(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 60 2004 005 219 T2** 2007.06.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 661 355 B1**
(21) Deutsches Aktenzeichen: **60 2004 005 219.1**
(86) PCT-Aktenzeichen: **PCT/US2004/002407**
(96) Europäisches Aktenzeichen: **04 705 725.2**
(87) PCT-Veröffentlichungs-Nr.: **WO 2005/020541**
(86) PCT-Anmeldetag: **27.01.2004**
(87) Veröffentlichungstag der PCT-Anmeldung: **03.03.2005**
(97) Erstveröffentlichung durch das EPA: **31.05.2006**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **07.03.2007**
(47) Veröffentlichungstag im Patentblatt: **28.06.2007**

(51) Int Cl.[8]: ***H04L 29/06*** (2006.01)
G06F 1/00 (2006.01)

(30) Unionspriorität:
494836 P **13.08.2003** **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., 30457 Hannover

(72) Erfinder:
ZHANG, Junbiao, Bridgewater, NJ 08807, US; LI, Jun, Plainsboro, NJ 08536, US; RAMASWAMY, Kumar, Princeton, NJ 08540, US

(54) Bezeichnung: **VERFAHREN UND EINRICHTUNG ZUR SICHERUNG DER INHALTSABLIEFERUNG ÜBER EIN KOMMUNIKATIONSNETZ ÜBER INHALTSSCHLÜSSEL**

Beschreibung

Technisches Gebiet

[0001] Die vorliegende Anmeldung betrifft allgemein den elektronischen Datentransfer und insbesondere Verfahren zum Sichern elektronischer Informationen in einer Vernetzungsumgebung.

Allgemeiner Stand der Technik

[0002] Beim Abliefern von Multimedia-Inhalt über einen Netzwerkbetrieb kann ein Benutzer oder Inhaltsanforderer (CR) eine Einrichtung wie etwa ein Mobiltelefon oder einen persönlichen Datenassistenten (PDA) bedienen, um eine Anforderung zu einem Inhaltsserver (CS) zu senden, die den Inhaltsserver dafür authorisiert, sofort die angeforderten Daten, Informationselemente oder den angeforderten Inhalt herunterzuladen. In einem anderen Aspekt kann der CR von dem CS anfordern, die angeforderten Daten, Informationselemente oder den angeforderten Inhalt zu einem eingeplanten Zeitpunkt herunterzuladen. Weiterhin kann der CR anfordern, daß die Daten, Informationselemente oder der Inhalt zu einer zweiten Einrichtung, d.h. einem Inhaltsempfänger oder -verbraucher (CC) sofort oder zu einem eingeplanten Zeitpunkt heruntergeladen werden. Dieser letztere Vorgang ist geeignet, wenn die CR-Einrichtung in einem Netzwerk niedriger Bandbreite betrieben wird und nicht genug Bandbreite zum Herunterladen der erforderlichen Informationen besitzt. Zum Beispiel kann ein Benutzer eine zellulare Einrichtung verwenden, die über ein langsames Netzwerk arbeitet, um Audio- und/oder visuelle (Multimedia-)Informationen, die zu einer Empfangseinrichtung wie etwa einem Haus- oder Laptop-Computer abzuliefern sind, anzufordern. In WO 02/47356A und WO 01/59549A wird der verschlüsselte Inhalt von dem Inhaltsanbieter vor der Authentifikationsprozedur an den Inhaltsverbraucher abgeliefert.

[0003] Bevor der CS die angeforderten Informationen liefert, müssen CR und/oder CC jedoch authorisiert werden, jeweils die gewünschten Informationen anzufordern und/oder zu empfangen.

[0004] Folglich werden Einrichtungen benötigt, die Media-Inhalt besser vor unbefugtem Zugriff sowie vor Zugriff von unbefugten Teilnehmern sichert.

Kurzfassung

[0005] Es wird ein Verfahren zum Entwürfeln von über ein Netzwerk empfangenem sicherem Inhalt offengelegt. Bei einer Ausführungsform ist das Verfahren in einer Empfangseinrichtung, die sich an einem abgesetzten Standort in Kommunikation mit einem Netzwerk befindet, für folgendes betreibbar: Empfangen eines ersten Informationselements, das unter Verwendung eines dem abgesetzten Standort bekannten Verschlüsselungsschlüssels verwürfelt wird, Entwürfeln des ersten Informationselements unter Verwendung eines entsprechenden Entschlüsselungsschlüssels, wobei das Informationselement einen Zugangscode und einen Inhaltsschlüssel enthält, Empfangen eines zweiten Informationselements, das unter Verwendung des Inhaltsverschlüsselungsschlüssels verwürfelt wird, nachdem der Server, der für die zweiten Informationen Host ist, den Zugangscode verifiziert und Entwürfeln des zweiten Informationselements unter Verwendung des Inhaltsschlüssels. In einem anderen Aspekt der Erfindung ist ein Ort des gewünschten Inhalts in dem ersten Informationselement enthalten. Der Ort kann auch unter Verwendung des Schlüssels verschlüsselt werden.

Kurze Beschreibung der Zeichnungen

[0006] Fig. 1 zeigt ein Diagramm eines beispielhaften Inhaltsablieferrahmens;

[0007] Fig. 2 zeigt einen beispielhaften Prozeß zum Bereitstellen von sicherer Inhaltsablieferung für den in Fig. 1 gezeigten Ablieferrahmen;

[0008] Fig. 3 zeigt ein Diagramm eines weiteren beispielhaften Inhaltsablieferrahmens;

[0009] Fig. 4 zeigt einen beispielhaften Prozeß zur Bereitstellung von sicherer Inhaltsablieferung in dem in Fig. 3 gezeigten Inhaltsablieferrahmen;

[0010] Fig. 5 zeigt ein Flußdiagramm eines Prozesses zum Verwürfeln von Inhaltsinformationen, die gemäß einem Aspekt der Erfindung gesichert werden;

[0011] Fig. 6 zeigt ein Flußdiagramm eines Prozesses zum Entwürfeln von sicheren Inhaltsinformationen gemäß einem Aspekt der Erfindung; und

[0012] Fig. 7 zeigt eine Einrichtung zum Ausführen des hier gezeigten Prozesses.

[0013] Es versteht sich, daß diese Zeichnungen lediglich zum Zwecke der Veranschaulichung der Konzepte der Erfindung dienen und nicht als Definition der Grenzen der Erfindung bestimmt sind. Die in Fig. 1–Fig. 7 gezeigten und in der beigefügten ausführlichen Beschreibung beschriebenen Ausführungsformen sollen als veranschaulichende Ausführungsformen verwendet werden und nicht als die einzige Art der Ausübung der Erfindung aufgefaßt werden. Außerdem wurden zum Identifizieren ähnlicher Elemente dieselben Bezugszahlen verwendet, möglicherweise gegebenenfalls durch Bezugszeichen ergänzt.

Ausführliche Beschreibung

[0014] Fig. 1 zeigt ein Diagramm der Kommunikation eines Inhaltsablieferrahmens **100** mit einem Inhaltsanforderer (CR) **110**, der sich durch das Netzwerk **130** in Kommunikation mit dem Inhaltsserver (CS) **120** befindet. Der CS **120** kommuniziert ferner durch das Netzwerk **140** mit dem Inhaltsverbraucher **150**. Bei einer beispielhaften Konfiguration kann es sich bei dem Netzwerk **130** um ein langsames Netzwerk handeln, während das Netzwerk **140** ein schnelles Netzwerk sein kann. Bei einer anderen Konfiguration kann es sich bei dem Netzwerk **130** und **140** um dasselbe Netzwerk oder um verschiedene Netzwerke vergleichbarer Geschwindigkeiten handeln. Bei einer Ausführungsform kann der CR **110** ein Mobiltelefon und das Netzwerk **130** ein relativ langsames drahtloses Netzwerk sein. Das Netzwerk **140** kann ein schnelles Netzwerk sein, wie etwa das Internet oder ein spezialisiertes Inhaltsabliefernetzwerk (CDN). Bei einer anderen Ausführungsform kann es sich bei dem CR **110** um einen Laptop-Computer handeln und das Netzwerk **130** kann ein mit dem Internet, das durch das Netzwerk **140** repräsentiert werden kann, verbundenes lokales Netzwerk sein.

