República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0612027-0 A2**

BRPI0612027A2

(22) Data de Depósito: 13/04/2006
(43) Data da Publicação: 13/10/2010
(RPI 2075)

(51) Int.Cl.:
H04L 9/08
H04N 7/167

(54) Título: **MÉTODO PARA TRANSMITIR UM FLUXO DE DADOS PARA O DISPOSITIVO, DISPOSITIVO DE LEITURA DE COMPUTADOR, MÉTODO PARA RECEBER UM FLUXO DE DADOS DE UM SISTEMA DE COMUNICAÇÃO DURANTE A SESSÃO DE MULTIMÍDIA, MÉTODO PARA OBTER O FLUXO DE DADOS DO SISTEMA DE COMUNICAÇÃO, E, MÉTODO PARA TRANSMITIR OS DADOS STREAMING PARA O RECEPTOR**

(30) Prioridade Unionista: 12/05/2005 US 11/127,780

(73) Titular(es): NOKIA CORPORATION

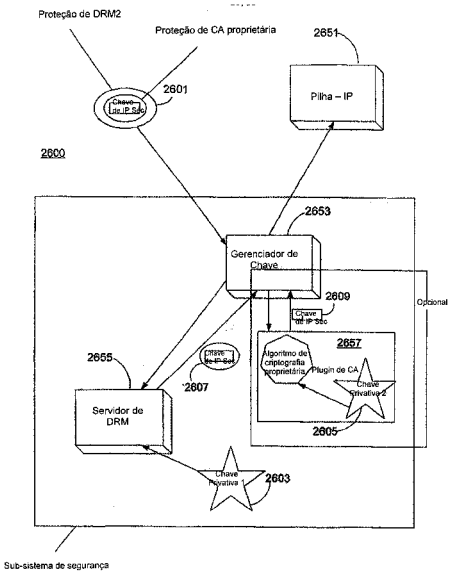
(72) Inventor(es): JUKKA ANTERO ALVE, PEKKA LLAMANI LAHTINEN

(74) Procurador(es): Araripe & Associados

(86) Pedido Internacional: PCT IB2006001047 de 13/04/2006

(87) Publicação Internacional: WO 2006/120516de 16/11/2006

(57) Resumo: MÉTODO PARA TRANSMITIR UM FLUXO DE DADOS PARA O DISPOSITIVO, DISPOSITIVO DE LEITURA DE COMPUTADOR, MÉTODO PARA RECEBER UM FLUXO DE DADOS DE UM SISTEMA DE COMUNICAÇÃO DURANTE A SESSÃO DE MULTIMIDIA, MÉTODO PARA OBTER O FLUXO DE DADOS DO SISTEMA DE COMUNICAÇÃO, E, MÉTODO PARA TRANSMITIR OS DADOS STREAMING PARA O RECEPTOR. A presente invenção provê métodos, aparelhos, e sistemas para entregar o conteúdo streaming protegido para o dispositivo de recepção. Em um aspecto da presente invenção, um radio difusor provê o conteúdo streaming. Para assegurar os visualizadores são autorizados apropriadamente, o conteúdo streaming é cifrado com a chave de tráfego. A chave de tráfego é fornecida para os usuários através da mensagem de fluxo da chave, que é cifrada com a tecla de serviço, O usuário obtém ao menos um objeto de direito dos emissores de direito e ao menos um objeto de direito inclui a chave de serviço, de forma que o conteúdo streaming possa ser usado. Ao menos um objeto de direito também contêm a informação considerando os direitos de uso que podem ser configurados pelo emissor de direitos de forma que, dependendo do usuário e/ou do dispositivo de recepção, diferentes direitos podem estar disponíveis. A mensagem de fluxo de chave pode incluir um valor variável de categoria de programa que indica o tipo de conteúdo e em conjunção com os direitos do objeto, determina quais direitos de uso existem para o conteúdo streaming.



PI0612027-0

"MÉTODO PARA TRANSMITIR UM FLUXO DE DADOS PARA O DISPOSITIVO, DISPOSITIVO DE LEITURA DE COMPUTADOR, MÉTODO PARA RECEBER UM FLUXO DE DADOS DE UM SISTEMA DE COMUNICAÇÃO DURANTE A SESSÃO DE MULTIMÍDIA, MÉTODO PARA OBTER O FLUXO DE DADOS DO SISTEMA DE COMUNICAÇÃO, E, MÉTODO PARA TRANSMITIR OS DADOS DE FLUXOS CONTINUOS PARA O RECEPTOR."

CAMPO DA INVENÇÃO

Esta invenção se refere à distribuição de conteúdo de multimídia protegido. Em particular, a invenção fornece aparelhos e métodos para o uso no fornecimento do controle melhorado sobre os direitos do usuário às porções do conteúdo protegido.

