbraucht oder verwendet werden.

[0018] Solch ein Zugangsberechtigungssystem (CA), das für DTV-Rundfunktechnologie entworfen ist, ist ein transportbasiertes System. Dies bedeutet, dass CA-Informationen für eine bestimmte Sendeanstalt nur auf ihrem eigenen RF-Kanal übertragen werden. Jede Sendeanstalt ist für ihre eigenen Informationen verantwortlich und somit besteht keine Notwendigkeit für einen zuvor eingeführten Verhaltenskodex, um Informationen unter mehreren Sendeanstalten zu koordinieren und/oder zu synchronisieren. Ferner basiert das CA-System auf dem Laden von elektronischem Bargeld auf Karten. Ein(e) Benutzer(in) lädt seine(ihre) Karte mit einem gewissen Bargeldbetrag auf (von Debit- oder Kreditkonten), und verwendet die Karte danach, um Ereignispakete zu kaufen, monatliche Abonnements zu bezahlen oder spezielle Programme mit sendungsweisem Bezahlungsmodus zu kaufen. Ein Ereignispaket kann zum Beispiel alle Spiele Ihrer bevorzugten professionellen Sportfranchise oder alle Spielfilme am späten Sonntag auf einem einzigen oder mehreren virtuellen Kanälen umfassen.

[0019] Der Rundfunkkanal wird nur verwendet, um die Dienste und Informationen für den Zugang zu diesen Diensten zu liefern. Alle übrigen Transaktionen werden unter Verwendung eines Rückkanals ausgeführt (d.h. ein Modem und eine Telefonverbindung). Das Senden von adressierbaren Mitteilungen ist nicht notwendig. Die Rundfunkdienste sind durch die Verwendung eines allgemeinen Verwürfelungsalgorithmus geschützt. Die Schlüssel, die bei diesem Vorgang und Ereigniskaufinformationen verwendet werden, werden mit einem globalen öffentlichen Schlüssel verschlüsselt und werden dem Benutzer über den MPEG-2 Strom geliefert. Bei Ereignispaketen werden dem Benutzer Paketzertifikate von dem CA-Server **60a** über den Rückkanal gesen-

det. Wie nachstehend ausführlicher beschrieben, werden Zertifikate üblicherweise signiert, um die Unversehrtheit des Zertifikats sicherzustellen. Das heißt, um sicherzustellen, dass das richtige und unveränderte Zertifikat von dem Sender empfangen wird. Durch ein erneuerbares Sicherheitsmodul, d.h. und eine intelligente Karte, wird auf Dienste zugegriffen.

[0020] Symmetrische Schlüsselkryptografie beinhaltet die Verwendung desselben Algorithmus und Schlüssels für sowohl die Verschlüsselung als auch die Entschlüsselung. Die Basis öffentlicher Schlüsselkryptografie liegt in der Verwendung von zwei zusammengehörenden Schlüsseln, einem öffentlichen und einem privaten. Der private Schlüssel ist ein geheimer Schlüssel und es ist rechnerisch nicht machbar, den privaten Schlüssel von dem öffentlichen Schlüssel, welcher öffentlich verfügbar ist, abzuleiten. Jeder mit einem öffentlichen Schlüssel kann eine Mitteilung verschlüsseln, aber nur die Person oder Einrichtung, die den zugeordneten und vorbestimmten privaten Schlüssel hat, kann sie entschlüsseln. Auf ähnliche Weise kann eine Mitteilung durch einen privaten Schlüssel verschlüsselt werden und jeder mit Zugang zu dem öffentlichen Schlüssel kann diese Mitteilung entschlüsseln. Verschlüsselungsmitteilungen, bei denen ein privater Schlüssel verwendet wird, können als „Signieren" bezeichnet werden, da jeder, der den öffentlichen Schlüssel besitzt, überprüfen kann, dass die Mitteilung durch die Partei gesendet wurde, die den privaten Schlüssel hat. Dies kann man sich so wie das Überprüfen einer Signatur auf einem Dokument vorstellen.

[0021] Eine digital signierte Mitteilung besteht aus einer im Klartext (d.h. unverschlüsselten) gesendeten Mitteilung, an welche die Signatur angehängt ist. Die angehängte Signatur wird durch Verschlüsseln von entweder der Mitteilung selbst oder einer Zusammenfassung der Mitteilung produziert; wobei eine Zusammenfassung der Mitteilung durch Hash-Kodieren der Mitteilung erhalten wird. (Hash-Kodieren beinhaltet, dass die Mitteilung, vor dem Verschlüsseln der Mitteilung, einem Einweg-Hash-Algorithmus unterzogen wird, wie beispielsweise dem von Ron Rivest entwickelten MD5 oder dem von dem National Institute of Standards and Technology (NIST) und der National Security Agency (NSA) entwickelten SHA-1.) Infolgedessen kann der Empfänger der signierten Mitteilung die Unversehrtheit (d.h. die Quelle oder den Ursprung) der Mitteilung überprüfen. (Im Vergleich dazu besteht ein öffentliches Schlüsselzertifikat oder digitales Zertifikat aus einer Mitteilung, die einen öffentlichen Schlüssel beinhaltet, die im Klartext gesendet wird, an welche eine Signatur angehängt ist.) Signaturüberprüfung beinhaltet das Nachprüfen der Signatur durch Entschlüsselung.

[0022] Wie vorstehend definiert, sind die fünf Hauptkomponenten des CA-Systems, die Sendeanstalt, der CA-Lieferant, die Abrechnungszentrale (z.B. eine Bank), der Endbenutzer und die Zertifikatsautorität. **Fig. 2** stellt die gesamte Systemarchitektur dar und identifiziert diese fünf Komponenten mit ihren Kommunikationsverbindungen und Datenflüssen.

[0023] Der Endbenutzer kommuniziert mit dem CA-Lieferanten wegen des Herunterladens von Zertifikaten durch eine Punkt-zu-Punkt-Verbindung wie beispielsweise eine Telefonleitung. Die Telefonleitung wird, falls erforderlich, für automatische Transaktionen und für Sprachverbindung verwendet. Ein Freigabeprotokoll für automatische Transaktionen ist das Punkt-zu-Punkt-Protokoll (PPP). Sicherheit wird auf der Anwendungsschicht unter Verwendung privater Protokolle implementiert.