[0015] Fig. 2 zeigt eine beispielhafte Funktionsweise **200** zum Bereitstellen von sicherer Inhaltsablieferung über die in

[0016] Fig. 1 gezeigte Netzwerkkonfiguration. Bei dieser beispielhaften Funktionsweise erzeugt der CR **110** eine Anforderung von Informationsinhalt, die als Pfeil **210** gezeigt ist, an den CS **120** über das Netzwerk **130**. Bei einer beispielhaften Ausführungsform kann die Anforderung **210** einen mit dem Inhaltsverbraucher (CC) **150** assoziierten Verschlüsselungsschlüssel enthalten. Wenn zum Beispiel der CC **150** Verschlüsselung mit öffentlichen/privaten Schlüsseln verwendet, kann der öffentliche Schlüssel des CC **150** mit der Bezeichnung Pu dem CS **120** zugeführt werden. Außerdem kann man mit digitalen Zertifikaten verifizieren, daß der Inhaltsanforderer **110** dafür authorisiert ist, auf den CS **120** zuzugreifen. In einem anderen Aspekt kann es sich bei dem Schlüssel P_u um einen Schlüsselwert handeln, der dem CS **120** und dem CC **150** bekannt ist oder den sie sich teilen.

[0017] Der bereitgestellte Verschlüsselungsschlüssel kann selbst unter Verwendung eines Schlüssels, der sowohl CR **110** als auch CS **120** bekannt ist oder von ihnen geteilt wird, verwürfelt oder verschlüsselt werden. Die Verwendung eines gemeinsam benutzten Schlüssels mit der Bezeichnung So und der Repräsentation durch den Pfeil **210** stellt dem CS **120** sicher, daß der CR **110** authorisiert ist, eine Anforderung zu stellen. In einem Aspekt kann dem CR **110** der gemeinsam benutzte Schlüssel So bei der Registration für den durch den CS **120** bereitgestellten Dienst zugeführt werden. In einem Aspekt kann der CR **110** unter Verwendung einer gesicherten Verbindung mit dem CS **120** kommunizieren, die durch Senden eines herkömmlichen Benutzernamens und eines Paßworts zu dem CS **120** aufgebaut werden kann. Als Reaktion kann der CS **120** dem Benutzer CR **110** den gemeinsam benutzten Schlüssel So zuführen. Außerdem kann in der Anforderung ein Verweis auf den gekennzeichneten CC **150**, z.B. eine Internet-Protokoll-Adresse oder ein Ort usw. enthalten sein.

[0018] Nachdem er authentifiziert, daß der CR **110** authorisiert ist, die Anforderung **310** zu stellen, erzeugt der CS **120** einen Inhaltszugriffs-Berechtigungsnachweis (CAC) oder Zugangscode für den gekennzeichneten Inhaltsverbraucher. Der CAC dient zum Zugriff auf den angeforderten Inhalt durch den gekennzeichneten CC **150** zu einem späteren Zeitpunkt. Eine als Pfeil **220** repräsentierte Benachrichtigung wird dem CC **150** zugeführt. In diesem Fall enthält die Benachrichtigung **220** den CAC und einen Inhaltsschlüssel mit der Bezeichnung K_c. Der Schlüssel K_c dient zum Verwürfeln oder Verschlüsseln des angeforderten Inhalts. Der CAC und K_c werden unter Verwendung des mit dem CC **150** assoziierten Schlüssels P_u, der in diesem beispielhaften Fall von dem CR **110** bereitgestellt wurde, verschlüsselt. Eine als LIC repräsentierte Benutzungsbegrenzung oder Lizenz kann außerdem mit dem Inhaltsschlüssel K_c assoziiert werden. In diesem Fall kann die Lizenz LIC begrenzen, wie oft oder wie lange dieser Schlüssel K_c gültig gemacht wird.

[0019] Eine solche Benutzungsbegrenzung für den Schlüssel K_c liefert ein Mittel zum Begrenzen der nachfolgenden Verteilung des Inhalts.

[0020] Der CC **150** entschlüsselt oder entwürfelt die Benachrichtigungsnachricht, um den CAC und den Schlüssel K_c zu erhalten, unter Verwendung des mit dem Schlüssel P_u assoziierten Entschlüsselungsschlüssels. Dann wird der CAC wie als Pfeil **225** gezeigt zu dem CS **120** gesendet, um die Übertragung oder das Herunterladen des angeforderten Informationselements zu authorisieren. In dieser dargestellten Sequenz wird das Herunterladen des Inhalts durch den Pfeil **230** repräsentiert. Nach dem Empfang wird das Informationselement wie durch den Pfeil **240** repräsentiert unter Verwendung des bereitgestellten Schlüssels K_c entwürfelt oder entschlüsselt. Der CC **150** kann nun den von dem CC **110** angeforderten entwürfelten Inhalt betrachten. Wie für Fachleute bekannt wäre, dient der Schlüssel K_c zum Verschlüsseln und Entschlüsseln des bereitgestellten Inhalts und kann somit als ein Verschlüsselungsschlüssel, ein Entschlüsselungsschlüssel oder als ein Inhaltsablieferschlüssel bezeichnet werden.

[0021] Obwohl die hier beschriebene Sequenz eine relativ sofortige Übertragung des angeforderten In-

halts ermöglicht, ist für Fachleute erkennbar, daß die Übertragung des CAC von CS **120** zu einem vorbestimmten Zeitpunkt auftreten kann, oder mit einer vorbestimmten Verzögerung, die von dem Zeitpunkt des Stellens der anfänglichen Anforderung berechnet wird. Die Übertragung des CAC von dem CC **150** zu dem CS **120** kann automatisch oder manuell durchgeführt werden. Im manuellen Fall kann ein Benutzer eine Aktion auf dem CC **150** einleiten, um die Übertragung des CAC zu verursachen. Ähnlich kann der CS **120** die Übertragung des CAC und des Inhaltsschlüssels K_c bis zu einem bekannten Zeitpunkt oder bis nach dem Vergehen eines bekannten Zeitoffsets verzögern.

[0022] Fig. 3 zeigt ein Diagramm eines Inhaltsablieferrahmens **300** gemäß einem Aspekt der vorliegenden Erfindung. In diesem beispielhaften Fall kommunizieren wie zuvor beschrieben CR **110** und CS **120** über das Netzwerk **130**. Außerdem kommuniziert der CS **120** über das Netzwerk **150** mit dem CDN-Makler **310**, und der CDN-Makler **310** kann ferner über das Netzwerk **330** mit einem oder mehreren Edge-Servern, die durch EX **320** repräsentiert werden, kommunizieren. Ferner hat der CC **150** in diesem beispielhaften Fall Zugang zu mindestens einem Netzwerk **330**. Wie zuvor besprochen, kann es sich bei den Netzwerken **130**, **140** und **330** um Netzwerke handeln, die verschiedene, dieselbe oder vergleichbare Datenübertragungsraten aufweisen. Zum Beispiel kann das Netzwerk **130** ein langsames Netzwerk mit niedriger Bandbreite sein und die Netzwerke **140** und **130** können schnelle Netzwerke mit großer Bandbreite sein. Ferner kann das Netzwerk **130** ein spezialisiertes Inhaltsabliefernetzwerk (CDN) repräsentieren. Wie für Fachleute erkennbar ist, kann es sich bei dem Netzwerk **130**, **140** und **330** auch um dasselbe Netzwerk handeln. Die gezeigte CDN-Konfiguration und die Verwendung des CDN-Maklers **310** ermöglicht es dem System, angeforderten Inhalt zu anderen Edge-Servern zu verteilen, als sich lokal bei einer Vielzahl von Benutzern, die denselben Inhalt anfordern können, befinden können.