DESCRIÇÃO DA TÉCNICA ANTERIOR

O fluxo de vídeo, fluxo de dados e a programação de radiodifusão digital em banda larga estão crescendo em popularidade em aplicações de rede sem fio, por exemplo, nos serviços de multidifusão por Protocolo Internet (IP). Para suportar essas aplicações sem fio, os sistemas de transmissão sem fio transmitem o conteúdo dos dados que suportam serviços de dados a vários terminais sem fio simultaneamente. O conteúdo das mídias digitais ou outros dados são transmitidos usando vários protocolos de aplicação, protocolos de transporte e protocolos de rede. Por exemplo, um sistema de radiodifusão fornece a transmissão dos dados IP onde o serviço de audiovisual é transmitido de modo que o vídeo de MPEG4-AVC, os componentes áudio e dados auxiliares de MPEG4-AAC são empacotados e encapsulados para Protocolo de Transporte em Tempo Real (RTP) e/ou Controle Automático de Nível (ALC). Os pacotes são formatados subseqüentemente para UDP e IP e transmitidos sobre MPE em MPEG2-TS (por exemplo, DVB- H). Em um domínio de pacotes comutados, o conceito de sessão multimídia pode requerer que um ou mais componentes da sessão (áudio, vídeo e dados auxiliares no caso acima) estejam logicamente ligados em conjunto. As partes da sessão multimídia são enviadas entre um tempo de início e de fim comuns. Entretanto, com um ambiente de radiodifusão todos os receptores que podem receber o sinal de broadcast podem

receber os dados transportados pelo sinal de broadcast. É importante que o fornecedor de conteúdo limite o acesso ao conteúdo multimídia de modo que somente os receptores habilitados possam apresentar o conteúdo multimídia aos usuários.

Os sistemas de Gerenciamento de Direitos Digitais (*Digital Rights Management* - DRM), como o sistema de DRM *Open Mobile Alliance* (OMA), estão sendo usados para fornecer acesso a arquivos discretos, como Arquivos de Conteúdo Digital OMA DRM (DCF). Como uma solução possível, um dispositivo (conforme foi instruído pelo seu usuário humano) de um Provedor de Conteúdo obtém o DCF (por exemplo, um arquivo de música em MP3, o qual é criptografados por uma chave de conteúdo). O dispositivo obtém separadamente (isto é, compra) de um *Emissor de Direitos* (RI) um *Objeto de Direitos* (RO) que pode incluir (entre outras coisas) duas partes: a chave de conteúdo para decifrar o DCF e direito de uso para o DCF. Os direitos de uso controlam a maneira pela qual o dispositivo (e conseqüentemente seu usuário humano) o conteúdo pode ser copiado, etc. Emissores de Direitos RIs diferentes podem fornecer Objeto de Direitos RO's para o mesmo DCF por preços diferentes com diferentes direitos de uso.

Frequentemente, por exemplo, no caso de OMA DRM, os direitos de uso são expressos em Linguagem de Expressão de Direitos (*Rights Expression Language* – REL) que pode conter condicionalmente com base em variáveis como dias de semana, o tempo do dia, período de dias, etc.,... Por exemplo, pode ser afirmado que um direito de uso particular se estende por um determinado período de tempo. Exemplos de REL incluem *Open Digital Rights Language* (ODRL) e direitos extensivo de Markup Language (XrML).

Recentemente, os sistemas DRM estão sendo instalados para vender serviços de fluxos, além dos arquivos discretos de DCF. Um caso especial de tais serviços de fluxos é o verdadeiro serviço de fluxo de difusão de radio (daqui em diante, serviços de broadcast) onde múltiplos dispositivos recebem o mesmo fluxo de radiodifusão. Por exemplo, o OMA DRM foi proposto para vender e comprar serviços de difusão de dados de IP (IPDC), e a solução está sendo padronizada pela

organização de Digital Vídeo Broadcasting (DVB), de modo a (entre outras coisas) suportar os receptores portáteis de televisão no topo da tecnologia de difusão de radio DVB-H (*Digital Vídeo Broadcasting - portátil*).

As funções organizacionais típicas incluem: 1) uma emissora de difusora que obtém o conteúdo de fluxo de provedores de conteúdo e o transmite de forma criptografada sobre o caminho de radio e, 2) múltiplos RI's, quem vendem RO's para decriptografar o conteúdo e formatando os direitos de uso para eles nos múltiplos dispositivos de recepção de radiodifusão. Os RO's podem ser entregues sobre o mesmo caminho de difusão de radio como até o conteúdo criptografado, ou através de canais separados de interação, tais como portadoras de dados celulares (por exemplo, GSM, GPRS (Serviço Geral de Radio Pacote)).

Neste cenário, não é tipicamente possível para a chave em cada RO para decriptografar diretamente o conteúdo do fluxo, já que o conteúdo do fluxo é contínuo (ao contrário dos arquivos discretos de DCF). Uma técnica conhecida de decriptografar conteúdo é uma hierarquia de chave tal como usada no acesso condicional DVB. As emissoras de difusoras enviam seqüências de conteúdo de fluxo cada uma criptografada por uma chave de tráfego (TK)5 trocando periodicamente a chave de tráfego. Pelo menos, sempre que a chave de tráfego muda, é enviada uma *Key Stream Message (*KSM*),* contendo a chave de tráfego criptografada por uma chave de serviço. Os RO's contém as chaves de serviço, os dispositivos de recepção podem então usar as chaves de serviço para decriptografar o conteúdo do fluxo. Na prática, os KSM's devem ser transmitidos com muita freqüência de maneira a habilitar a "chave de canal" rápida de um serviço para outro.