[0024] Kommunikation zwischen dem CA-Lieferanten und der Sendeanstalt kann durch ein lokales Netz (LAN) oder Weitverkehrsnetz (WAN) erstellt werden. Wie schon zuvor, ist Sicherheit in der Anwendungsebene unter Verwendung privat definierter Protokolle eingebettet, die über bestehende Netzübergangsprotokolle laufen. Die Sendeanlagenausrüstung, die benötigt wird, um die gesendeten Ströme zu schützen, kann aus einem Fertigprodukt bestehen, das von mehreren CA-Lieferanten erhältlich ist.

[0025] Sendeanstalten sind verantwortlich für das Liefern von: (1) den Diensten, und (2) den Berechtigungsmitteilungen. Solche Berechtigungsmitteilungen umfassen Zugangsinformationsmitteilungen (AIM), die nachstehend ausführlicher beschrieben werden, (oder alternativ Berechtigungssteuerungsmitteilungen und Berechtigungsverwaltungsmitteilungen), die jedem Benutzer erlauben, diese Dienste zu kaufen. Die Kommunikation zwischen einer Sendeanstalt und dem Benutzer folgt daher dem Punkt-zu-Mehrpunkt-Modell der Rundfunktechnologie. Gesendete AIM enthalten keine Adressen, die einzigartig für jeden Benutzer oder Abonnenten sind, was für Satelliten- oder Kabelsysteme typisch ist.

[0026] Wenn DTV **40a** keine Rückwärtskanalverbindung aufweist, die zum Kommunizieren mit dem CA-Server benötigt wird, dann erfordert das Laden von Bargeld auf die Karte, dass der Benutzer entweder auf eine DTV-Einheit mit Rückwärtskanalunterstützung zugreift, oder zu einer bestimmten Stelle geht (Bank, Geldautomat, Regionalbüro des Lieferanten), um die Karte aufladen zu lassen. Das CA-Bedienungspersonal fungiert als die Bank des Karteninhabers oder des Benutzers, während die Abrechnungszentrale als die Bank des

Händlers fungiert. Die Kartengesellschaft könnte der Vermittler zwischen dem CA-Bedienungspersonal und den Banken der Sendeanstalten sein, die einen Transaktionsverrechnungsdienst bereitstellen. Der feste Betrag an „Bargeld", der in die intelligente Karte oder das Zugangsberechtigungsmodul geladen wird, kann nun verwendet werden, um Dienste zu bezahlen, die durch eine Sendeanstalt angeboten werden.

[0027] Welcher Mechanismus für Bargeldtransfer auch angewendet wird, der Benutzer verlangt einen Transfer eines spezifischen Geldbetrags von einem Kredit- oder Debitkonto auf die CA-Karte. Nach der ordnungsgemäßen Überprüfung der Identität des Individuums und Berechnung von Benutzermitteln, wird die Transaktion autorisiert, und der nominale Geldbetrag wird in der CA-Karte gespeichert.

[0028] Sobald das Geld in die Karte geladen ist, kann ein Benutzer jede Anzahl von Diensten kaufen, die durch Sendeanstalten angeboten werden. Jeder Kauf reduziert den Betrag an verfügbarem Geld in der Karte um den Preis des Dienstes. Die durch die Sendeanstalten angebotenen Dienste können in zwei Kategorien unterteilt werden, Ereignisse mit sendungsweiser Bezahlung (PPV) und Pakete. Ein Ereignis besteht aus einem TV-Programm mit einem zugewiesenen Zeitschlitz in einem Programmführer und ein Paket besteht einfach aus einer Sammlung von Ereignissen. Beispiele für Pakete sind (1) alle NBA-Spiele in einer gegebenen Saison, (2) die Spielfilme am späten Sonntag auf einem einzigen oder mehreren virtuellen Kanälen, (3) Abonnement eines bestimmten virtuellen Kanals wie beispielsweise HBO. Alle Ereignisse müssen einen einzigen oder mehrere ihrer audiovisuellen Ströme unter Verwendung eines allgemeinen symmetrischen Schlüsselalgorithums verwürfeln. Berechtigungspakete, welche Kaufinformationen und Entwürfelungsschlüssel enthalten, müssen mit einem allgemeinen öffentlichen Schlüsselalgorithmus verschlüsselt werden.

[0029] Nach dem Kauf eines Ereignisses kann ein Eintrag in der intelligenten Karte gespeichert werden, der später an den CA-Lieferanten transferiert werden kann. Sobald die gespeicherten Kaufinformationen an die CA-Datenbank gesendet sind, kann ein CA-Lieferant Sendeanstalten für die erbrachten Dienste bezahlen. Darüber hinaus verfügt jede intelligente Karte über einen nichtflüchtigen Speicher, um die folgenden Informationen zu behalten.

[0030] Ein 32-Bit-Feld stellt die Kartenseriennummer dar. Ein 128-Bit BCD-Feld für die (Kredit- oder Debit-) Kartennummer des Benutzers. Ein 10-Byte-Feld für die Telefonnummer des CA-Servers. Ein 10-Byte-Feld für eine alternative Telefonnummer des CA-Servers. Ein 40-Bit BCD-Feld, um den Geldbetrag zu speichern, der für den Benutzer verfügbar ist. Ein Feld für eine Signatur auf dem letzten Zertifikat für elektronisches Bargeld. Ein 8-Bit-Feld, um einen Schwellenwert zu speichern, um den Benutzer zu informieren, dass das verfügbare elektronische Bargeld weniger als ein vorbestimmter Schwellenwert beträgt, oder um einen automatischen Rückruf an den CA-Server zu initiieren, um Geld hinzuzufügen. Ein 40-Bit BCD-Feld für den Geldbetrag, der ohne Benutzerbeteiligung auf die Karte geladen wird, wenn das elektronische Bargeld weniger als der Schwellenwert beträgt. Der Betrag wird durch den Benutzer bestimmt und während der Kartenaktivierung an den CA-Server gesendet. Wenn dieser Wert Null ist, wird das automatische Laden von elektronischem Bargeld nicht erlaubt. Zwei 768-Bit-Felder zum Speichern des privaten Schlüssels zum Entschlüsseln der AIM und zum Speichern des öffentlichen Schlüssels zum Überprüfen der Signatur auf Zertifikaten. Ein 21-Byte-Feld zum Speichern des DES-Schlüssels zum Entwürfeln der Rundfunkdienste. Zwei 96-Byte-Felder zum Speichern des Schlüssels, um den aktuellen privaten Schlüssel zu ersetzen, und für den Schlüssel, um den aktuellen Überprüfungsschlüssel zu ersetzen. Ein 8-Byte-Feld zum Speichern des symmetrischen DES-Schlüssels für sichere Kommunikation mit dem CA-Server wird auch bereitgestellt. Es liegt in dem Umfang dieser Erfindung, dass ein Verwürfelungsalgorithmus aus einem anderen Code als dem DES bestehen kann.