[0023] Fig. 4 zeigt eine beispielhafte chronologische Sequenz **400** zum Bereitstellen sicherer Inhaltsablieferung über die in Fig. 3 gezeigte Netzwerkkonfiguration. In dieser Sequenz fordert der CR **110** wie durch den Pfeil **210** repräsentiert an, daß der CS **120** dem CC **150** wie zuvor besprochen gekennzeichneten Inhalt zuführt. Der Inhaltsserver **120** erhält Informationen bezüglich eines gekennzeichneten ES in Assoziation mit dem CC **150** aus dem CDN-Makler **310**. Ferner erzeugt der CS **120** einen CAC und erzeugt einen Cache-Inhaltszugriffs-Berechtigungsnachweis (CCAC). In einem Aspekt der Erfindung enthält der CAC die Adresse des gekennzeichneten CC **150** und ein Paßwort. Ähnlich enthält der CCAC die Adresse eines gekennzeichneten Edge-Servers (ES) **320** und ein zweites Paßwort. CAC und CCAC werden verschlüsselt und dem CDN-Makler **310** wie durch den Pfeil **410** repräsentiert zugeführt. In diesem Fall werden CAC und CCAC unter Verwendung eines als S_1 bezeichneten Schlüssels, der CS **120** und den CDN-Makler **310** bekannt ist oder von diesen gemeinsam benutzt wird, verschlüsselt. Der CDN-Makler **310** entschlüsselt die gesendeten Informationen und verschlüsselt CAC und CCAC in diesem Fall unter Verwendung eines als S_2 bezeichneten Schlüssels neu. Der Schlüssel S_2 ist dem CDN-Makler **310** und dem ES **320** gemeinsam bzw. wird von ihnen geteilt. Der ES **320** verwendet den CAC zum Zugriff auf den angeforderten Inhalt wie durch den Pfeil **430** repräsentiert, der unter Verwendung eines Inhaltsschlüssels K_c aus dem CS **120** verwürfelt wird. Ferner liefert der CS **120** wie durch den Pfeil **220** eine Benachrichtigung an den CC 150. Ähnlich wie die in Fig. 2 gezeigte enthält die Benachrichtigung **220** Informationen bezüglich den Ort der angeforderten Informationen oder des angeforderten Inhalts, z.B. die Adresse des ES **320**, und den verschlüsselten oder verwürfelten CCAC und Inhaltsschlüssel K_c. Wie zuvor beschrieben, werden CCAC und der Schlüssel K_c unter Verwendung des Schlüssels P_u verschlüsselt, der mit dem CC **150** assoziiert oder diesem bekannt ist. Ferner kann auch der Ort des Inhalts verschlüsselt werden. In einem weiteren Aspekt kann der Ort des Inhalts unverwürfelt bereitgestellt werden.

[0024] Der CC **150** kann dann die Informationen entschlüsseln und den empfangenen CCAC wie durch den Pfeil **340** dargestellt zu dem ES **320** senden. Der CC **150** kann dann den angeforderten oder gewünschten Inhalt, der unter Verwendung des Schlüssels K_c verschlüsselt wurde, wie durch den Pfeil **230'** repräsentiert herunterladen. Der CC **150** kann dann wie zuvor beschrieben den empfangenen Inhalt entschlüsseln. In einem anderen Aspekt der Erfindung kann der Schlüssel K_c mit einer Benutzungsbegrenzungslizenz assoziiert werden, die die Dauer der Gültigkeit des Schlüssels K_c begrenzt.

[0025] Fig. 5 zeigt ein Flußdiagramm eines beispielhaften Prozesses **500** zum Entschlüsseln von angefordertem Inhalt gemäß den Prinzipien der Erfindung. Bei diesem beispielhaften Prozeß wird im Block **510** bestimmt, ob eine Nachricht empfangen wurde. Wenn die Antwort negativ ist, wartet der Prozeß weiter auf den Empfang einer Nachricht. Wenn die Antwort dagegen bestätigend ist, wird die Nachricht unter Verwendung eines privaten Schlüssels im Block **520** entschlüsselt oder entwürfelt. Aus der entschlüsselten Nachricht wird der Inhaltszugangscode und ein Schlüssel K_c erhalten. Zum Beispiel ist mit Bezug auf die in Fig. 2 gezeigte Sequenz der Inhaltszugangsschlüssel oder -code der erzeugte CAC, während mit Bezug auf Fig. 3 der Inhaltszugangsschlüssel oder -code der erzeugte CCAC ist.

[0026] In einem Aspekt der Erfindung kann auch der Ort des gewünschten Inhalts in die Nachricht aufgenommen werden. Der Ort kann im Klartext bereitgestellt oder verwürfelt werden. In einem Aspekt der Erfindung kann der Inhaltsort dem CC **150** bekannt sein und muß somit nicht in der gesendeten Nachricht enthalten sein.

[0027] Im Block **540** wird bestimmt, ob der angeforderte Inhalt heruntergeladen werden soll. Wenn die Antwort negativ ist, wartet der Prozeß im Block **540**, bis eine bestimmte Anzeige, daß Herunterladen gewünscht ist, empfangen wird. Eine Anzeige, daß Herunterladen gewünscht ist, kann zum Beispiel zu einem bekannten Zeitpunkt, zu einem bekannten Zeitoffset von einer angeforderten Zeit oder manuell durch einen Benutzer auftreten. Die bekannte Zeit oder das bekannte Zeitoffset können vom Benutzer während der anfänglichen Anforderung bereitgestellt werden.

[0028] Wenn eine Anzeige empfangen wird, wird der Inhaltszugangsschlüssel (CAC oder CCAC) im Block **550** zu dem bekannten oder spezifizierten Inhaltsort gesendet. Im Block **560** wird der Inhalt empfangen, und im Block **570** wird bestimmt, ob der gesamte Inhalt empfangen wurde. Wenn die Antwort negativ ist, fährt die Verarbeitung im Block **560** weiter mit dem Empfang des gewünschten Inhalts fort. Wenn die Antwort jedoch bestätigend ist, wird der Inhalt unter Verwendung des bereitgestellten Inhaltsschlüssels, d.h. K_c, entschlüsselt.

[0029] Fig. 6 zeigt ein Flußdiagramm eines Prozesses **600** zum Erzeugen von Inhaltsablieferschlüsseln oder -codes gemäß den Prinzipien der Erfindung. In diesem dargestellten Prozeß wird im Block **610** bestimmt, ob eine Nachricht empfangen wurde. Wenn die Antwort negativ ist, wartet der Prozeß weiter auf eine Nachricht.

[0030] Wenn die Antwort dagegen bestätigend ist, wird im Block **620** bestimmt, ob der Absender authorisiert ist, Inhaltsablieferung anzufordern. Wenn die Antwort negativ ist, kehrt der Prozeß zum Block **610** zurück, um weiter auf eine Nachricht zu warten. Wenn die Antwort dagegen bestätigend ist, wird im Block **625** die Anforderrungsnachricht unter Verwendung eines beiden Teilnehmern gemeinsamen Schlüssels entschlüsselt. Die Nachricht enthält Informationen bezüglich des gewünschten Inhalts und kann einen gewünschten Verbraucherort enthalten, wenn der gewünschte Verbraucherort keine bekannte, vorangestellte oder vorbestimmte, z.B. im voraus gekennzeichnete, Adresse ist. Diese Informationen können unverschlüsselt gesendet werden. Dann werden der öffentliche Schlüssel des Verbrauchers oder andere Verschlüsselungsinformationen verschlüsselt gesendet.

[0031] Im Block **630** werden ein Inhaltszugangsschlüssel und ein Inhaltsschlüssel K_c erzeugt und werden unter Verwendung des öffentlichen Schlüssels oder anderer Verschlüsselungsinformationen, die von dem Anforderer oder Benutzer bereitgestellt werden, verschlüsselt. Die verschlüsselten Informationen werden über eine Benachrichtigungsnachricht im Block **340** zu dem Verbraucher gesendet.

[0032] Im Block **650** wird bestimmt, ob der gewünschte Inhalt an einem dem Verbraucher bekannten Ort gespeichert oder geführt wird, d.h. der Inhaltsort vordefiniert oder vorbestimmt ist. Wenn die Antwort bestätigend ist, wird die Verarbeitung abgeschlossen. Wenn die Antwort dagegen negativ ist, wird der Ort des Inhalts unter Verwendung des bereitgestellten öffentlichen Schlüssels oder der anderen Verschlüsselungsinformationen im Block **660** verschlüsselt und im Block **665** zu dem Verbraucher gesendet.