A chave de serviço também muda periodicamente, embora a freqüência de mudança seja tipicamente muito mais baixa. Uma nova chave de serviço é então solicitada para o dispositivo continuar a decriptografar o conteúdo do fluxo. Portanto um novo RO, com uma nova chave de serviço poderá ser obtida pelos dispositivos para substituir os antigos. Por conseguinte, os RO's têm um certo período de validade, que é igual ao tempo durante o qual a chave de serviço pode ser usada para decifrar as chaves de tráfego de maneira a decifrar o conteúdo defluxo.

Como especificado acima, um RO para um serviço de radiodifusão serve para decriptografar e tornar acessível o conteúdo do fluxo, para o período de validade do RO. Como no caso de DCF, o RO pode também ser usado para estabelecer os direitos de uso expressos em REL para o mesmo período da validade. Como um exemplo, considere o DVB-H baseado serviço de difusão de televisão portátil. Os dispositivos são permitidos tipicamente para processar em uma tela (de modo que um usuário humano possa ver) o serviço de televisão, tal como um programa em um canal, à medida que é recebido. Os direitos de uso podem estabelecer que o dispositivo / usuário pode fazer com o conteúdo do fluxo, que pode ser o serviço de televisão. Por exemplo, os direitos de uso podem prover que o conteúdo possa ser gravado, podem ser reproduzidos em um tempo mais tarde, podem ser copiados para um outro dispositivo, podem somente ser vistos ou o que os direitos são desejados para ser providos.

Embora esta metodologia possa fornecer um determinado nível de funcionalidade, há ainda um problema. Cada RO pode estabelecer apenas um conjunto de direitos de uso para o período de validade. Esse nível de controle pode ser insuficiente. Por exemplo, pode haver tipos diferentes de programas de televisão em um serviço portátil de difusão de televisão que os RIs possam desejar fornecer níveis diferentes de controle a respeito do uso. Os RI's podem desejar permitir um direito de uso liberal "faz qualquer coisa" para determinados tipos ou partes de conteúdo tal como notícias, propagandas ou pesquisas, mas restringem os direitos de uso para outros tipos ou partes de conteúdo, tais como eventos esportivos ou exibição de filmes. Assim, enquanto o os RO's com períodos relativamente longos de validade são muito bons para o acesso de conteúdo de fluxo (isto é decriptografia), seria útil proporcionar uns meios refinados de prover direitos de uso com a freqüência e/ou a precisão aumentada dentro do período da validade do RO de modo que, o uso do tipo ou da parte do conteúdo esteja de acordo com os direitos de uso que se pretende sejam concedidos para o tipo ou a parte de conteúdo.

Além disso, os direitos a determinado conteúdo podem variar dependendo da

hora ou do dia da semana. Além disso, um usuário pode ter direitos diferentes por partes diferentes de conteúdo. Por exemplo, a fim de melhorar o faturamento, a um usuário é permitido freqüentemente acessar os serviços de multimídia premium somente se o usuário subscrever o serviço ou requisita o serviço (por exemplo, pagar-para-ver). Entretanto, o conteúdo pode também ser separado em períodos de tempo. Assim, por exemplo, um usuário pode decidir subscrever uma edição de fim de semana melhor que uma subscrição para a semana toda. Os RI's podem desejar permitir que algum do conteúdo disponível na subscrição da edição do fim de semana seja conservado e enviado livremente a outra ao limitar outras partes do conteúdo a um único uso ou para um conjunto mais controlado de distribuição.

RESUMO DA INVENÇÃO

Como um aspecto da invenção, um seletor que consiste em alguns bits, transmitidos freqüentemente, pode selecionar os direitos para uma parte particular do conteúdo de um conjunto de direitos previamente adquiridos e contidos dentro de um ou mais RO's. Como o seletor é relativamente pequeno, a transmissão freqüente do seletor tem pouco impacto sobre a largura de faixa disponível. Por conseguinte, um ou o mais RO's, que mudam muito menos freqüentemente, pode fornecer os detalhes dos direitos, daí resultando em economia de canal de radiodifusão. Assim, um ou o mais RO pode ainda utilizar toda a potencialidade do REL para definir o que direitos são para cada parte do conteúdo.

Um outro aspecto da presente invenção fornece métodos, aparelhos, e sistemas de distribuição de conteúdo protegido de multimídia a um dispositivo de recepção. As partes do conteúdo multimídia protegido e de informação chave associadas são inseridas ao mesmo tempo na seqüência de sinais. Conseqüentemente, a informação chave pode freqüentemente ser mudada enquanto mantém a sincronização com o conteúdo multimídia. Em uma incorporação da invenção, as intermitências de fatia do tempo são enviadas de um aparelho de transmissão para um dispositivo de recepção por um sistema de comunicações que inclui um sistema de DVB-H, um sistema de DVB-T, um sistema de ATSC, e um sistema de ISDB-T. Os KSMs, que são enviados muito

freqüentemente, cada um contém uma quantidade pequena de informação da categoria do programa que traduz em uma variável REL e seleciona desse modo os direitos condicionais de uso dos RO's de todo os RI's, ou (como uma outra implementação) do RO de cada RI individualmente. Em uma incorporação, a seleção pode ser um programa específico de televisão.

Como um outro aspecto da invenção, a informação de categoria de programa enviada no KSM poderia ser usada para selecionar um conjunto completo de RO's, ou possivelmente um de diversos RO's secundários relacionados com o mesmo RO principal.

