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

(10) **DE 600 12 351 T2** 2005.08.04

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 222 819 B1**
(21) Deutsches Aktenzeichen: **600 12 351.0**
(86) PCT-Aktenzeichen: **PCT/US00/28942**
(96) Europäisches Aktenzeichen: **00 973 676.0**
(87) PCT-Veröffentlichungs-Nr.: **WO 01/030083**
(86) PCT-Anmeldetag: **19.10.2000**
(87) Veröffentlichungstag der PCT-Anmeldung: **26.04.2001**
(97) Erstveröffentlichung durch das EPA: **17.07.2002**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.07.2004**
(47) Veröffentlichungstag im Patentblatt: **04.08.2005**

(51) Int Cl.[7]: **H04N 7/167**
H04N 7/16, H04N 5/00

(30) Unionspriorität:
160355 P **19.10.1999** **US**

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

(73) Patentinhaber:
Thomson Licensing S.A., Boulogne, Cedex, FR

(74) Vertreter:
derzeit kein Vertreter bestellt

(72) Erfinder:
DUFFIELD, Jay, David, Indianapolis, US; DEISS, Scott, Michael, Zionsville, US

(54) Bezeichnung: **SYSTEM UND VERFAHREN ZUM ÜBERPRÜFEN DER BERECHTIGUNG ZUR ÜBERTRAGUNG GESCHÜTZTEN INFORMATIONSINHALTS**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung betrifft allgemein eine digitale Audio/Video-Übertragung und insbesondere ein Verfahren zur Prüfung der Berechtigung für einen Zugriff zu einem ansonsten geschützten Inhalt.

Hintergrund der Erfindung

[0002] Erweiteter bedingter Zugriff (XCA = Extended Conditional Access) ist ein System zum Schutz des digitalen, codierten Audio/Video (A/V)-Inhalts während der Übertragung und Speicherung. Unter dem XCA-System wird der Inhalt eines ökonomischen Wertes verschachtelt oder verschlüsselt, um einen unberechtigten Zugriff zu verhindern. Der XCA ermöglicht die Aufzeichnung eines verschlüsselten Inhalts, ermöglicht jedoch nicht die Entwürfelung des Inhalts, die nicht legitim ist. Der berechtigte Inhalt ist zum Beispiel derjenige, der ein Original oder auf andere Weise durch den Copyright-Inhaber berechtigt. Natürlich bezieht sich die Entwürfelung auf den Vorgang der Entschlüsselung. Wenn ein nicht-berechtigter Inhalt nicht entwürfelt ist, kann er nicht betrachtet werden.

[0003] Ein anderes Merkmal des XCA-Aufbaus ist die Vorstellung eines bedingten Zugriffs (CA = Conditional Access) und des örtlichen Schutzes. CA bezeichnet den Zugriff zu einem geschützten Inhalt wie einer Programmierung. Auswechselbare Sicherheitseinheiten bewirken sicherheitsbezogene Funktionen. Der Inhalt des ökonomischen Wertes wird durch Anwendung eines CA-Service geliefert. Zum Beispiel verschlüsseln digitale Sattelitensysteme einen Videoinhalt und die Entwürfelungsschlüssel für die Massenverteilung zu ihren Abonnenten. Manche Abonnenten können sich entscheiden, den Inhalt zu kaufen. In diesem Fall werden sie mit den benötigten Schlüsseln zur Wiedergewinnung/Erlangung des Entwürfelungsschlüssels versorgt. Diejenigen Abonnenten, die nicht wünschen, den Inhalt zu kaufen, erhalten keinen Zugriff zu diesen Schlüsseln. In der XCA-Terminologie ist dies der Vorgang eines CA.

[0004] XCA-Systeme benutzen einen Rückkanal zum Empfang der Berechtigungsprüfung der örtlichen Tasten und Identitäten, die für den Zugriff zu dem Inhalt benötigt werden. Das bildet ein Problem insofern, als die meisten Geräte ein Verfahren für einen Rückweg irgendeiner Art haben müssen, damit dieses arbeitet.