[0033] Im Block **670** wird der Inhaltszugangsschlüssel oder -code unter Verwendung eines Verschlüsselungsschlüssels, der zwischen dem Inhaltsserver und dem Edge-Server, der den gewünschten Inhalt enthält oder enthalten wird, bekannt ist, verschlüsselt. Im Block **680** wird der Inhalt unter Verwendung des Inhaltsablieferschlüssels K_c verschlüsselt. Die Verwendung des Schlüssels K_c zum Verwürfeln des Inhalts ist vorteilhaft, da der Server keine zusätzliche Sicherheitsebenen erfordert, um einen unbefugten Zugriff auf den Inhalt zu verhindern. Das Speichern der Medien unter Verwendung des Schlüssels K_c ist weiterhin vorteilhaft, da es den Inhalt in einer Form speichert, die gleichgültig, ob der Inhaltsserver oder ein Edge-Server den Inhalt abliefert, für den Verbraucher transparent ist. Im Block **685** wird der Inhalt zu dem Ort des Verbrauchers oder Benutzers gesendet. Für Fachleute ist erkennbar, daß der in Fig. 5 gezeigte Prozeß insbesondere die in Fig. 4 gezeigte Sequenz betrifft, die gegenüber den in Fig. 1 gezeigten zusätzliche Prozeßsequenzschritte enthält. Es versteht sich jedoch auch, daß der Prozeß **600** auch die in Fig. 1 gezeigten Sequenzschritte betreffen kann, wenn der Ort des des Inhalts dem Verbraucher bekannt ist.

[0034] Fig. 7 zeigt ein System **700** zum Implementieren der Prinzipien der Erfindung, so wie sie in der in Fig. 2–Fig. 4 gezeigten beispielhaften Verarbeitung abgebildet ist. Bei dieser beispielhaften Systemausführungsform **700** werden Eingangsdaten aus Quellen **705** über das Netzwerk **750** empfangen und gemäß einem oder mehreren Programmen (entweder Software oder Firmware), die von dem Verarbeitungssystem **710** ausgeführt werden, verarbeitet. Die Ergebnisse des Verarbeitungssystems **710** können dann zur Betrachtung auf dem Display **780**, der Meldeeinrichtung **790** und/oder einem zweiten Verarbeitungssystem **795** über das Netzwerk **770** übertragen

werden.

[0035] Genauer gesagt enthält das Verarbeitungssystem **710** eine oder mehrere Eingangs-/Ausgangseinrichtungen **740**, die Daten über das Netzwerk **750** von den dargestellten Quelleneinrichtungen **705** empfangen. Die empfangenen Daten werden dann an den Prozessor **720** angelegt, der mit der Eingangs-/Ausgangseinrichtung **740** und dem Speicher **730** kommuniziert. Die Eingangs-/Ausgangseinrichtungen **740**, der Prozessor **720** und der Speicher **730** können über ein Kommunikationsmedium **725** kommunizieren. Das Kommunikationsmedium **725** kann ein Kommunikationsnetzwerk repräsentieren, z.B. einen ISA-, PCI-, PCMCIA-Bus, eine oder mehrere interne Verbindungen einer Schaltung, einer Schaltungskarte oder einer anderen Einrichtung, sowie Teile und Kombinationen dieser und anderer Kommunikationsmedien.

[0036] Das Verarbeitungssystem **710** und/oder der Prozessor **720** können einen in der Hand gehaltenen Rechner, ein spezielles oder Vielzweck-Verarbeitungssystem, einen Desktop-Computer, einen Laptop-Computer, einen Palm-Computer oder eine Einrichtung eines persönlichen digitalen Assistenten (PDA) sowie Teile oder Kombinationen dieser oder anderer Einrichtungen repräsentieren, die die dargestellten Operationen durchführen können.

[0037] Der Prozessor **720** kann eine zentrale Verarbeitungseinheit (CPU) sein oder speziell zugeordnete Hardware/Software, wie zum Beispiel ein PAL, ASIC, FGPA, die betreibbar ist, um Computeranweisungscode oder eine Kombination aus Code und möglichen Operationen auszuführen. Bei einer Ausführungsform kann der Prozessor **720** Code enthalten, der, wenn er ausgeführt wird, die hier dargestellten Operationen durchführt. Der Code kann im Speicher **730** enthalten sein, aus einem Speichermedium, wie zum Beispiel einer CD-ROM oder Diskette mit der Darstellung als **783**, gelesen oder heruntergeladen werden, kann durch eine manuelle Eingabeeinrichtung **785**, wie etwa eine Tastatur oder ein Eingabetastenfeld bereitgestellt werden oder kann aus einem (nichtgezeigten) magnetischen oder optischen Medium gegebenenfalls gelesen werden. Von der Eingabeeinrichtung **783**, **785** und/oder dem magnetischen Medium bereitgestellte Informationselemente können wie gezeigt durch die Eingangs- /Ausgangseinrichtung **740** dem Prozessor **720** zugänglich sein. Ferner können die von der Eingangs-/Ausgangseinrichtung **740** empfangenen Daten unmittelbar dem Prozessor **720** zugänglich oder in den Speicher **730** gespeichert sein. Der Prozessor **720** kann ferner die Ergebnisse der Verarbeitung dem Display **780**, der Aufzeichnungseinrichtung **790** oder einer zweiten Verarbeitungseinheit **795** zuführen.

[0038] Für Fachleute ist erkennbar, daß die Begriffe Prozessor, Verarbeitungssystem, Computer oder Computersystem eine oder mehrere Verarbeitungseinheiten repräsentieren können, die mit einer oder mehreren Speichereinheiten und anderen Einrichtungen, z.B. Peripheriegeräten, die elektronisch mit der mindestens einen Verarbeitungseinheit verbunden sind und mit ihr kommunizieren, kommunizieren. Ferner können die dargestellten Einrichtungen elektronisch über interne Busse, z.B. serieller, paralleler, ISA-Bus, Mikrokanal-Bus, PCI-Bus, PCMCIA-Bus, USB, usw. oder eine oder mehrere interne Verbindungen einer Schaltung, Schaltungskarte oder einer anderen Einrichtung sowie durch Teile oder Kombinationen dieser und anderer Kommunikationsmedien oder ein externes Netzwerk z.B. das Internet und Intranet, mit einer oder mehreren Verarbeitungseinheiten verbunden sein. Bei anderen Ausführungsformen können anstelle von oder in Kombination mit Softwareanweisungen zur Implementierung der Erfindung Hardwareschaltkreise verwendet werden. Zum Beispiel können die hier dargestellten Elemente auch als diskrete Hardwareelemente implementiert oder auf eine einzige Einheit integriert werden.

[0039] Es versteht sich, daß die dargestellten Operationen sequenziell oder parallel unter Verwendung verschiedener Prozessoren zur Bestimmung spezifischer Werte durchgeführt werden können. Das Verarbeitungssystem **710** kann sich auch in bidirektionaler Kommunikation mit jeder der Quellen **705** befinden. Das Verarbeitungssystem **710** kann ferner Daten über eine oder mehrere Netzwerkverbindungen von einem Server oder Servern z.B. über ein globales Computerkommunikationsnetz wie etwa das Internet, Intranet oder großflächiges Netzwerk (WAN), ein städtisches Netzwerk (MAN), ein lokales Netzwerk (LAN), ein terrestrisches Ausstrahlungssystem, ein Kabelnetzwerk, ein Satellitennetzwerk, ein drahtloses Netzwerk oder ein Fernsprechnetzwerk (POTS) sowie über Teile oder Kombinationen dieser und anderer Arten von Netzwerken Daten empfangen oder senden. Es versteht sich, daß die Netzwerke **750** und **770** auch interne Netzwerke oder eine oder mehrere interne Verbindungen einer Schaltung, Schaltungskarte oder einer anderen Einrichtung sowie von Teilen und Kombinationen dieser und anderer Kommunikationsmedien oder externer Netzwerke, z.B. des Internets und Intranets, sein können.

[0040] Es wurden hier grundsätzliche neuartige Merkmale der vorliegenden Erfindung, so wie sie für bevorzugte Ausführungsformen dieser gelten, gezeigt, beschrieben und herausgestellt. Es versteht sich aber, daß verschiedene Auslassungen und Substitutionen und Änderungen an den beschriebenen Vorrichtungen, der Form und den Einzelheiten der offengelegten Einrichtungen und ihrer Funktionsweise von Fachleuten vorgenommen werden können, ohne von dem Gedanken der vorliegenden Erfindung abzuweichen. Obwohl die vorliegende Erfindung in Be-

zug auf die Sicherung von Multimediainhalt offengelegt wurde, ist für Fachleute erkennbar, daß die hier beschriebenen Verfahren und Einrichtungen auf beliebige Informationen angewandt werden können, die sichere Übertragung und authorisierten Zugang erfordern. Es ist ausdrücklich beabsichtigt, daß alle Kombinationen der Elemente, die im wesentlichen dieselbe Funktion auf im wesentlichen dieselbe Weise durchführen, um dieselben Ergebnisse zu erzielen, in den Schutzumfang der Erfindung fallen. Substitutionen von Element von einer beschriebenen Ausführungsform zu einer anderen werden auch vollständig beabsichtigt und in Betracht gezogen.