BREVE DESCRIÇÃO DOS DESENHOS

Uma compreensão mais completa da presente invenção e das vantagens da mesma pode ser adquirida referindo-se à descrição seguinte e na consideração dos desenhos que as acompanham, nos quais os mesmos números de referência indicam as mesmas características e em que:

A Figura 1 mostra os serviços de transmissão do Protocolo da Internet (IP) que utilizam a transmissão da fatia de tempo de acordo com uma incorporação da invenção;

A figura 2 mostra uma pilha de protocolo que suporta a transmissão de dados de multimídia de acordo com uma incorporação da invenção;

A figura 3 mostra uma configuração componente para uma sessão multimídia de acordo com uma incorporação da invenção;

A figura 4 mostra uma configuração de componente para uma sessão multimídia mostrada de acordo com uma incorporação da invenção;

A figura 5 mostra uma variação da configuração componente mostrada na figura 4 de acordo com uma incorporação da invenção;

A figura 6 mostra uma variação da configuração componente mostrada na figura 4 de acordo com uma incorporação da invenção;

A figura 7 mostra uma variação da configuração de componente mostrada na figura 4 de acordo com uma incorporação da invenção;

A figura 8 mostra uma variação da configuração de componente mostrada na

figura 4 de acordo com uma incorporação da invenção;

A figura 9 mostra uma variação da configuração de componente mostrada na figura 4 de acordo com uma incorporação da invenção;

A figura 10 mostra um componente a configuração para uma sessão multimídia de acordo com uma incorporação da invenção;

A figura 11 mostra uma variação da configuração de componente mostrada na figura 10 de acordo com uma incorporação da invenção;

A figura 12 mostra uma variação da configuração de componente mostrada na figura 10 de acordo com uma incorporação da invenção;

A figura 13 mostra uma variação da configuração de componente mostrada na figura 10 de acordo com uma incorporação da invenção;

A figura 14 mostra uma variação da configuração de componente mostrada na figura 10 de acordo com uma incorporação da invenção;

A figura 15 mostra uma variação da configuração de componente mostrada na figura 10 de acordo com uma incorporação da invenção;

A figura 16 mostra uma variação da configuração de componente mostrada na figura 10 de acordo com uma incorporação da invenção;

A figura 17 mostra um procedimento para receber uma sessão multimídia de acordo com uma incorporação da invenção;

A figura 18 mostra um diagrama de fluxo para a arquitetura mostrada na figura 17 de acordo com uma incorporação da invenção;

A figure 19 mostra um sistema para transferência satisfeita protegida que suporta serviços de DVB-H IPDC (difusão de dados de IP) de acordo com a técnica anterior;

A figura anterior 20 mostra um sistema que suporta serviços de DVB-H IPDC de acordo com uma incorporação da mostra da invenção;

A figura 21 um diagrama de fluxo para dados transmissores para serviços de DVB-H IPDC no sistema mostrado na figura 20 de acordo com uma incorporação da invenção;

A figura 22 mostra um sistema que suporta serviços de DVB-H IPDC de

acordo com uma incorporação da invenção;

A figura 23 mostra um sistema que suporta serviços de DVB-H IPDC de acordo com uma incorporação da invenção;

A figura a 24 mostra que um aparelho para aquele suporta um módulo da transmissão como mostrado nas figuras 20, 22, e 23 de acordo com uma incorporação da invenção;

A figura 25 mostra um aparelho que recebe uma transmissão multimídia e que aplica chaves de IPSec de acordo com uma incorporação da invenção;

A figura 26 mostra um aparelho que recebe uma transmissão multimídia e que decifra as chaves de IPSec de acordo com uma incorporação da invenção;

A figura 27 mostra um sistema para desdobrar um módulo de conexão de software de segurança de acordo com uma incorporação da invenção;

A figura 28 mostra o exemplo de um método da técnica anterior de prover conteúdo;

A figura 29 mostra um método de fornecer o fluxo continuo de conteúdo cifrado de acordo com uma incorporação da invenção;

A figura 30 mostra um método de transmitir o fluxo continuo de conteúdo de acordo com uma incorporação da invenção;

A figura 31 mostra uma linha de tempo de mudanças às chaves de tráfego de acordo com uma incorporação da invenção;

A figura 32 mostra uma divisão de segmentos de programa de acordo com uma incorporação da invenção; e.

A figura 33 mostra um sistema para prover o uso de uma pluralidade de objetos de direitos de acordo com uma incorporação da invenção.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Na seguinte descrição das várias incorporações, é feita referência aos desenhos que acompanham e formam uma parte do mesmo, e nos quais são mostradas, a guisa de ilustração, as várias incorporações em que a invenção pode ser praticada. Deve-se entender que outras incorporações podem ser utilizadas e que modificações estruturais e funcionais podem ser feitas sem se afastar do

conceito da presente invenção.

Para ajudar na organização e para a facilidade do leitor, a descrição detalhada é fornecida em duas seções. Primeiramente, nas figuras 1-27, são fornecidos os detalhes a respeito dos métodos de enviar e de receber o conteúdo de acordo com aspectos da presente invenção. Em seguida, nas figuras 28-33, são divulgados os detalhes a respeito dos métodos e o aparelho para controlar os direitos de uso para partes de conteúdo.