[0005] Ein verbessertes Verfahren für die Schlüssel und Identifizierer der Berechtigungsschlüssel benutzt für den Zugriff zu einem anderen Falls geschützten Inhalt in dem XCA, und andere Systeme mit einem bedingten Zugriff sind erwünscht.

[0006] Systeme für einen bedingten Zugriff (CA = Conditional Access) sind im Stand der Technik bekannt zur Bildung eines Schutzes eines Inhalts (z. B. audio/visueller Inhalt), die von einem Serviceanbieter (z. B. Sattelitenprogrammanbieter, Kabelprogrammanbieter usw.) zu einem Systembenutzer übertragen werden. Die PCT Anmeldung WO 99/07150, veröffentlicht am 11. Februar 1999, lehrt ein System für einen bedingten Zugriff, in dem verschlüsselte Programme von einem Serviceanbieter zu einer oder mehreren Set Top Boxen übertragen werden. Die Programme werden entschlüsselt durch sogenannte Entitlement Management Messages (EMMs) und Entitlement Control Messages (ECMs), die durch die Set Top Box empfangen werden.

Zusammenfassung der Erfindung

[0007] Ein Verfahren zur Prüfung, ob ein Quellengerät berechtigt ist, mit einem ansonsten geschützten Inhalt zu kommunizieren (z. B. verwürfelte Servicedienste) zu einem Senkengerät in einem System für einen bedingten Zugriff mit: Bildung eines im wesentlichen einzigartiger Identifizierers für die Quelle- und Senkengeräte zu einer Behörde für eine Gültigkeitserklärung. Die Behörde für die Gültigkeitserklärung ermittelt einen Zustimmungscode unter Anwendung von Daten für die Quelle und die Senkengeräte, die Daten entsprechend den kommunizierten Identifizierern, und das Quellengerät ermittelt einen örtlichen Code aus den Daten für die Quelle und die Senkengeräte und vergleicht wenigstens einen Teil des Zustimmungscodes mit wenigstens einem Teil eines örtlichen Codes für die Prüfung, ob das Quellengerät für die Kommunikation des Inhalts zu dem Senkengerät berechtigt ist.

Kurzbeschreibung der Figuren

[0008] Fig. 1 zeigt ein System gemäß einem Aspekt der vorliegenden Erfindung, und

[0009] Fig. 2 zeigt ein System gemäß einem zweiten Aspekt der vorliegenden Erfindung.

Detaillierte Beschreibung der Erfindung

[0010] Gemäß der vorliegenden Erfindung dient ein Inhaber oder Benutzer oder Operator von Geräten in einem XCA-System als Teil eines viablen Rückweges. Ein Hauptproblem ergibt sich jedoch, wenn ein Operator eines Geräts als ein Rückkanal benutzt wird. Von einem Benutzer kann man nicht erwarten, eine Zahl mit 768 Bit richtig zu lesen oder einzugeben. Jedoch werden große Zahlen benötigt zur Verhinderung von sogenannten "brute-force cryptanalysis"-Angriffen, d. h. der Versuch jeder möglichen Signatur, bis man arbeitet. Dieses Problem prüft, das die Nachricht, z. B. ein öffentlicher Schlüssel, die empfangen worden ist, gültig ist. Zertifikate oder Signatu-

ren, die dafür dienen, haben im allgemeinen eine Länge von wenigstens 20 Byte, und im allgemeinen näher zu 100 Byte. Die Signatur muss genügend mögliche Werte haben, um sogenannte "brute-force"-Angriffe unbrauchbar zu machen. Gemäß der Erfindung wird dasselbe Ziel erreicht mit einem wesentlich kleineren Schlüsselplatz durch Begrenzung, welche Ressourcen für einen "brute-force"-Angriff benutzt werden können.