Patentansprüche

1. Einrichtung (**150**), die sich an einem abgesetzten Standort in Kommunikation mit einem Netzwerk mit mindestens einem Server (**120**) befindet, umfassend:
einen mit einem Speicher kommunizierenden Prozessor, wobei der Prozessor betreibbar ist, um Code für folgendes auszuführen:
Empfangen eines ersten Informationselements, das einen Zugangscode und einen Inhaltsschlüssel umfaßt, der unter Verwendung eines dem abgesetzten Standort bekannten Verschlüsselungsschlüssels verwürfelt wird, wobei der Zugangscode als Reaktion auf eine Anforderung eines zweiten Informationselements durch einen Inhaltsanforderer (**110**) erzeugt wird;
Entwürfeln des ersten Informationselements unter Verwendung eines entsprechenden Entschlüsselungsschlüssels;
Senden des Zugangscodes zu einem Server, der für das zweite Informationselement Host ist; und
Empfangen des unter Verwendung des Inhaltsschlüssels verwürfelten zweiten Informationselements, nachdem der Server, der für das zweite Informationselement Host ist, den Zugangscode verifiziert.

2. Einrichtung nach Anspruch 1, wobei der Prozessor ferner betreibbar ist, um Code für folgendes auszuführen:
Entwürfeln des zweiten Informationselements unter Verwendung des Inhaltsschlüssels.

3. Einrichtung nach Anspruch 1, wobei das erste Informationselement eine Benutzungsbegrenzungsangabe enthält.

4. Einrichtung nach Anspruch 1, wobei der Prozessor ferner betreibbar ist, um Code für folgendes auszuführen:
Senden des unverschlüsselten Zugangscodes, ausgewählt aus der folgenden Gruppe:
automatisch, zu einem vorbestimmten Zeitpunkt, zu einem vorbestimmten Zeit-Offset, als Reaktion auf eine manuelle Eingabe.

5. Einrichtung nach Anspruch 1, wobei der Inhaltsschlüssel aus der folgenden Gruppe ausgewählt wird:
ein öffentlicher Schlüssel, ein gemeinsam benutzter Schlüssel.

6. Einrichtung nach Anspruch 3, wobei die Benutzungsbegrenzungsangabe aus der folgenden Gruppe ausgewählt wird: Anzahl der Benutzungen, Zeitraum.

7. Einrichtung nach Anspruch 1, wobei das erste Informationselement ferner einen Inhaltsort enthält.

8. Einrichtung nach Anspruch 7, wobei der Prozessor ferner betreibbar ist, um Code zum Senden des Inhaltsorts auszuführen.

9. Einrichtung nach Anspruch 7, wobei der Inhaltsort bekannt ist.

10. Verfahren zum Betrieb in einer Empfangseinrichtung (**150**), die sich an einem abgesetzten Standort in Kommunikation mit einem Netzwerk mit mindestens einem Server (**120**) befindet, zum Entwürfeln von über das Netzwerk empfangenem sicherem Inhalt, mit den folgenden Schritten:
Empfangen eines ersten Informationselements, das einen Zugangscode und einen Inhaltsschlüssel umfaßt, der unter Verwendung eines dem abgesetzten Standort bekannten Verschlüsselungsschlüssels verwürfelt wird, wobei der Zugangscode als Reaktion auf eine Anforderung eines zweiten Informationselements durch einen Inhaltsanforderer (**110**) erzeugt wird;
Entwürfeln des ersten Informationselements unter Verwendung eines entsprechenden Entschlüsselungsschlüssels;
Senden des Zugangscodes zu einem Server, der für das zweite Informationselement Host ist; und
Empfangen des unter Verwendung des Inhaltsschlüssels verwürfelten zweiten Informationselements, nachdem der Server, der für das zweite Informationselement Host ist, den Zugangscode verifiziert; und
Entwürfeln des zweiten Informationselements unter Verwendung des Inhaltsschlüssels.

11. Verfahren nach Anspruch 10, wobei das erste Informationselement eine Benutzungsbegrenzungsangabe enthält.

12. Verfahren nach Anspruch 10, wobei der Inhaltsschlüssel aus der folgenden Gruppe ausgewählt wird: ein öffentlicher Schlüssel, ein gemeinsam benutzter Schlüssel.

13. Verfahren nach Anspruch 11, wobei die Benutzungsbegrenzungsangabe aus der folgenden Gruppe ausgewählt wird: Anzahl der Benutzungen,

Zeitraum.

14. Verfahren nach Anspruch 10, wobei das erste Informationselement ferner einen Inhaltsort enthält.

15. Verfahren nach Anspruch 14, wobei der Inhaltsort bekannt ist.

16. Verfahren zum Transferieren von sicherem Inhalt über ein Netzwerk, mit den folgenden Schritten:
Empfangen einer Anforderung von Inhalt an einem ersten Server (**120**) über ein erstes Netzwerk von einer Dateianforderungseinrichtung (**110**), wobei die Anforderung einen Verschlüsselungsschlüssel enthält, der einem gekennzeichneten abgesetzten Standort bekannt ist;
Erzeugen eines ersten Informationselements, das einen Zugangscode und einen Inhaltsschlüssel enthält, in dem Server als Reaktion auf die Anforderung von Inhalt durch die Dateianforderungseinrichtung;
Transferieren des ersten Informationselements zu dem gekennzeichneten abgesetzten Standort mit einer Dateiempfangseinrichtung (**150**), wobei der Zugangscode und der Inhaltsschlüssel unter Verwendung des Verschlüsselungsschlüssels verwürfelt werden;
Empfangen des Zugangscodes von dem gekennzeichneten abgesetzten Standort mit der Dateiempfangseinrichtung; und
Transferieren des sicheren Inhalts nach der Verifikation des Zugangscodes über ein zweites Netzwerk, wobei der sichere Inhalt unter Verwendung des Inhaltsschlüssels verschlüsselt wird.

17. Verfahren nach Anspruch 16, wobei das erste Netzwerk und das zweite Netzwerk dasselbe Netzwerk sind.

18. Verfahren nach Anspruch 16, wobei die Dateianforderungseinrichtung aus der folgenden Gruppe ausgewählt wird: persönlicher digitaler Assistent, Mobiltelefon, Notebook-Computer und Personal Computer.

19. Verfahren nach Anspruch 16, wobei die Dateiempfangseinrichtung aus der folgenden Gruppe ausgewählt wird: persönlicher digitaler Assistent, Mobiltelefon, Notebook-Computer und Personal Computer.

20. Verfahren nach Anspruch 16, wobei das erste Netzwerk ein drahtloses Netzwerk ist.

21. Verfahren nach Anspruch 16, wobei das erste Informationselement einen Ort des Inhalts enthält.

22. Verfahren nach Anspruch 16, ferner mit dem folgenden Schritt:
Senden des Inhalts zu mindestens einem anderen Server, der mit dem ersten Server kommuniziert, wobei der Inhalt unter Verwendung des Inhaltsschlüssels verwürfelt wird.

23. Verfahren nach Anspruch 22, ferner mit den folgenden Schritten:
Transferieren des sicheren Inhalts über ein zweites Netzwerk nach Verifikation des Zugangscodes, wobei der sichere Inhalt unter Verwendung des Inhaltsschlüssels verwürfelt wird.

24. Verfahren nach Anspruch 16, wobei der Schritt des Transferierens des Zugangscodes und des Inhaltsschlüssels über das erste Netzwerk erfolgt.

25. Verfahren nach Anspruch 16, wobei der Schritt des Transferierens des Zugangscodes und des Inhaltsschlüssels über das zweite Netzwerk erfolgt.