[0031] Die Karte muss Informationen für PPV-Ereignisse und die Pakete speichern, die durch den Benutzer gekauft werden. Wenn der Kartenspeicher voll ist, wird dem Benutzer nicht erlaubt, zusätzliche Ereignisse zu kaufen.

[0032] Der Datenaustausch zwischen der Karte und dem Wirtsrechner basiert auf einer gut definierten allgemeinen Schnittstelle, d.h. dem National Renewable Security Standard (NRSS) EIA-679 Teil A oder Teil B. Da die Telefonleitung eine weitgehend verfügbare physische Verbindung ist, ist das zwischen dem CA-Server und dem Wirtsrechner gewählte Protokoll das Punkt-zu-Punkt-Protokoll (PPP), RFC 1548, das als Standard 51 angenommen ist, wobei Sicherheit innerhalb von PPP-Datengrammen bereitgestellt wird. Die hier beschriebene technologische Innovation schließt nicht die Verwendung von alternativen Protokollen auf dem Rückkanal aus, die sich von dem PPP unterscheiden.

[0033] PPP ist ein Protokoll, das auf den HDLC-Standards von ISO basiert, wie durch ITU-T für X.25 Systeme angenommen. Es wurde durch die IETF entwickelt, um Datengramme von mehreren Protokollen über

Punkt-zu-Punkt-Verbindungen zu transportieren. Das Rahmenformat besteht aus einem 16-Bit Protokollfeld (in RFC 1700 definiert, „zugewiesene Zahlen"), gefolgt von einem Informationsfeld variabler Länge und dann gefolgt von einem Auffüllfeld, das optionale Bytes enthält, die hinzugefügt werden, um die Rahmenlänge anzupassen (falls von dem Empfangsprotokoll gefordert).

[0034] Für das Austauschen von Daten zwischen der Karte und dem CA-Server, ist ein neues Protokoll definiert, das einen Protokollfeldwert 0 × 00FF aufweist. Für dieses neue Protokoll beträgt der Wert des Auffüllfelds immer null. Das neue Protokoll stellt zuverlässige Übertragung unter Verwendung von Bestätigungs- (ACK) und negativen Bestätigungsmitteilungen (NACK) bereit, welche in das erste Byte des Informationsfelds eingefügt sind, wobei beide Mitteilungen ein 8-Bit uimsbf-Format verwenden.

[0035] Einer ACK können Informationen folgen (Huckepack-Bestätigung), die als Antwort gesendet werden. Wenn das Empfangsende eine korrupte Mitteilung detektiert, antwortet es mit einer NACK und verlangt erneute Übertragung durch den Sender.

[0036] Unter Verwendung des vorstehenden Protokolls, initiiert die intelligente Karte einen Rückruf an den CA-Server bei allen nachfolgenden Bedingungen:

1. Die Karte ist das erste Mal in das DTV eingeschoben worden.
2. Der Benutzer hat eine Anforderung nach einem Paketkauf im Voraus unter Verwendung eines angezeigten Menus eingegeben.
3. Der Speicher der intelligenten Karte ist voll.
4. Die örtliche Zeit liegt innerhalb des Zeitintervalls (1 Uhr–6 Uhr) und es sind neue Einträge vorhanden, die gesendet werden sollen.
5. Die Karte hat eine Benachrichtigung über einen neuen privaten Schlüssel oder Überprüfungsschlüssel empfangen.
6. Das Geld der intelligenten Karte beträgt weniger als der spezifizierte Schwellenwert und automatisches Herunterladen von elektronischem Bargeld ist freigegeben.
7. Der Benutzer hat eine Anforderung nach Geld unter Verwendung eines angezeigten Menus eingegeben.
8. Der Benutzer hat eine Anforderung eingegeben, einen Paketkauf zu stornieren.

[0037] Abhängig von der Bedingung, sendet die intelligente Karte eine anfängliche Alarmmitteilung, um den CA-Server über den Benutzer und den Zweck des Anrufs zu informieren.

[0038] Wenn der Benutzer die Karte das erste Mal in das DTV einschiebt, werden spezifische Informationen der Karte an den CA-Server zur Registrierung gesendet. Diese Informationen sind mit Kcallback verschlüsselt.

Karte → CA-Server:	Alarmmitteilung (mit Alarm Typ = 0 × 01)
Karte ← CA-Server::	ACK-Mitteilung
Karte → CA-Server:	Karteninformationsmitteilung
Karte ← CA-Server:	ACK-Mitteilung

[0039] Ein Kauf im Voraus kann unter Verwendung eines angezeigten Menus getätigt werden. Als Antwort auf die Benutzeranfoderung sendet der CA-Server ein Paketzertifikat, das auf der Karte gespeichert wird. Zum Beispiel:

Karte → CA-Server:	Alarmmitteilung (mit Alarm Typ = 0 × 02)
Karte ← CA-Server:	ACK Mitteilung | Signierte Paketzertifikatsmitteilung
Karte → CA-Server:	ACK-Mitteilung

[0040] Das Paketzertifikatsformat enthält die nachfolgenden Felder. Ein 8-Bit-Feld, das eine Paketzertifikatsmitteilung angibt. Zwei Werte sind möglich, einer für ein erneuerbares Paketabonnement und einer für ein nicht erneuerbares Paketabonnement. Ein 32-Bit-Feld, das die Registrierungsautorität identifiziert, welche dem Feld Anbieter_Index Werte zuweist. Ein 16-Bit-Feld, das den Inhaltsanbieter identifiziert. Diese einzigartige Zahl ist bei der Registrierungsautoriät registriert, die durch den Format_Identifizierer identifiziert ist. Ein 16-Bit-Feld, das den Transportstrom identifiziert, in dem das Ereignis befördert wird. Ein 16-Bit-Feld, das den Paketidentifizierer angibt. Ein 8-Bit-Feld für das Titelfeld. Ein Feld variabler Länge für den Titel des Pakets unter Verwendung von ASCII mit Latein-1 Erweiterungen. Ein 40-Bit-Feld, welches den Preis des Pakets im BCD-Format angibt. Ein 24-Bit-Feld, welches das Ablaufdatum des Pakets angibt.

[0041] Die PPV-Ereigniskaufeinträge werden zeitweise in der Karte gespeichert, bis das Ereignis gesendet worden ist. Sie werden dem CA-Server ohne Beteiligung des Benutzers gesendet und, wenn entweder

(i) der Kartenspeicher keine weiteren Einträge speichern kann, oder
(ii) die örtliche Zeit in dem Zeitintervall (1 Uhr–6 Uhr) liegt und neue Einträge vorhanden sind, die gesendet werden sollen.