[0011] Fig. 1 zeigt ein System **10** für die Prüfung der Zugriffsberechtigung zu einem anderenfalls geschützten Inhalt. Das System **10** enthält ein Quellengerät **20** mit einem zugehörigen Identifizierer (SOURCEID), ein Senkengerät mit einem zugehörigen digitalen Schlüssel (PUBLICKEY), einen Benutzer oder Operator **50** des Quellengeräts **20** und ein Kopfende CA oder ein sogenanntes Trusted Third Party (TTP)-System 40.

[0012] Das Quellengerät **20** kann die Form eines Zugriffsgeräts annehmen wie einer Satteliten Set Top Box (STB) oder Medienspielers, wie ein digitaler Videokassettenspieler (DVHS) oder ein vielseitiger digitaler Plattenspieler (DVD), während das Senkengerät die Form eines digitalen Fernsehgeräts (DTV) annehmen kann.

[0013] Gemäß einem anderen Aspekt der Erfindung haben sowohl das Quellengerät **20** als auch das Senkengerät **30** öffentlich zugängliche Seriennummern.

[0014] Im allgemeinen wird, um die Übertragung des Inhalts von dem Quellengerät **20** zu dem Senkengerät **30** zu schützen, so dass es nicht unerlaubt wiedergegeben oder auf andere Weise ungeeignet benutzt werden kann, die PUBLICKEY des Senkengeräts **30** zu dem Quellengerät **20** übertragen. Der durch das Quellengerät **20** gelieferte Inhalt wird durch ein PUBLICKEY des Senkengeräts **30** verwürfelt und in verwürfelter Form zu dem Senkengerät **30** übertragen. Das Senkengerät **30** benutzt den entsprechenden privaten Schlüssel, um den Inhalt zu entwürfeln und seine richtige Wiedergabe durch das Senkengerät **30** zu ermöglichen. Es sollte auch bemerkt werden, dass das obige durch Anwendung eines zweistufigen Vorgangs erfolgen kann, in dem der Inhalt durch einen symmetrischen Algorithmus erwürfelt und das Steuerwort für diese Verwürfelung durch Anwendung des PUBLICKEY gesendet wird.

[0015] Der PUBLICKEY und SOURCEID des Senken- und Quellengeräts **30** bzw. **20** werden durch die TTP aus den Seriennummern dieser Geräte ermittelt. Der ermittelte PUBLICKEY und SOURCEID werden durch die Geräte **20**, **30** und TTP getrennt, um die Berechtigung zu überprüfen, dass die Geräte **20**, **30** für den Zugriff zu dem Inhalt in Kombination arbeiten können.

[0016] Der Benutzer **50** erhält die Seriennummern von den jeweiligen Quellen- und Senkengerät **20** bzw. **30** (z. B. dadurch, dass sie aus den Geräten gelesen werden) und fordert das Kopfende CA-System auf, die Anwendung des Quellen- und Senkengerätes **20**, **30** in Kombination zu ermöglichen. Der Benutzer **50** liefert diese Seriennummern zu dem Kopfende CA-System **40** als Kommunikation **52**. Diese Seriennummern können zum Beispiel in einer Sprachkommunikation oder elektronisch oder akustisch gebildet werden. Das Kopfende CA-System **40** hat einen Zugriff zu einer Datenbank, die die gelieferten Seriennummern in SOURCEID und PUBLICKEY Daten umsetzt. Somit kann das Kopfende CA-System **40** die SOURCEID und PUBLICKEY Daten des Quellengeräts **20** und des Senkengeräts **30** z. B. durch Anwendung einer Lookup aus diesen kommunizierten Seriennummern identifizieren. Gemäß einem anderen Aspekt der vorliegenden Erfindung ist es wichtig, dass der Zusammenhang zwischen den Seriennummern und der SOURCEID nicht publik und nicht leicht feststellbar ist.