26. Verfahren nach Anspruch 16, wobei das zweite Netzwerk ein schnelles Netzwerk ist.

27. Verfahren nach Anspruch 26, wobei das zweite Netzwerk ein Inhaltsabliefernetzwerk ist.

28. Verfahren nach Anspruch 16, ferner mit dem folgenden Schritt:
Transferieren eines Orts des Inhalts zu dem gekennzeichneten abgesetzten Standort.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

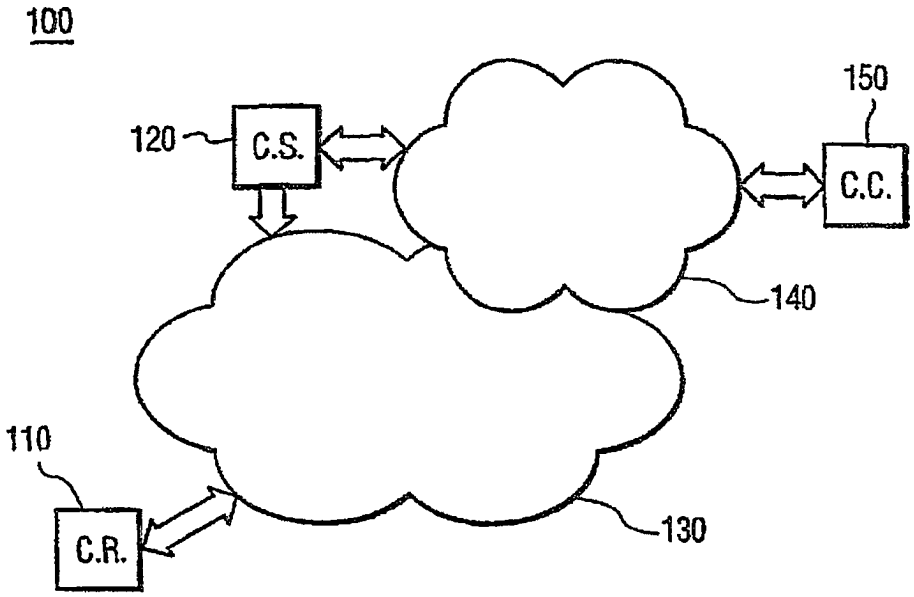

FIG. 1

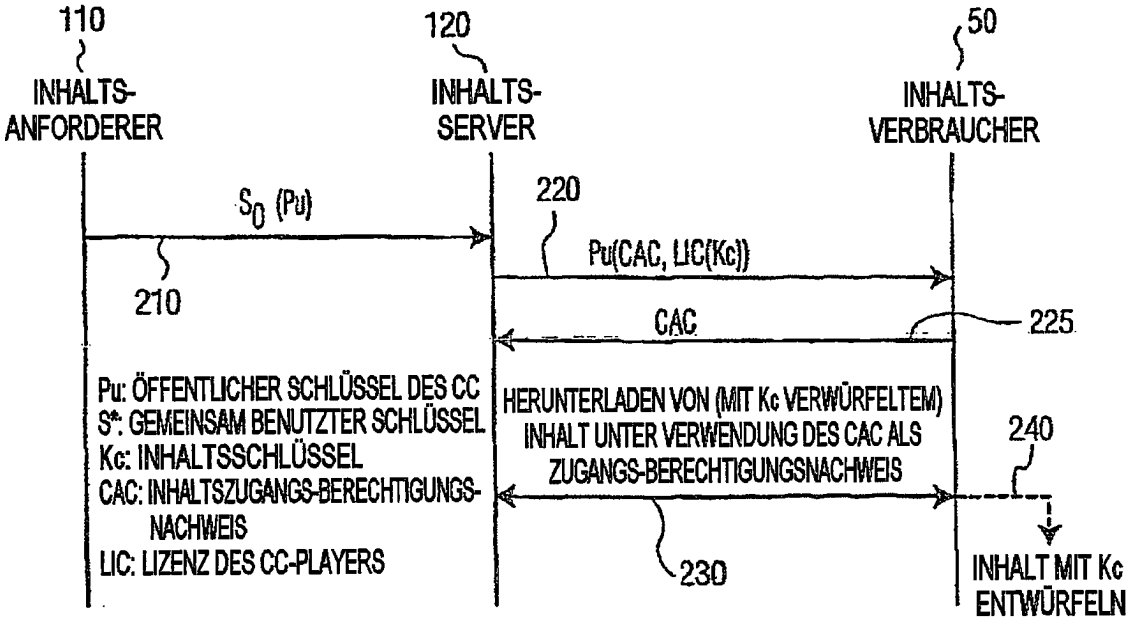

FIG. 2

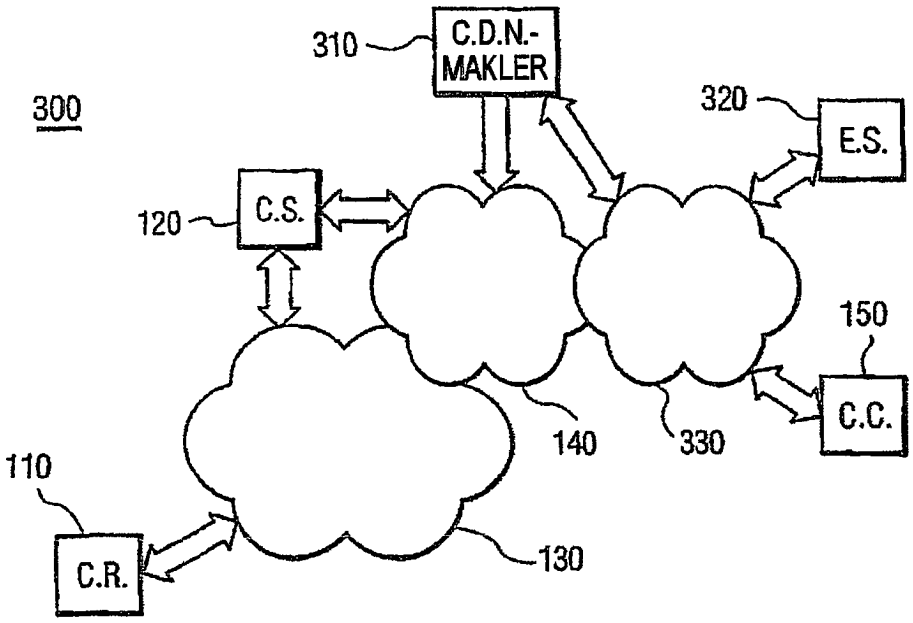

FIG. 3

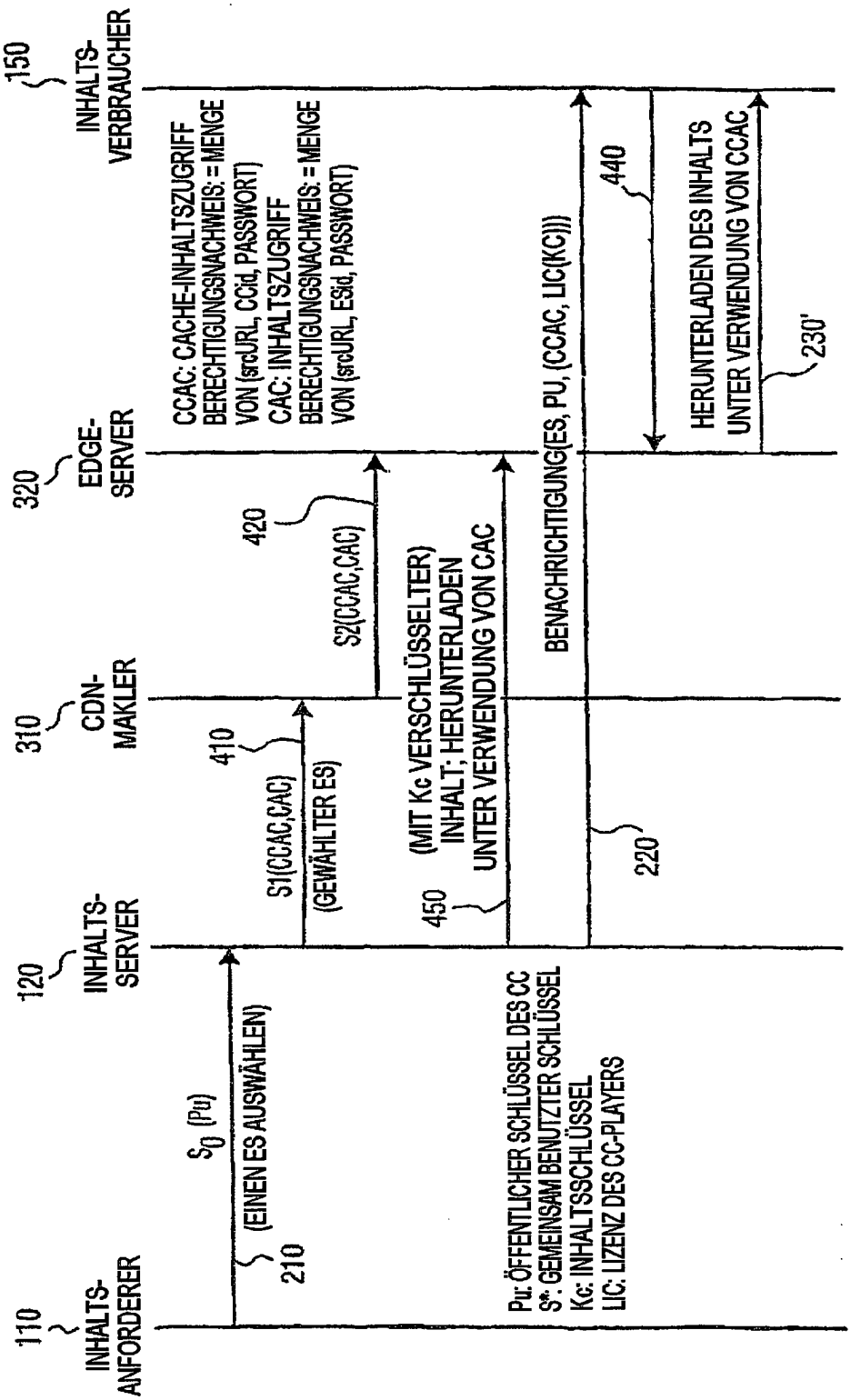
110
INHALTS-ANFORDERER
120
INHALTS-SERVER
310
CDN-MAKLER
320
EDGE-SERVER
150
INHALTS-VERBRAUCHER
210
(EINEN ES AUSWÄHLEN)
S_0 (Pu)
410
S1(CCAC,CAC)
(GEWÄHLTER ES)
420
S2(CCAC,CAC)
450
(MIT Kc VERSCHLÜSSELTER) INHALT; HERUNTERLADEN UNTER VERWENDUNG VON CAC
220