[0042] Alle Einträge werden mit Kcallback verschlüsselt.
(i) der Speicher der intelligenten Karte ist voll

Karte → CA-Server:	Alarmmitteilung (mit Alarm_Typ = 0 × 03)
Karte ← CA-Server:	ACK-Mitteilung
Karte→CA-Server:	Eine variable Anzahl von verschlüsselten PPV-Ereigniskaufeinträgen
Karte←CA-Server:	ACK-Mitteilung

(ii) Die örtliche Zeit liegt innerhalb des Zeitintervalls (1 Uhr–6 Uhr) und es sind neue Einträge vorhanden, die gesendet werden sollen.

Karte → CA-Server:	Alarmmitteilung (mit Alarm Typ = 0 × 04)
Karte ← CA-Server:	ACK-Mitteilung
Karte → CA-Server:	Eine variable Anzahl von verschlüsselten PPV-Ereigniskaufeinträgen
Karte ← CA-Server:	ACK-Mitteilung

[0043] Wenn der private Schlüssel oder Überprüfungsschlüssel ersetzt werden muss, wird unter Verwendung des Rundfunkkanals eine Benachrichtigung an die Karten gesendet. Jeder Benutzer muss dann einen Rückruf initiieren, um den neuen Schlüssel zu erhalten.

Karte → CA-Server:	Alarmmitteilung (mit Alarm_Typ = 0 × 05)
Karte ← CA-Server:	ACK-Mitteilung | Schlüsselersatzmitteilung
Karte → CA-Server:	ACK-Mitteilung

[0044] Geld wird der Karte hinzugefügt, wenn:
1. das Geld der intelligenten Karte weniger als ein spezifischer Schwellenwert beträgt, oder
2. der Benutzer eine Anforderung nach Geld unter Verwendung eines angezeigten Menus eingibt, oder
3. die Karte zu einer entfernten Stelle mitgenommen wird, (wenn es keine örtliche Telefonverbindung gibt).

[0045] Die Entität, welche das Geld bereitstellt, überprüft immer die Kredit- oder Debitkarteninformationen, erzeugt ein elektronisches Bargeldzertifikat (ECC), und sendet es an die Karte. Das ECC-Mitteilungsformat besteht aus einem 8-Bit-Feld für den Mitteilungstyp und einem 40-Bit-Feld, um den BCD-Wert des Geldbetrages zu halten, welcher der intelligenten Karte hinzugefügt werden soll.
1) Automatisches Laden von elektronischem Bargeld ist freigegeben:

Karte→CA-Server:	Alarmmitteilung (mit Alarm_Typ = 0 × 06)
Karte←CA-Server:	ACK-Mitteilung
Karte→CA-Server:	Signatur auf elektronischem Bargeld
Karte←CA-Server:	ACK | Signierte Zertifikatsmitteilung für elektronisches Bargeld
Karte→CA-Server:	ACK-Mitteilung

2) Das Zertifikat für elektronisches Bargeld enthält den vorbestimmten, festen Betrag an elektronischem Bargeld. Automatisches Herunterladen von elektronischem Bargeld ist gesperrt. Der Benutzer geht folgendermaßen vor:

Karte → CA-Server:	Alarmmitteilung (mit Alarm_Typ = 0 × 07)
Karte ← CA-Server:	ACK-Mitteilung
Karte → CA-Server:	Signatur auf elektronischem Bargeld | Mitteilung über elektronischen Bargeldbetrag
Karte ← CA-Server:	ACK-Mitteilung | Signierte Zertifikatsmitteilung für elektronisches Bargeld
Karte → CA-Server:	ACK-Mitteilung

[0046] Der Benutzer kann einen Kauf unter Verwendung eines auf dem Bildschirm angezeigten Menus stornieren. Die von der Karte vorgenommenen Aktionen hängen von der Art des Kaufs ab:

(i) Paketkauf: Ein Anruf wird an den CA-Server initiiert.

Karte → CA-Server:	Alarmmitteilung (mit Alarm_Typ = 0 × 08)
Karte ← CA-Server:	ACK-Mitteilung
Karte → CA-Server:	Eintrag des stornierten Paketkaufs
Karte ← CA-Server:	ACK-Mitteilung | Signierte Zertifikatsmitteilung für elektronisches Bargeld
Karte → CA-Server:	ACK-Mitteilung

(ii) PPV-Ereigniskauf: Wenn die Frist zum Stornieren des Ereignisses noch nicht verstrichen ist, wird der ausgewählte Eintrag vollständig gelöscht.

[0047] Die AIM werden als private Daten in dem Anpassungsfeld der Transportstrompakete befördert, welche die Videodaten befördern. Diese AIM könnten auch in dem Transportstrom mit verschiedenen PID unter Verwendung der Werkzeuge und Funktionen befördert werden, welche für ECM-Übertragung in MPEG-2 verfügbar sind. Die Anpassung Feld Steuerung-Bits sollen „10" sein (nur Anpassungsfeld, keine Nutzlast) oder „11" (Anpassungsfeld gefolgt von Nutzlast). Die maximale Zykluszeit für AIM-Mitteilungen mit demselben AIM_Identifizierer soll 500 ms betragen.