Métodos e Aparelhos para prover Conteúdo em Fluxo Contínuo

A figura 1 mostra a transmissão de serviços do Protocolo de Internet (IP) que utilizam a transmissão de fatia de tempo de acordo com uma incorporação da invenção. Uma estação base transmite por radiodifusão de pacotes de dados para uma pluralidade de serviços de IP usando os fluxos contínuos de dados 101, 103, 105, e 107 (a cada fluxo de dados é alocado uma parte de uma capacidade da taxa de dados.) Na incorporação, a estação base pode suportar a funcionalidade que é tipicamente supostamente assumida como uma estação base transceptora (BTS), um controlador da estação base (BSC), uma combinação de um BTS e um BSC, e um nó B, que é uma designação de terceira geração (3G) de uma estação base transceptora. A transmissão de dados é essencialmente contínua de modo que os pacotes de dados para um serviço do IP estão continuamente sendo conduzidos através de um fluxo de dados.

A fim de aliviar a perda de pacotes de dados, os fluxos de dados 101, 103, 105, e 107 são mapeadas por estações base em rajadas de pacotes 109, 111, 113, e 115 de dados, respectivamente, em que as rajadas são transmitidas sobre canais de radio ao invés dos fluxos de dados 101, 103, 105, e 107. Cada fluxo de dados (101, 103, 105, e 107), e conseqüentemente cada rajada (109, 111, 113, e 115), suportam pelo menos um serviço de dados. Assim, cada rajada pode suportar uma pluralidade de serviços de dados (por exemplo, um grupo de serviços de dados relacionados).

As taxas de dados associadas com as rajadas 109, 111, 113, e 115 são tipicamente maiores do que as taxas de dados que são associadas com os fluxos de

dados 101, 103, 105, e 107 de modo que um número correspondente de pacotes de dados possa ser enviado em um tempo mais curto. Na incorporação, os fluxos de dados 101, 103, 105, e 107 correspondem às taxas de dados contínuas de aproximadamente 100 Kbit/sec. As rajadas 109, 111, 113, e 115 correspondem tipicamente a aproximadamente 4 Mbit/sec (mas pode estar em um excesso de 10 Mbit/sec) com uma duração aproximada de um segundo. Contudo, outras incorporações podem usar taxas de dados diferentes para fluxos de dados 101-107 e para rajadas 109-115

Na incorporação, a capacidade inteira da taxa de dados é alocada a uma rajada em um tempo dado. Como mostrado em figura 1, as rajadas 109, 111, 113, e 115 são intercalados em tempo. Uma duração inativa de tempo (durante a qual pacotes de dados não são transmitidos para o serviço de dados particular) ocorre entre transmissões consecutivas de uma rajada (por exemplo, rajada 109). Um sistema de transmissão sem fio pode utilizar a duração inativa de tempo durante o qual o terminal sem fio pode ser instruído para transferir a uma outra estação base para concluir uma transferência. A outra estação base pode transmitir os mesmos dados que a estação base que serve previamente ao terminal sem fio usando uma freqüência de centro diferente e uma quantidade diferente de deslocamento de fase. A utilização de fatia de tempo permite que um terminal reduza o consumo de energia elétrica que é fornecido por uma fonte de alimentação (tipicamente uma bateria).

O terminal sem fio pode manter o sincronismo preciso, como com o sistema de posicionamento global (GPS), para determinar um tempo absoluto em que cada uma rajada ocorre. Em uma outra incorporação, o terminal sem é provido com informação em torno de um período de tempo em cada rajada, informando o terminal sem fio sobre a rajada subseqüente. Com uma incorporação da invenção, a informação do período de tempo inclui um parâmetro em tempo real (que corresponde ao "delta-t" com o DVB-H) que indica um intervalo do tempo a partir do início de uma fatia de tempo de rajada ao início fatia de tempo de rajada seguinte do mesmo serviço e que seja sinalizado em um cabeçalho de seção de MPE. O período de tempo pode ser incluído em um pacote do IP, um quadro encapsulado

multiprotocolo, qualquer outro quadro de pacote, e uma terceira geração (3G) ou Serviço Geral de Rádio Pacote (GPRS) ou dados de modulação, tais como sinalizar o parâmetro do transmissor. Alternativamente, o terminal sem fio pode detectar uma ocorrência de uma rajada recebendo um preâmbulo do sinal, que possa ser uma seqüência de dados que seja conhecida a priori ao terminal sem fio. Em uma outra incorporação, o terminal sem fio pode receber uma mensagem aérea em um canal aéreo de uma estação base. A mensagem aérea pode conter a informação de sincronismo a respeito da ocorrência das rajadas. O canal aéreo pode ser logicamente ou fisicamente distinto do canal de rádio de enlace descendente que suporta a transmissão das rajadas.