[0017] In Fig. 1 berechnet das Kopfende CA-System **40** einen Hash-Code dieser beiden Werte, z. B. der SOURCEID und der PUBLICKEY als eine Zustimmungs-Hash-Kalkulation und liefert sie zu dem Benutzer **50** als eine persönliche Identifikationsnummer (PIN = Personal Identification Number) (dargestellt als Kommunikation **42**). Der Benutzer **50** gibt dann diese PIN in das Quellengerät **20** ein (dargestellt als Kommunikation **54**), der dieselbe Hash-Berechnung hat, z. B. als eine örtliche Hash-Berechnung unter Anwendung des SOURCEID in dem Quellengerät **20** und der durch das Senkengerät **30** gelieferte PUBLICKEY (dargestellt als Kommunikation **34**). Wenn der PIN mit dem Hash übereinstimmt, dann erkennt das Quellengerät **20** dass die PUBLICKEY, die in der Kommunikation von dem Senkengerät **30** gebildet wird, für die Anwendung gültig ist, dass das Kopfende CA-System **40** diesen Schlüsselempfangen hat und das Kopfende CA-System **40** sie für die Anwendung freigibt, so dass das Quellengerät **20** und das Senkengerät **30** berechtigt werden, in Kombination miteinander zu arbeiten.

[0018] Gemäß einem anderen Aspekt der vorliegenden Erfindung und wie oben angegeben, wird entweder der SOURCEID und/oder der Algorithmus für die Berechnung des Hash geheim gehalten. Wie der Fachmann auf diesem Gebiet verstehen wird, verhindert die Tatsache, dass ein potentieller Pirat oder sogenannter Hacker nicht diesen Eingang zu der Hash-Funktion hat wirkungsvoll einen sogenannten "brute-force" Angriff mit einem leistungsfähigeren Computer verhindert.

[0019] Gemäß einem anderen Aspekt der vorliegenden Erfindung hat der PIN Code einen genügend großen Zwischenraum oder Leerzeichen, dass eine

ausgedehnte Suche nach einer gültigen Signatur prohibitiv lang wird. Ein Weg, um dieses zu erreichen, besteht darin, dass das Quellengerät **20** eine beachtliche Zeit für die Zustimmung des PIN Codes einnimmt, zum Beispiel entweder mit einer komplexen Berechnung oder mit einer Wartezeit nach der Berechnung. Ein angenommener Wert für diese Anwendung, z. B. Kopierschutz für ein Heim-A/V-Netz, könnte bei 9 bis 10 digitalen PIN und einer Berechnungszeit von einer Sekunde liegen. Das würde eine im Mittel zu lange Suchzeit von 5×10^8 oder 5×10^9 Sekunden oder ungefähr 16 oder 160 Jahre erfordern.

[0020] Gemäß einem anderen Aspekt der vorliegenden Erfindung kann ein anderer Eingang zu der Hash-Funktion ein Titel-Code oder Medium sein, wie eine Magnetband- oder DVD-Seriennummer. Das ermöglicht, dass zum Beispiel individuelle Titel oder Bänder für die Anwendung angenommen oder abgelehnt werden. Man kann eine nennenswerte Zeitersparnis durch Speicherung der Seriennummern für einen bestimmten Benutzer **50** in dem Kopfende CA-System **40** erreichen, so dass der Benutzer sie nicht für jede Transaktion liefern muss.

[0021] Gemäß einem anderen alternativen Aspekt der vorliegenden Erfindung kann ein anderer Eingang zu der Hash-Funktion eine Anzeige für eine Gesamtlaufzeit oder verstrichene Zeit seit der ersten Zustimmung sein. Das ermöglicht, dass die Zustimmung automatisch nach einer Einstell- oder Benutzungszeit ausläuft. Wenn ein gesonderter Zeitcode benötigt wird, kann dieser von dem Quellengerät **20** zu dem Benutzer **50** signalisiert werden. Die Zeitcodes sollten ausreichend zufallsgesteuert sein, so dass der Benutzer **50** nicht vermuten oder auf andere Weise voraussagen kann, welches der nächste Zeitcode sein wird. Wenn der Benutzer **50** dieses tun könnte, könnte er im voraus anrufen und sein System im wesentlichen vorautorisieren durch Erlangung der PIN Codes, bevor sie benötigt werden.