BENACHRICHTIGUNG(ES, PU, (CCAC, LIC(KC)))
440
HERUNTERLADEN DES INHALTS UNTER VERWENDUNG VON CCAC
230'
CCAC: CACHE-INHALTSZUGRIFF BERECHTIGUNGSNACHWEIS: = MENGE VON (srcURL, CCid, PASSWORT)
CAC: INHALTSZUGRIFF BERECHTIGUNGSNACHWEIS: = MENGE VON (srcURL, ESid, PASSWORT)
Pu: ÖFFENTLICHER SCHLÜSSEL DES CC
S*: GEMEINSAM BENUTZTER SCHLÜSSEL
Kc: INHALTSSCHLÜSSEL
LIC: LIZENZ DES CC-PLAYERS

FIG. 4

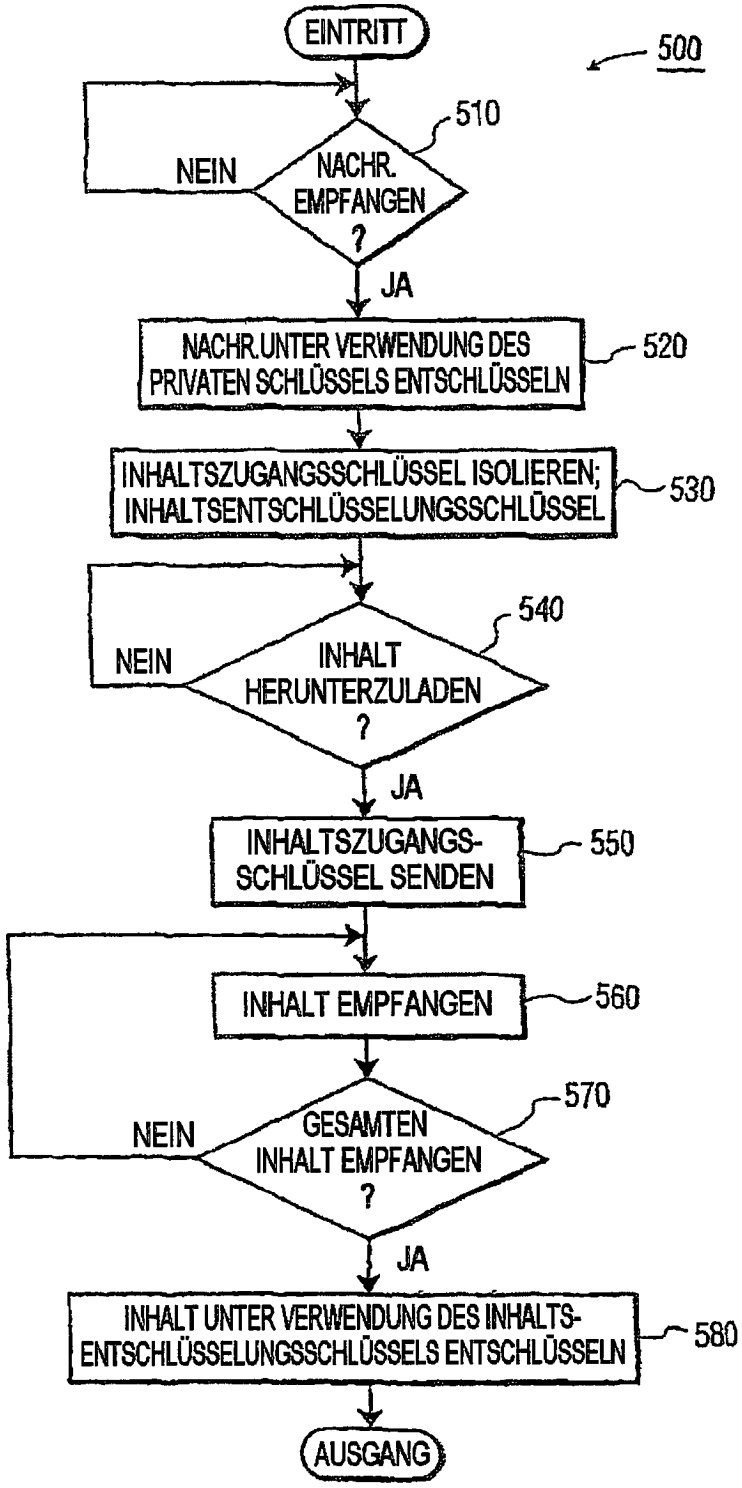
EINTRITT
500
510
NEIN
NACHR. EMPFANGEN ?
JA
NACHR.UNTER VERWENDUNG DES PRIVATEN SCHLÜSSELS ENTSCHLÜSSELN
520
INHALTSZUGANGSSCHLÜSSEL ISOLIEREN; INHALTSENTSCHLÜSSELUNGSSCHLÜSSEL
530
540
NEIN
INHALT HERUNTERZULADEN ?
JA
INHALTSZUGANGS-SCHLÜSSEL SENDEN
550
INHALT EMPFANGEN
560
570
NEIN
GESAMTEN INHALT EMPFANGEN ?
JA
INHALT UNTER VERWENDUNG DES INHALTS-ENTSCHLÜSSELUNGSSCHLÜSSELS ENTSCHLÜSSELN
580
AUSGANG