[0048] Die Bit-Stromsyntax für die Zugangsinformationsmitteilung enthält die nachfolgenden Felder. Einen einzigartigen 8-Bit Identifizierer für diese Zugangsinformationsmitteilung. Das Feld AIM_Identifizierer ist das zweite Byte in dem Abschnitt private Daten des Anpassungsfelds. Das erste Byte ist zum Identifizieren des öffentlichen Schlüssels zugeteilt, der beim Schützen der AIM verwendet wird (wenn mehrere öffentliche Schlüssel in einem gegebenen DMA verwendet werden). Ein 8-Bit-Feld, das die Anzahl von Bytes in der AIM spezifiziert, das unmittelbar dem Feld AIM_Länge folgt. Ein 32-Bit-Feld, das die Registrierungsautorität identifiziert, welche dem Feld Anbieter_Index Werte zuweist. Ein 16-Bit-Feld, das den Inhaltsanbieter identifiziert. Diese einmalige Zahl ist bei der Registrierungsautoriät registriert, die durch den Format_Identifizierer identifiziert ist. Ein 24-Bit-Feld, das ein bestimmtes TV-Programm oder Ereignis identifiziert. Zugewiesen durch den Inhaltsanbieter, der durch den Anbieter_Index identifiziert ist, identifiziert es in einzigartiger Weise all diejenigen Programme, die in der Datenbank des Inhaltsanbieters registriert sind. Ein 16-Bit-Feld, das den Transportstrom identifiziert, in dem das Ereignis befördert wird. Ein 16-Bit-Feld, das in einzigartiger Weise den bestimmten Dienst identifiziert, der das Ereignis überträgt. Ein 14-Bit-Feld, das in einzigartiger Weise ein bestimmtes Ereignis innerhalb eines gegebenen Dienstes dieses Transportstroms identifiziert. Während Programm_Ereignis_Identifizierer ein Wert ist, der ein Ereignis für einen Inhaltsanbieter identifiziert, ist Ereignis_Identifizierer der Programmführerindex eines Ereignisses. Eine Sendeanstalt, die gleichzeitig als Inhaltsanbieter fungiert, möchte wahrscheinlich beide Zahlen gleich haben, aber dies könnte anderweitig nicht gültig sein. Ein 32-Bit-Feld, das die Anfangszeit des Ereignisses anzeigt. Ein 20-Bit-Feld, das die Länge des Ereignisses gemessen in Sekunden anzeigt. Ein 10-Bit-Feld zum Speichern der ersten 10 Zeichen des englischen Titels für das Ereignis, das diese Mitteilung beschreibt. Wenn der tatsächliche Titel weniger als 10 Zeichen aufweist, dann muss das Titelsegment mit ESC-Zeichen aufgefüllt werden, bevor es in dieses Feld eingebunden wird. Ein 5-Byte BCD-Feld, das die Kosten des Ereignisses anzeigt. Ein 16-Bit-Feld, welches die Pakete anzeigt, zu dem dieses Ereignis gehört. Das höchstwertige Bit entspricht dem ersten Paket, während das niedrigstwertige Bit dem 16-ten Paket entspricht. Wenn das Ereignis zu dem k-ten Paket gehört, dann soll das k-te Bit dieses Felds auf eins gesetzt werden. Mehr als ein einziges Bit kann auf eins gesetzt werden, um ein Ereignis zu zeigen, das zu mehreren Paketen gehört. Ein 64-Bit-Feld für den DES-Schlüssel (oder ein 168-Bit-Feld für den TDES-Schlüssel), der zum Entwürfeln der Video- und Audiosignale für das in Betracht gezogene Ereignis notwendig ist. Ein 40-Bit-Feld, das anzeigt, dass der Benutzer einen neuen privaten Schlüssel oder Überprüfungsschlüssel erhalten muss, indem er den CA-Server anruft. Wenn ein Kennzeichen auf 1 ge-

setzt ist, muss der Schlüssel bis zu der angezeigten Frist ersetzt werden. Ein 8-Bit-Feld zum Identifizieren der gesamten Länge (in Bytes) der nachfolgenden AIM-Schlüsselwortliste.

[0049] Bei einer Ausführungsform der vorliegenden Erfindung können Berechtigungsverwaltungsmitteilungen (ECM) anstatt AIM verwendet werden. Das Format der ECM ist privat gemäß MPEG-2 and ATSC-Spezifikationen definiert. Ein bestimmtes Format, das verwendet werden kann, umfasst ein 8-Bit-Feld für Tabellenidentifizierung, 3 Anzeigebits, ein 12-Bit-Feld für Abschnittslänge, ein 8-Bit-Feld für Protokollversion, ein 5-Bit-Feld für Versionsnummer, 2 Felder für Abschnittsnummer, ein Feld für öffentlichen Schlüssel, ein Feld für Transportstromidentifizierung, Felder für eine größere und kleinere Kanalnummer, 2 Felder für Ereignisidentifizierung, Felder für Strom PID und für Schlüsselwortlänge, ein Feld für Verschlüsselungsprüfung, ein Feld für Füllbytes, und ein 32-Bit-Feld für CRC.

[0050] Die Sicherheit des Systems basiert auf standardmäßigen und weitverbreitet akzeptierten öffentlichen Schlüssel- und symmetrischen Schlüsselalgorithmen. Die gewählten Algorithmen sind RSA für Verschlüsselung des öffentlichen Schlüssels und TDES und/oder DES für Verwürfelung des symmetrischen Schlüssels. Es gibt ein globales RSA öffentlich/privates Schlüsselpaar, Kpub/Kpri, für das gesamte System. Alle Sendeanstalten nutzen den öffentlichen Schlüssel gemeinsam und der entsprechende private Schlüssel ist in den fälschungssicheren auf NRSS-A basierten intelligenten Karten untergebracht, welche durch die CA-Anbieter an die Verbraucher verteilt werden. Dieser öffentliche Schlüssel wird verwendet, um die AIM zu schützen, die an dem Kopfende erzeugt werden.

[0051] Die AIM, die mit dem öffentlichen Schlüssel verschlüsselt werden, befördern die Steuerworte (CW), welche aus symmetrischen DES-Schlüsseln, KDES, bestehen, die beim Verwürfeln des Audio-/Videoinhalts in dem ECB-Modus verwendet werden. Nach dem Entschlüsseln der AIM mit ihrem privaten Schlüssel erhält die Karte die DES-Schlüssel und entwürfelt Audio-/Videoströme. An dem Kopfende: Verwürfeln: E_{KDES}(A/V-Strom), Verschlüsselung: E_{Kpub} (AIM). Auf der Karte: Entschlüsselung: $D_{Kpri}(E_{Kpub}(AIM))$, Entwürfelung: $D_{KDES}(E_{K-DES}$(A-/V-Strom)).

[0052] Die Sicherheit des Systems kann auf eine Reihe von Wegen verbessert werden. Ein machbarer Lösungsansatz besteht daraus, mehrere öffentliche Schlüssel an dem Kopfende zum Verschlüsseln der AIM zu verwenden. Solches Verwenden von mehreren Schlüsseln kann in Bereichen von überlappenden Märkten vorteilhaft sein, zum Beispiel kann der Benutzer terrestrischen digitalen Rundfunk von mehr als dem Hauptmarkt empfangen. Ein anderes Beispiel wäre, wenn die Gesamtheit der Empfänger in einem gegebenen DMA in getrennte Untermengen unterteilt ist und jeder Untermenge ein verschiedener privater Schlüssel zugewiesen wird, würde ein Angriff auf einen privaten Schlüssel das System nicht gefährden.