As rajadas são transmitidas típica e periodicamente por uma estação base. Por exemplo, uma rajada subseqüente pode ocorrer T segundos após a rajada 109, em que uma rajada é transmitida a cada T segundos. O terminal sem fio pode manter o sincronismo preciso, como ocorre com o Sistema de Posicionamento Global (GPS), para determinar um tempo absoluto em que cada uma rajada ocorre. Em uma outra incorporação, o terminal sem fio é provido de informação sobre o período de tempo em cada um rajada, informando ao terminal sem fio sobre a rajada subseqüente. Com uma incorporação da invenção, a informação do período de tempo inclui um parâmetro em tempo real (que corresponde ao "delta-t" com o DVB-H) que indica um intervalo do tempo do início de uma rajada de fatia de tempo ao início da rajada de fatia de tempo seguinte do mesmo serviço e que é sinalizado em um cabeçalho de seção do MPE. O período de tempo pode ser incluído em um pacote IP, um quadro encapsulado multiprotocolo, qualquer outro quadro de pacote, e uma terceira geração (3G) ou canal de Serviço Geral de Rádio Pacote (GPRS) ou modulação de dados, tais como sinalizar do parâmetro do transmissor. Alternativamente, o terminal fio pode detectar uma ocorrência de uma rajada recebendo um preâmbulo de sinal, que possa ser uma seqüência de dados que seja conhecida a priori ao terminal sem fio. Em uma outra incorporação, o terminal sem fio pode receber uma mensagem aérea em um canal aéreo de uma estação base. A mensagem aérea pode conter a informação de sincronismo a respeito da ocorrência

de rajadas. O canal aéreo pode ser lógica ou fisicamente distinto do canal de rádio de enlace descendente que suporta a transmissão de rajadas

As rajadas 109, 111, 113, e 115 podem ser formatadas usando um encapsulamento multiprotocolo de acordo com a Seção 7 da Norma Européia EN 301 192 "*Digital Video Broadcasting (DVB), DVB Specification for Data Broadcasting*". O encapsulamento pode estar em conformidade com as normas do Protocolo da Internet (IP).

Em uma incorporação da invenção, uma transmissão vídeo digital (DVB-H) fornece serviços móveis de mídias aos terminais sem fio, por exemplo, unidades portáteis sem fio. Na incorporação, o sistema de DVB-H é compatível com DVB-T (transmissão vídeo digital para a operação terrestre) e suporta aprimoramentos para melhor operação de suporte de terminais portátil sem fio. O sistema de DVB-H suporta os serviços de dados com base no qual a informação pode ser transmitida como datagramas IP. O sistema de DVB-H incorpora aprimoramentos (com respeito a um sistema de DVB-T) que facilita o acesso aos serviços baseados IP de DVB em terminais portátil sem fio. (as incorporações alternativas da invenção suportam variações de sistemas digitais de transmissão de vídeo incluindo DVB-T, ATSC, e ISDB-T.) Os aprimoramentos do DVB-H são baseados na camada física da camada física de DVB-T com um número de aprimoramentos da camada de serviço visando melhorar a recepção e a vida da bateria no ambiente portátil. Assim, os aprimoramentos de DVB-H complementam os serviços terrestres digitais existentes, oferecendo aos provedores de serviço a possibilidade expandir o mercado ao mercado do portátil sem fio.

A figura 2 mostra uma pilha 200 de Protocolo da Internet (IP) que suporta a transmissão de dados de multimídia de acordo com uma incorporação da invenção. O conteúdo de mídia digital ou outros dados são transmitidos usando vários protocolos de aplicação, protocolos de transporte e protocolos de rede. Com pilha 200 do IP, uma transmissão de dados de IP suporta um serviço audiovisual que tem o vídeo 201 de MPEG4-AVC, o áudio 203 de MPEG4-AAC e os componentes de dados auxiliares 205. Cada componente (201, 203, ou 205) é processado pelo

codificador 207, pelo codificador 209, ou pelo codificador 211 a fim obter os pacotes que são formatados para a camada 213 do Protocolo de Tempo Real (RTP). Os pacotes (datagramas) são processados subseqüentemente pela camada 215 do UDP (*User Datagram Protocol*) e pela camada 217 do Protocolo da Internet (IP). Os datagramas são associados com as rajadas de fatia de tempo formatando os datagramas usando um encapsulamento multiprotocolo (que corresponde tipicamente a uma camada da ligação no modelo OSI) como, por exemplo, de acordo com a seção 7 da norma européia EN 301 192 "*Digital Video Broadcasting (DVB), DVB specification for data broadcasting.*" O encapsulamento pode estar em conformidade com as normas do Protocolo da Internet (IP).

Uma seção de multimídia é associada tipicamente com um ou mais componentes de seção (áudio, vídeo e dados auxiliares no caso acima) que são logicamente acoplados juntos. As partes da seção são enviadas entre um tempo de início e de fim comuns. Ambos os tempos de inicio e de fim podem ser definidos ou não definidos. A figura 3 mostra uma configuração de componente para uma seção de multimídia 301 de acordo com uma incorporação da invenção

O componente 303 corresponde a uma pluralidade de datagramas (incluindo os datagramas 309 e 315); o componente 305 corresponde a uma pluralidade de datagramas (incluindo os datagramas 311 e 317); e o componente 307 corresponde a uma pluralidade de datagramas (incluindo os datagramas 313 e 319). Os componentes 303, 305 e 307 são transmitidos dentro de pacotes IP que são encapsulados para transferência de mensagens de uma camada portadora de suporte. Cada componente 303, 305 e 307, tem um endereço IP de origem definido; um endereço IP de destino e uma porta usada nos pacotes IP que transportam dados associados com o componente. Componentes diferentes podem ter um endereço IP de origem, um endereço IP de destino e uma porta definida independentemente. Nas variações da incorporação, uma seção se multimídia pode ter um número diferente de componentes.