FIG. 5

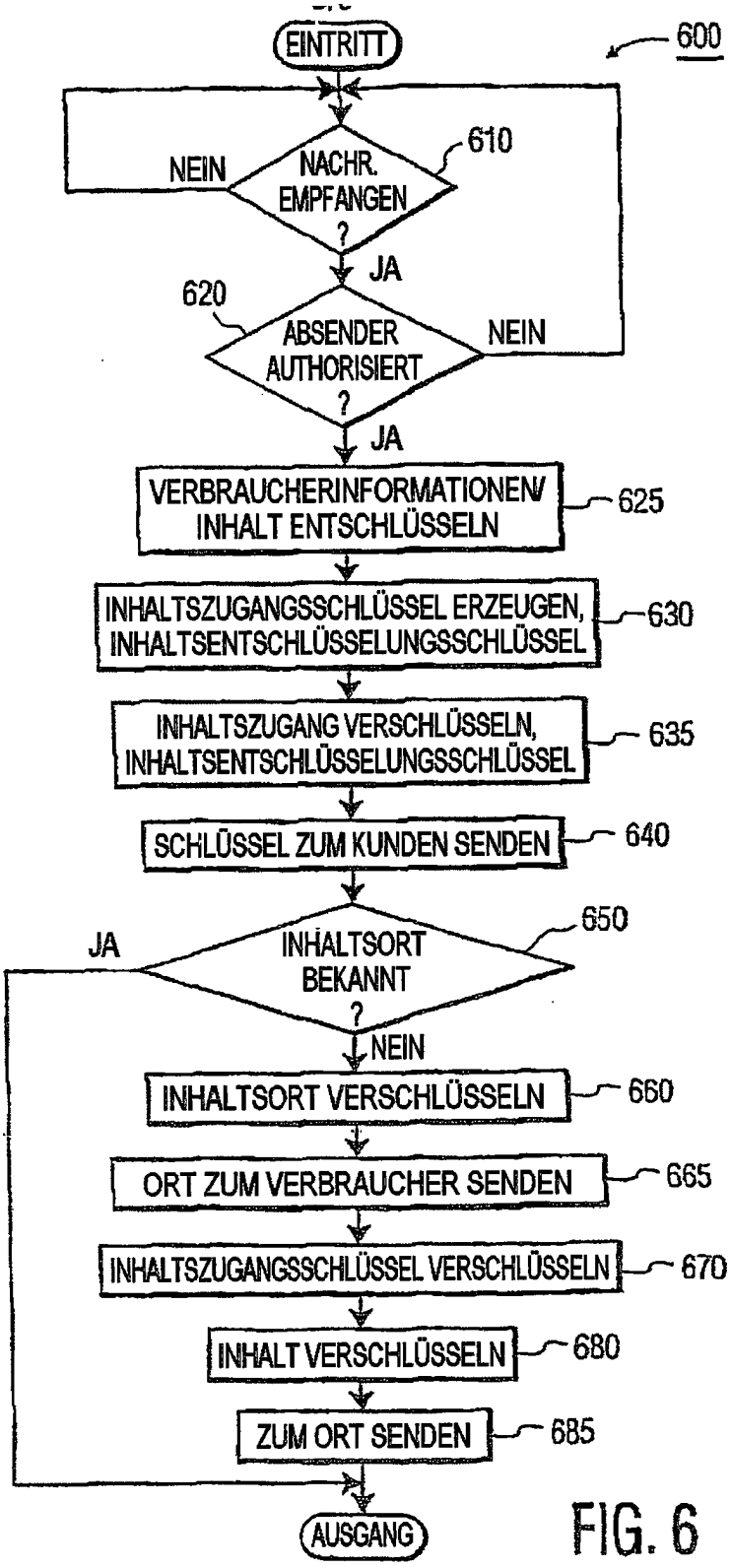
EINTRITT
600
NACHR. EMPFANGEN ?
610
NEIN
JA
ABSENDER AUTHORISIERT ?
620
NEIN
JA
VERBRAUCHERINFORMATIONEN/ INHALT ENTSCHLÜSSELN
625
INHALTSZUGANGSSCHLÜSSEL ERZEUGEN, INHALTSENTSCHLÜSSELUNGSSCHLÜSSEL
630
INHALTSZUGANG VERSCHLÜSSELN, INHALTSENTSCHLÜSSELUNGSSCHLÜSSEL
635
SCHLÜSSEL ZUM KUNDEN SENDEN
640
INHALTSORT BEKANNT ?
650
JA
NEIN
INHALTSORT VERSCHLÜSSELN
660
ORT ZUM VERBRAUCHER SENDEN
665
INHALTSZUGANGSSCHLÜSSEL VERSCHLÜSSELN
670
INHALT VERSCHLÜSSELN
680
ZUM ORT SENDEN
685
AUSGANG

FIG. 6

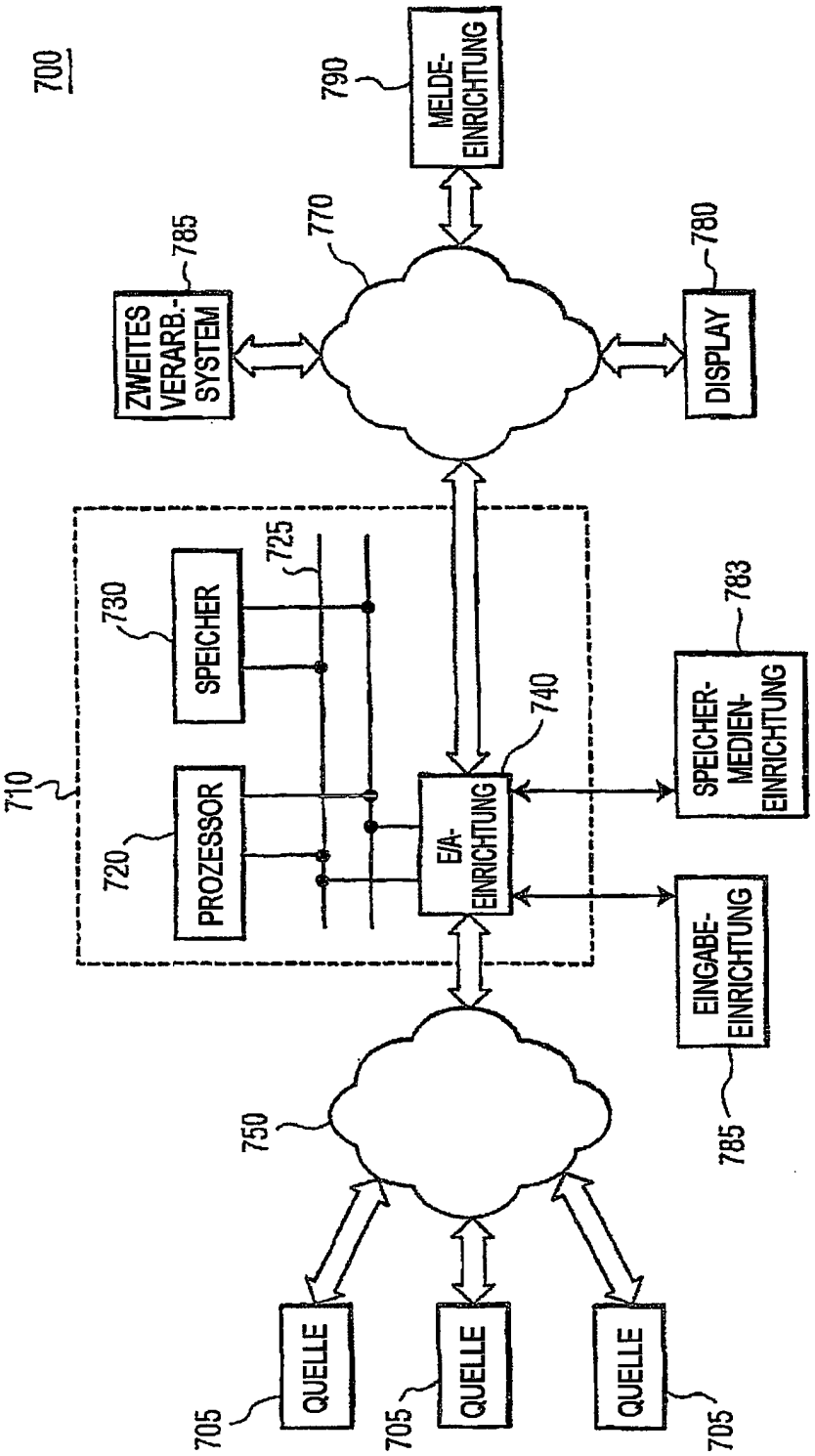
700
790
MELDE-EINRICHTUNG
785
ZWEITES VERARB.-SYSTEM
770
780
DISPLAY
710
730
SPEICHER
725
720
PROZESSOR
740
E/A-EINRICHTUNG
783
SPEICHER-MEDIEN-EINRICHTUNG
EINGABE-EINRICHTUNG
785
750
705
QUELLE
705
QUELLE
705
QUELLE

FIG. 7