[0053] Zum Beispiel kann die Verschlüsselung am Kopfende vier Schlüssel beinhalten, E_{Kpub1}(AIM), E_{Kpub2}(AIM), E_{Kpub3}(AIM), E_{Kpub4}(AIM). Die Entschlüsselung auf der Karte würde dann auf einem der nachfolgenden vier Schlüssel basieren, Kartentyp 1: $D_{Kpri1}(E_{KPub1}(AIM))$, Kartentyp 2: $D_{Kpri2}(E_{Kpub2}(AIM))$ Kartentyp 3: $D_{kpri3}(E_{Kpub3}(AIM))$, und Kartentyp 4: $D_{Kpri4}(E_{Kpub4}(AIM))$. Der beim Verschlüsseln der AIM verwendete öffentliche Schlüssel ist unter Verwendung des Identifizierers in dem ersten Byte des Anpassungsfelds identifiziert. Dieses Feld gibt den öffentlichen Schlüssel an, der zum Verschlüsseln der AIM verwendet wird. Wenn der Wert i ist, ist der aktive öffentliche Schlüssel Kpubi.

[0054] Die Zertifikate elektronischen Bargelds weisen den Geldbetrag aus, welcher der Karte hinzugefügt werden soll. Die Paketzertifikate umfassen den Preis des Pakets, das dem Kunden angeboten wird. Da beide Zertifikate sensitive Daten tragen, muss es einen Signaturmechanismus geben, der die Unversehrtheit dieser Mitteilungen sicherstellt. Daher werden alle Zertifikate über einen Kanal mit einem Rückkopplungsweg gesendet, zum Beispiel einen Rückwärtskanal unter Verwendung eines Modems.

[0055] Obwohl die Paketzertifikate normalerweise von dem CA-Server gesendet werden, kann es verschiedene Quellen (z.B. Geldautomaten oder andere besondere Terminals) zum Herunterladen von elektronischem Bargeld auf die Karte geben. Wenn jede Quelle mit einem einzigartigen privaten Schlüssel signiert, muss DTV mehrere öffentliche Schlüssel führen. Das vorliegende CA-System wendet ein ID-basiertes Authentifizierungsschema an, um die Signaturüberprüfung unter Verwendung von nur einem einzigen öffentlichen Schlüssel zu erlauben.

[0056] Wie schon zuvor erwähnt, müssen die Sendeanstalten, CA-Server und die intelligenten Karten bestimmte Schlüssel speichern, um an den Verwürfelungs-, Verschlüsselungs- und Signaturprotokollen teilzunehmen. Die Speicherung und Verwendung von allen Typen von Schlüsseln ist in **Fig. 3** zusammengefasst.

[0057] Kpub wird auf der Seite der Sendeanstalt geführt, und wird verwendet, um die DES-Schlüssel zu verschlüsseln, die lokal erzeugt werden, um die A-/V-Ströme zu verwürfeln. Die Karte weist den entsprechenden Kpri zum Wiederherstellen der DES-Schlüssel auf.

[0058] Ksig wird verwendet, um Zertifikate für Pakete und für elektronisches Bargeld zu signieren. Die signierten Zertifikate werden mit Kver überprüft, der auf der Karte gespeichert ist. Bei dem ID-basierten Schema, das in Abschnitt 8.2 beschrieben ist, ist Ksig für jeden Zertifikatsanbieter (CA-Lieferanten, Geldautomaten, usw.) einzigartig, aber Kver ist allen Zertifikatanbietern gemeinsam.

[0059] Kcallback wird zwischen der Karte und dem CA-Server gemeinsam genutzt und wird verwendet, um sensitive ausgetauschte Informationen zu verschlüsseln. Die von der Karte an den CA-Server gesendeten Informationen sind Geldkartennummer, festes elektronisches Bargeld und Ereigniskaufeinträge. Falls erforderlich, werden Kpri und Kver durch den CA-Server ersetzt. Kcallback kann für jede Karte einzigartig sein. Sein Ersatz ist nur durch Senden einer neuen Karte an den Benutzer möglich.

[0060] Während die Erfindung ausführlich unter Bezugnahme auf ihre zahlreichen Ausführungsformen beschrieben worden ist, wird es nach dem Lesen und Verstehen des Vorausgehenden ersichtlich sein, dass den Fachleute zahlreiche Änderungen an den beschriebenen Ausführungsformen einfallen, und es vorgesehen ist, dass der Umfang der beigefügten Ansprüche solche Änderungen umfasst. Zum Beispiel kann die Erfindung erfolgreich sowohl mit digitalem terrestrischem Rundfunk als auch übertragenen digitalen Satellitensignalen verwendet werden.

Patentansprüche

1. Verfahren zum Verwalten von Zugang zu einem beschränkten übertragenen Ereignis, wobei das Ereignis von einem einzigen von einer Vielzahl von verschiedenen Dienstleistern übertragen wird, wobei jeder der Vielzahl für Ereignisübertragung denselben öffentlichen Schlüssel gemeinsam nutzt, wobei das Verfahren umfasst:
(a) Empfangen verschlüsselter Zugangsinformationen, die dem übertragenen Ereignis zugeordnet sind, wobei die Zugangsinformationen mit dem gemeinsam genutzten öffentlichen Schlüssel verschlüsselt werden und Daten umfassen, die den Kosten des übertragenen Ereignisses entsprechen;
(b) Entschlüsseln der Zugangsinformationen in einem Zugangsberechtigungsmodul unter Verwendung eines entsprechenden privaten Schlüssels, der dem gemeinsam genutzten öffentlichen Schlüssel zugeordnet ist, welcher in dem Zugangsberechtigungsmodul gespeichert ist;
(c) Überprüfen, in dem Zugangsberechtigungsmodul, dass die Kosten des übertragenen Ereignisses weniger betragen als eine vorgespeicherte Bargeldreserve;
(d) Empfangen des übertragenen Ereignisses von dem Dienstleister, wobei das übertragene Ereignis verwürfelt ist; und
(e) Entwürfeln des übertragenen Ereignisses in dem Zugangsberechtigungsmodul.

2. Verfahren nach Anspruch 1, wobei die Zugangsinformationen ferner einen Ereignisentwürfelungsschlüssel und Kaufinformationen umfassen, wobei die Kaufinformationen Kanalidentifizierungsdaten, Ereignisidentitätsdaten, Datums- und Zeitstempeldaten und Abrechnungsdaten umfassen.

3. Verfahren nach Anspruch 2, ferner den Schritt umfassend, Daten, die dem gekauften übertragenen Ereignis zugeordnet sind, an den Dienstleister zu transferieren, um Kontoinformationen eines Benutzers zu aktualisieren.