Enquanto a configuração exemplo de componente 300 mostra um alinhamento de datagrama entre os componentes 303, 305e 307, a incorporação

suporta configurações nas quais os datagramas não alinhados e o número de datagramas para um componente de áudio é tipicamente menor que o número de datagramas para um componente de vídeo durante um dado intervalo de tempo.

A figura 4 mostra uma configuração de componente 400 para uma seção de multimídia de acordo com uma incorporação da invenção. Os componentes 403, 405 e 407 são cifrados com a mesma chave que muda periodicamente na chave de fluxo 409 durante a seção de multimídia 401. (Nas figuras 4-16, um datagrama que é cifrado com chave kj é marcado como Ej.) A incorporação suporta diferentes métodos de criptografia que são aplicados aos componente 403, 405 ou 407, incluindo IPSEC-ESP (assim chamada criptografia de nível de IP; veja RFC na IPSEC-ESP).

Carga útil do pacote de seção de aplicação cifrada (por exemplo, SRTP ou DCF de OMA DRM 1.0 ou 2.0).

Criptografia. Os métodos de criptografia acima podem ser aplicados separadamente ou em combinação durante a sessão de multimídia. Os Componentes 403, 405, e 407 correspondem a uma diferente pluralidade de datagramas de conteúdo. A chave de fluxo 409 inclui uma pluralidade de datagramas associados, cada datagrama associado correspondendo a uma chave de criptografia. A criptografia é executada tipicamente em uma base de datagrama individual (ex. pacote). Por exemplo, datagramas de conteúdo 415, 425, 427, 435, e 437 são cifrados com chave kt (correspondendo ao datagrama associado 413).

A chave de fluxo 409 utiliza um protocolo de distribuição tal como RTP, ALC/FLUTE, UHTTP, DVBSTP, IP com uma carga útil, e UDP com uma carga útil. As chaves distribuídas na chave de fluxo 409 são tipicamente protegidas por uma outra chave que é designada receptora tem de modo a acessar os conteúdos de chave de fluxo 409 que transporta chaves, possibilitando assim o acesso aos componentes 403, 405 e 407. A distribuição de chave de fluxo 409 é sincronizada opcionalmente com componentes 403, 405 e 407, e.g., RTP marcação de tempo com o uso de Protocolo de Controle RTP

A figura 5 mostra uma variação da configuração de componente mostrado na

figura 4 de acordo com uma incorporação da invenção. A configuração de componente 500 é similar à configuração de componente 400. A sessão de multimídia 501 inclui componentes 503, 505, e 507 e chave de fluxo 509. O componente 505 é criptografado com chaves de fluxo 509, enquanto os componentes 503 e 507 não são.

A figura 6 mostra uma variação da configuração de componente mostrado na figura 4 de acordo com uma incorporação da invenção. A configuração de componente 600 é similar à configuração de componente 400. Entretanto, a chave de fluxo 609 inclui três séries de chaves 611, 613, e 615 que correspondem aos componentes 603, 605, e 607, respectivamente. As chaves podem mudar periodicamente, mas independentemente durante a sessão de multimídia 601, mas pode ser sincronizada uma com a outra.

A figura 7 mostra uma variação da configuração de componente mostrado na figura 4 de acordo com uma incorporação da invenção. A configuração de componente 700 é similar à configuração de componente 600 exceto que as chaves para cada componente são transportadas em diferentes chaves de fluxos que mudam durante a sessão de multimídia 701. Ao invés de ter uma chave de fluxo, a configuração de componente 700 que utiliza três chaves de fluxos 709, 711, e 713. As 709, 711, e 713 que corresponde aos componentes 703, 705, e 707, respectivamente.

A figura 8 mostra uma variação da configuração de componente mostrado na figura 4 de acordo com uma incorporação da invenção.com a configuração de componente 800, o componente 805 é cifrado com chaves de chave de fluxo 809. Entretanto, a chave de fluxo 809 fornece chaves que são atualmente aplicáveis para decifrar componente 805 assim como as chaves serão subseqüentemente usadas na decifração do componente 805. No exemplo mostrado na figura 8, a chave k] (correspondente ao datagrama 811) é aplicada atualmente aplicada enquanto que as chaves k2 (correspondente ao datagrama 813) e k3 (correspondente ao datagrama 815) são aplicadas subseqüentemente. Enquanto que os componentes 803 e 807 não são cifrados durante a sessão de multimídia 801, os componentes

803 e 807 podem ser cifrados com outras variações da incorporação. Tendo chaves que serão usadas subseqüentemente aplicadas, isso permite ao dispositivo receptor suavizar transições de chave durante a sessão de multimídia 801. Por exemplo, o dispositivo receptor pode configurar a pilha IP com uma nova chave para reduzir interrupções na decifração de datagramas de conteúdo.

A figura 9 mostra uma variação da configuração de componente mostrado na figura 4 de acordo com uma incorporação da invenção. A chave de fluxo 909 inclui a chave sendo atualmente aplicada ao componente 905 para criptografar bem como as chaves que serão aplicadas subseqüentemente quando a transição de chave estiver dentro de tempo incremental predeterminado do tempo atual. Por exemplo, antes da transição de chave 951, a chave de fluxo 900 inclui ambas as chaves ki (correspondentes ao datagrama 911) e k2 (correspondentes ao datagrama 913) e inclui k2 (correspondentes ao datagrama 915) após a transição de chave 951. como com a configuração de componente 800, a configuração de componente 900 ajuda o dispositivo receptor a suavizar os efeitos de transição de chave.