[0022] Gemäß einem anderen alternativen Aspekt der vorliegenden Erfindung beruht ein anderer PIN Code auf dem sogenannten "balkanizing" oder Teilung des Schlüsselzwischenraums der örtlichen Netze in kleinere Segmente, ohne zu der extremen Sicherheit mit der Anwendung einzigartiger Netzschlüssel überzugehen.

[0023] Fig. 2 zeigt ein anderes System **100**, das für die Berechtigungstasten und Identifizierer geeignet ist, die für den Zugriff auf andere Weise geschützten Inhalt benutzt werden. Das System **100** enthält ein Quellengerät **120** mit einem zugehörigen SOURCEID, ein Senkengerät **130** mit einer zugehörigen PUBLICKEY, einen Benutzer oder Operator **150** des Quellengeräts **120** und ein Kopfende CA-Systems **140**.

[0024] Senkengeräte können mit einer relativ kleinen Zahl von privaten Schlüsseln gebildet werden, zum Beispiel 10.000. Der Benutzer **150** liest die Seriennummern des Senkengeräts **130** und des Quellengeräts **120** (dargestellt als Kommunikation **132** bzw. 122). Der Benutzer **150** ruft dann in das Kopfende CA-System **140** liefert, die Seriennummer des Senkengeräts **130** und des Quellengeräts **120** und empfängt den PIN Code für dieses Senkengerät **130** (dargestellt als Kommunikationen **152**, **142**). Der PIN Code kann über eine sogenannte Lookup-Tabelle oder geeignete Berechnungen ermittelt werden. Der Benutzer **150** gibt dann diesen PIN Code in das Quellengerät **120** ein (dargestellt als Kommunikation **154**), und das Quellengerät **120** indexiert für den richtigen öffentlichen Schlüssel für die Anwendung für das Senkengerät **130** unter Anwendung einer Tabelle **160** von öffentlichen Schlüsseln.

[0025] Die Tabelle der öffentlichen Schlüssel **160** ist groß verglichen mit der Speicherung des Quellengeräts **120** selbst. Die Tabelle **160** wird verschlüsselt und zu Beginn des voraufgezeichneten Mediums (zum Beispiel Magnetbänder) gespeichert. Das ergibt im Bedarfsfall einen leichten Mechanismus für die Gewinnung des öffentlichen Schlüssels (PUBLICKEY), da jedes vorbespielte Band das Netz initiieren kann. Danach arbeitet das System **100** auf sich selbst, da das Quellengerät **120** sich an den richtigen Schlüssel für die Anwendung mit dem Senkengerät **130** erinnern kann.

[0026] Vorbespielte Medien wie Magnetbänder werden konventionell mit einem anderen, strengeren Verschlüsselungssystem verschlüsselt. Bei der vorliegenden Erfindung wird nur die digitale Strecke von dem Quellengerät **120** zu dem Senkengerät **130** mit diesem schwächeren örtlichen Schlüssel verschlüsselt. Während der örtliche Schlüssel für dieses Netz nicht einzigartig ist, wird es sehr schwierig sein, Kopien eines Materials herzustellen, wenn 10.000 unterschiedliche Versionen des Bandes für jeden Titel benötigt werden.