4. Verfahren nach Anspruch 3, wobei das Zugangsberechtigungsmodul eine intelligente Karte umfasst.

5. Verfahren nach Anspruch 4, wobei die intelligente Karte einen Kartenkörper mit einer Vielzahl von Kontakten auf einer Oberfläche des Kartenkörpers entweder gemäß ISO 7816 oder PCMCIA Kartenstandard umfasst.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

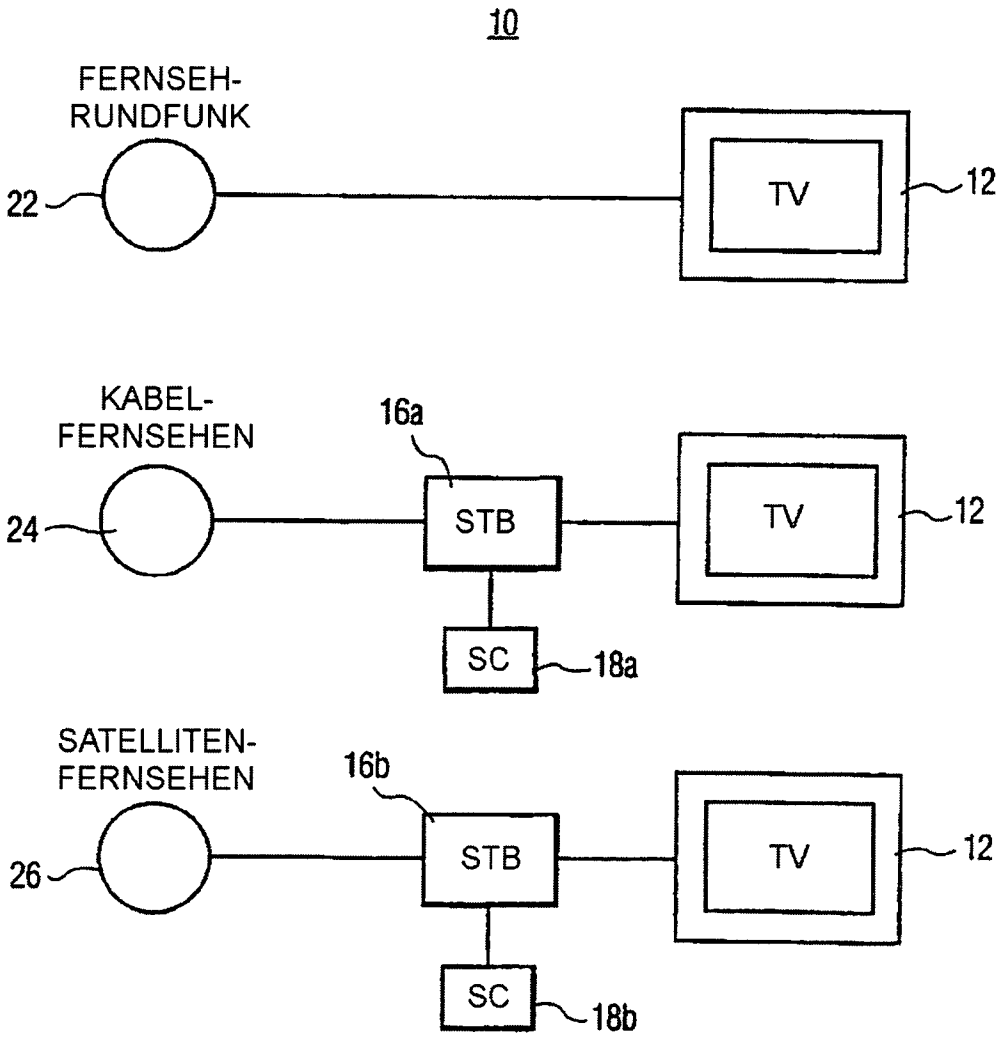

FIG. 1

STAND DER TECHNIK

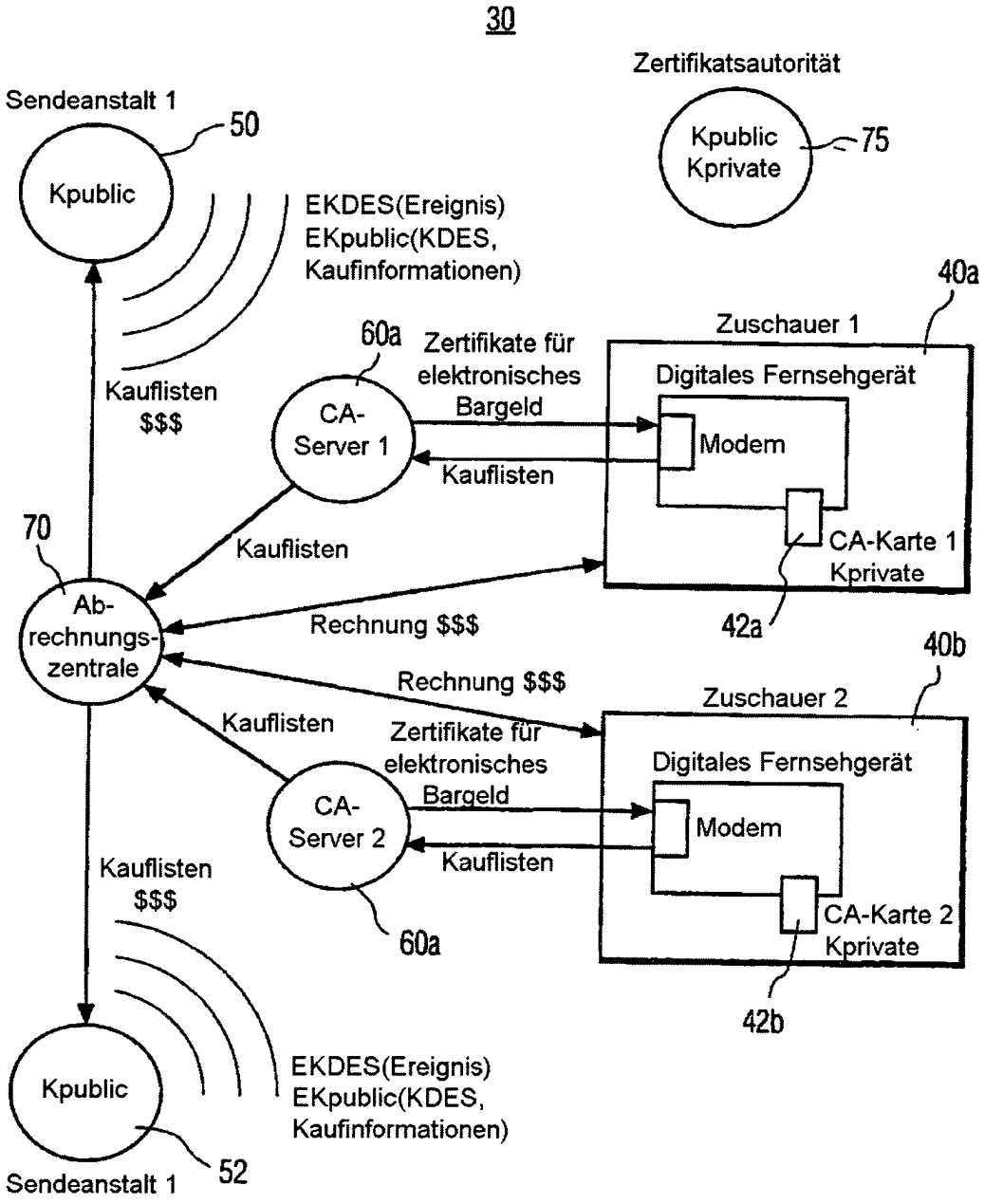
30
Zertifikatsautorität
Kpublic
Kprivate
75
Sendeanstalt 1
50
Kpublic
EKDES(Ereignis)
EKpublic(KDES,
Kaufinformationen)
Kauflisten
$$$
60a
Zertifikate für
elektronisches
Bargeld
CA-
Server 1
Kauflisten
40a
Zuschauer 1
Digitales Fernsehgerät
Modem
CA-Karte 1
Kprivate
42a
70
Kauflisten
Ab-
rechnungs-
zentrale
Rechnung $$$
Rechnung $$$
40b
Zuschauer 2
Kauflisten
Zertifikate für
elektronisches
Bargeld
Digitales Fernsehgerät
CA-
Server 2
Modem
Kauflisten
Kauflisten
$$$
CA-Karte 2
Kprivate
60a
42b
Kpublic
EKDES(Ereignis)
EKpublic(KDES,
Kaufinformationen)
Sendeanstalt 1
52