[0027] In dem Fall, dass einer der 10.000 örtlichen Schlüssel des oben beschriebenen Systems **100** bekannt wird, könnten "private" Benutzer oder Hacker ständig denselben PIN Code benutzen, damit der Inhalt durch Anwendung eines Quellengeräts **120** wiedergegeben werden kann. Das System **100** kann verbessert werden, in dem der PIN Code als Hash-Funktion des SOURCEID ausgebildet wird, ebenso als der Index in die Tabelle der öffentlichen Schlüssel **160**. Das zwingt den Benutzer **50**, einen einzigartigen PIN für jedes Quellengerät **120** zu bilden. Wenn eine überwältigende Anzahl von Anforderungen für einen bestimmten öffentlichen Schlüssel in der Indextabelle **160** eingehen, dann kann das benutzt werden als ein Signal, mit dem ein privater Schlüssel einen Kompromiss eingegangen ist.

Patentansprüche

1. Verfahren zur Prüfung, ob ein Quellengerät (**20**), das zur Übertragung eines geschützten Audio/Video-Inhalts geeignet ist, berechtigt ist, diesen geschützten Inhalt zu einem Senkengerät (**30**) zu kommunizieren, wobei das Senkengerät (**30**) in der Lage ist zur Entwürfelung des geschützten Inhalts und zur Wiedergabe des Audio/Video-Inhalts von dem Quellengerät, gekennzeichnet durch folgende Schritte:
Empfang eines Zustimmungs-Codes (PIN) bei dem Quellengerät (**20**), der unter Anwendung von Daten ermittelt wird, die zu den Quellen- bzw. Senkengerät gehören,
getrennte Ermittlung in dem Quellengerät (**20**) eines örtlichen Codes durch Anwendung entsprechender Daten für das Quellengerät bzw. das Senkengerät (PUBLICKEY, SOURCEID), und
Vergleich wenigstens eines Teils des Zustimmungs-Codes (PIN) mit wenigstens einem Teil des örtlichen Codes, wobei in Abhängigkeit von dem Vergleich das Quellengerät die Berechtigung für die Übertragung des geschützten Inhalts zu dem Senkengerät (**30**) zur Entwürfelung und Wiedergabe des Audio/Video-Inhalts prüft.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Zustimmungs-Code ermittelt wird aufgrund einer Hash-Berechnung unter Anwendung eines von im wesentlichen einzigartigen Identifizierern für das Quellen- und Senkengerät, und wobei der örtliche Code auf der Grundlage einer Hash-Berechnung ermittelt wird, durch Anwendung von Daten von dem Senkengerät und einem in dem Quellengerät vorgespeicherten Quellenidentifizierer.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Daten für das Quellengerät zur Ermittlung des örtlichen Codes keine öffentlichen Informationen sind, und wobei die Daten für das Senkengerät zur Ermittlung des örtlichen Codes öffentliche Informationen enthalten.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Identifizierer Seriennummern oder andere Identifizierungs-Codes enthalten, die für einen Benutzer zugänglich sind, und wobei die Daten von dem Senkengerät, die in der Hash-Berechnung benutzt werden, einen öffentlichen Schlüssel enthalten.

5. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Daten für das Quellen- und Senkengerät eine einzigartige Identifikation des Quellengeräts und einen öffentlichen Verschlüsselungsschlüssel für das Senkengerät enthalten.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Quellengerät kommuniziert, ob das Quellengerät berechtigt ist zur Lieferung des Inhalts zu dem Senkengerät zu einem Benutzer, und absichtlich kommunizieren, ob der verglichene Zustimmungs-Code und der örtliche Code konsistent sind.

7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Quellengerät aus einem Zugriffsgerät oder einem Mediaspieler gewählt ist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

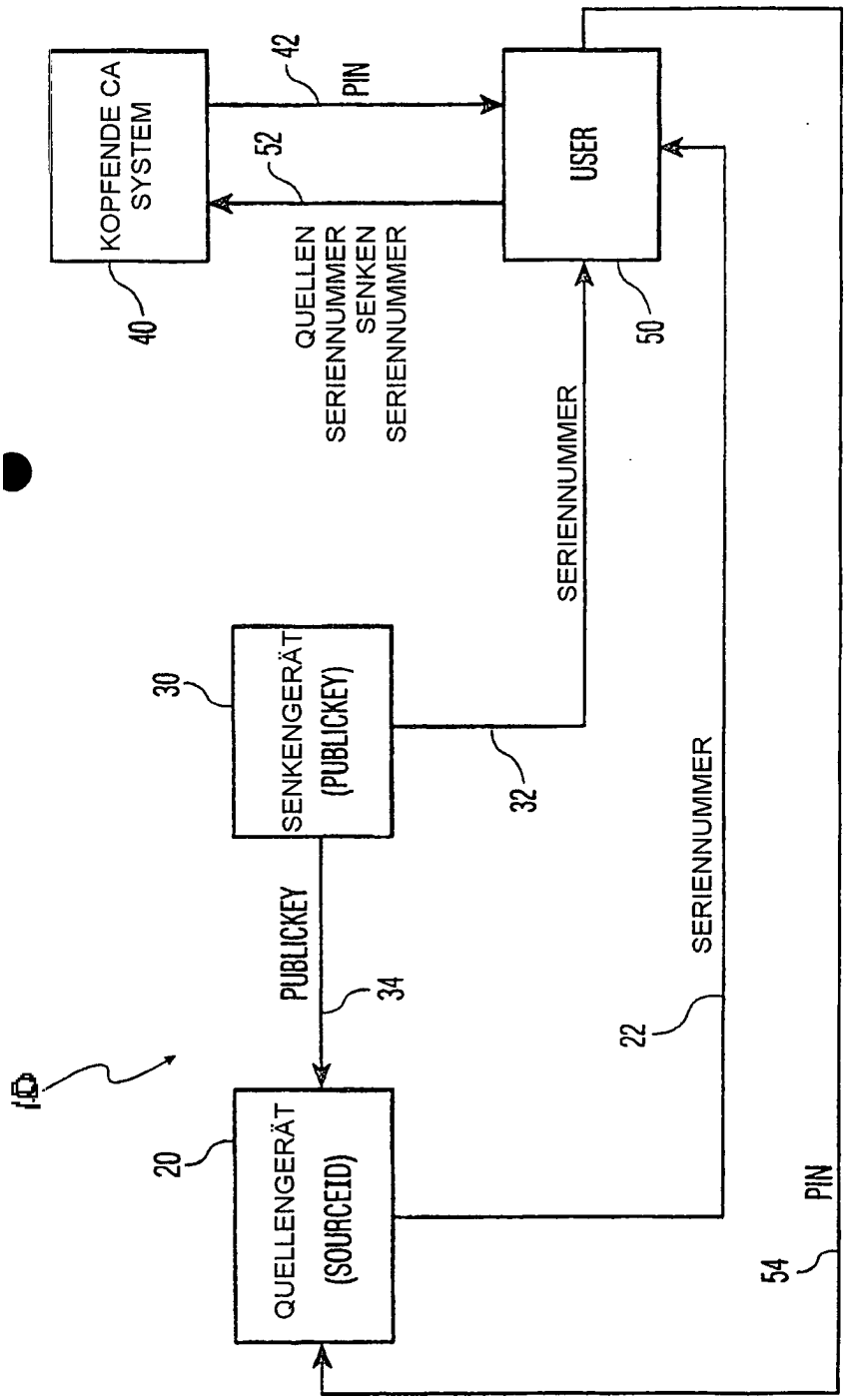

FIG. 1

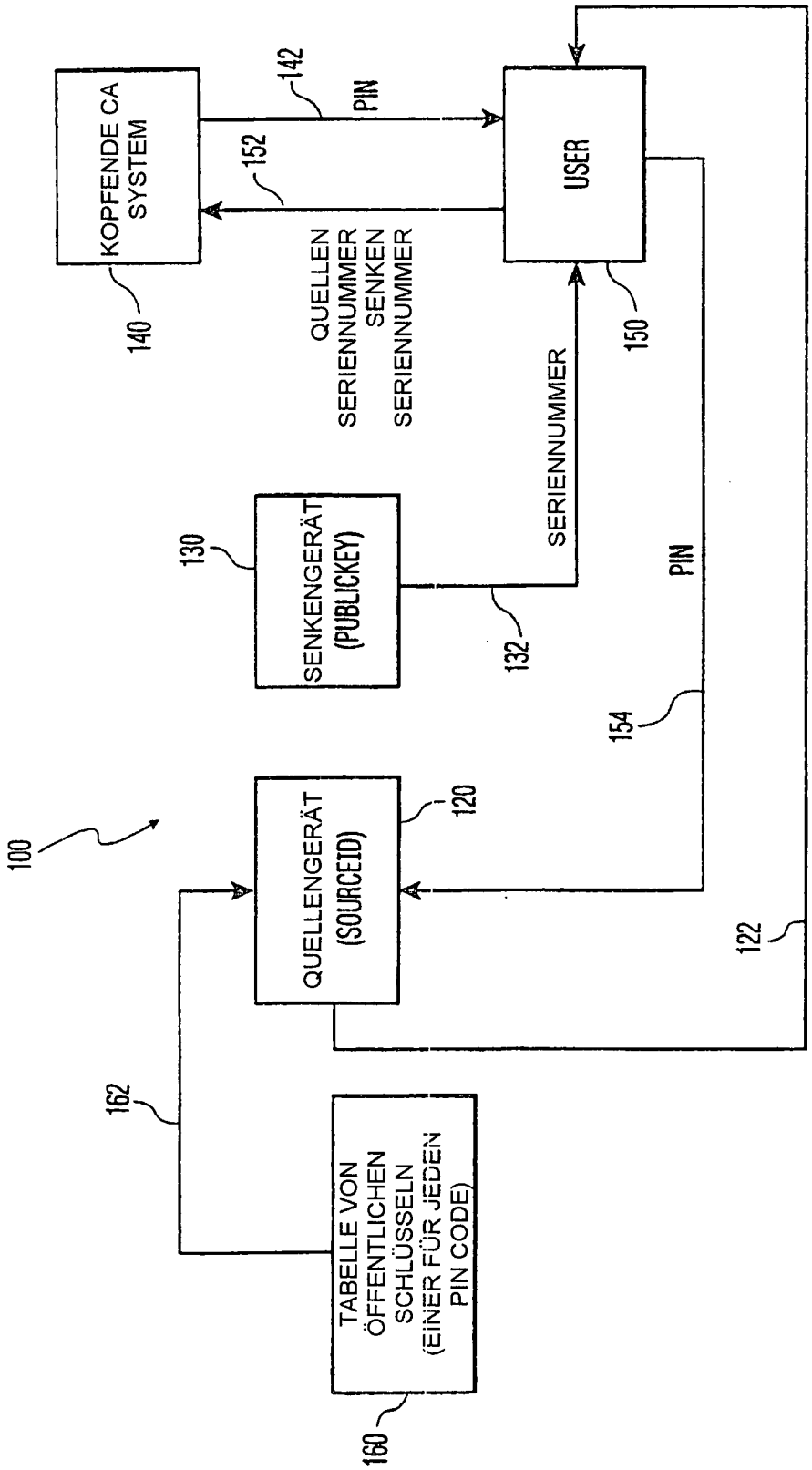
KOPFENDE CA SYSTEM
140
142
PIN
152
QUELLEN SERIENNUMMER
SENKEN SERIENNUMMER
USER
150
SERIENNUMMER
130
SENKENGERÄT (PUBLICKEY)
132
PIN
154
100
QUELLENGERÄT (SOURCEID)
120
122
162
TABELLE VON ÖFFENTLICHEN SCHLÜSSELN (EINER FÜR JEDEN PIN CODE)
160

FIG. 2