FIG. 2

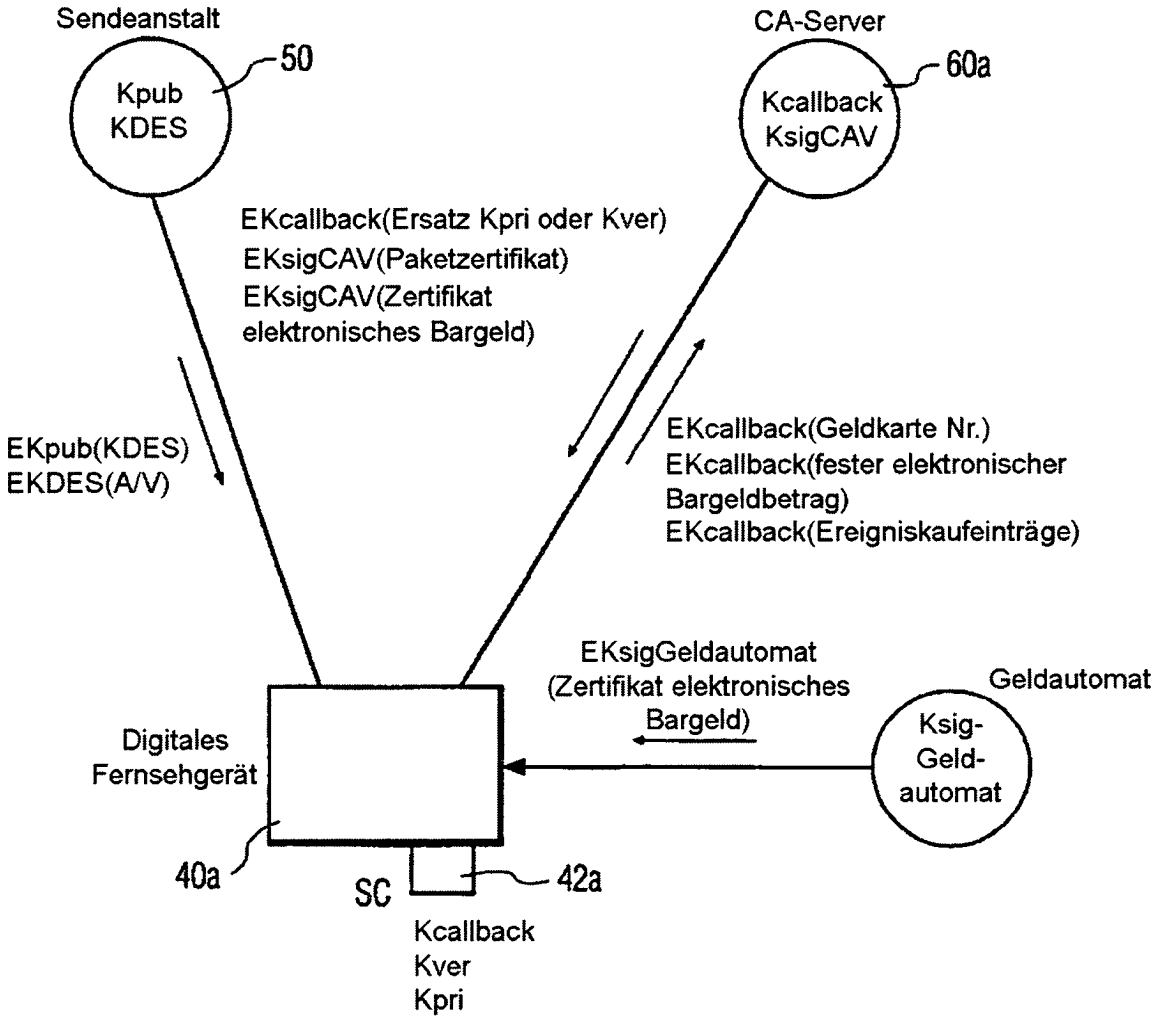
Sendeanstalt
50
Kpub
KDES
CA-Server
60a
Kcallback
KsigCAV
EKcallback(Ersatz Kpri oder Kver)
EKsigCAV(Paketzertifikat)
EKsigCAV(Zertifikat
elektronisches Bargeld)
EKpub(KDES)
EKDES(A/V)
EKcallback(Geldkarte Nr.)
EKcallback(fester elektronischer
Bargeldbetrag)
EKcallback(Ereigniskaufeinträge)
EKsigGeldautomat
(Zertifikat elektronisches
Bargeld)
Geldautomat
Ksig-
Geld-
automat
Digitales
Fernsehgerät
40a
SC
42a
Kcallback
Kver
Kpri

FIG. 3