A figura 10 mostra uma configuração de componente 1000 para uma sessão de multimídia 1001 de acordo com uma incorporação da presente invenção. Entretanto, em comparação com as configurações dos componentes 400 – 900, as chaves são transportadas em um ou mais componentes ao invés de ter uma chave de fluxo separada para transmitir as chaves. Com a configuração do componente 1000, o componente 1005 inclui datagramas de conteúdo (por exemplo, datagrama de conteúdo 1011) bem como datagrama 1009 que fornece chave k\ que foi usada para criptografar os componentes 1003, 1005 e 1007.

A figura 11 mostra uma variação da configuração de componente mostrado na figura 10 de acordo com uma incorporação da presente invenção. Com a configuração de componente 1100, o componente 1107 fornece a chave k! (correspondente ao datagrama 1109) e chave k2 (correspondente ao datagrama 1111) que são aplicados ao componente 1105 durante a sessão de multimídia 1101. No exemplo mostrado na figura 11, os componentes 1103 e 1107 não são cifrados com as chaves fornecidas pelo componente 1107.

A figura 12 mostra uma variação da configuração de componente mostrado na figura 10 de acordo com uma incorporação da presente invenção. A configuração de componente 1200 é similar à configuração de componente 1100. Entretanto, chaves são aplicadas a ambos componentes que transportam informação de chave (componente 1205) bem como outro componente (componente 1203) durante a sessão de multimídia 1201. Todavia, no exemplo mostrado na figura 12, o componente 1207 não está cifrado.

A figura 13 mostra uma variação da configuração de componente mostrado na figura 10 de acordo com uma incorporação da presente invenção. Com a configuração de componente 1300, cada componente 1303, 1305 e 1307 transporta chaves que são aplicadas aos mesmos componentes durante a sessão de multimídia 1301. Por exemplo, chaves k[pi] (correspondendo ao datagrama 1309) e kj2 (correspondendo ao datagrama 1311) são aplicadas ao componente 1303. As chaves k21 (correspondendo ao datagrama 1313) e k22 (correspondendo ao datagrama 1315) são aplicadas ao componente 1305, As chaves k3[iota] (correspondendo ao datagrama 1317) e k32 (correspondendo ao datagrama 1319) são aplicadas ao componente 1307.

A figura 14 mostra uma variação da configuração de componente mostrado na figura 10 de acordo com uma incorporação da presente invenção. Com a configuração de componente 1400, cada componente 1403, 1405 e 1407 transporta chaves que são aplicadas a um componente diferente durante a sessão de multimídia 1401. Por exemplo, as chaves k[pi] (correspondendo ao datagrama 1413 e transportada pelo componente 1405) e k12 (correspondendo ao datagrama 1419 e transportada pelo componente 1407) são aplicadas ao componente 1403. as chaves k21 (correspondendo ao datagrama 1417 e transportada pelo componente 1407) e k22 (correspondendo ao datagrama 1411 e transportada pelo componente 1403) são aplicadas ao componente 1405. As chaves k31 (correspondendo ao datagrama 1409 e transportada pelo componente 1403) e k32 (correspondendo ao datagrama 1415 e transportada pelo componente 1405) são aplicadas ao componente 1407.

A figura 15 mostra uma variação da configuração de componente mostrado

na figura 10 de acordo com uma incorporação da presente invenção. Com a configuração de componente 1500, a informação de chave é transportada em um datagrama de conteúdo ao invés de um datagrama separado. Por exemplo, a chave kj é incluída em datagrama de conteúdo 1509 com uma parte concatenada (ou com um cabeçalho especial) 1511 e k2 incluída em um datagrama de conteúdo 1513 com uma parte concatenada (ou com um cabeçalho especial) 1515. As chaves ki e k2 são aplicadas aos datagramas nos componentes 1503, 1505 e 1507.

A figura 16 mostra uma variação da configuração de componente mostrado na figura 10 de acordo com uma incorporação da presente invenção. A configuração de componente 1600 é similar à configuração de componente 800, no qual ambas a chave atual bem como as chaves subseqüentes são fornecidas. Por exemplo, o componente 1605 transporta a chave ki (correspondente ao datagrama 1609) e a chave k2 (correspondente ao datagrama 1611), onde a chave ki é aplicada atualmente aos componentes 1603 e 1607 e a chave k2 é subseqüentemente aplicada durante a sessão de multimídia 1601. De maneira similar, a chave k2 (correspondente ao datagrama 1613) e k3 (correspondente ao datagrama 1615) são transportadas subseqüentemente no componente 1605. Como a configuração do componente 800, componente 1600 ajuda o dispositivo receptor para suavizar as transições de chave.

A figura 17 mostra uma arquitetura 1700 para receber uma sessão de multimídia de acordo com uma incorporação da invenção. Com a arquitetura 1700, um dispositivo receptor recebe a rajada de fatia de tempo de dados 1701 contendo ambos os componentes da sessão IP e a chave de fluxo relacionada com os componentes da sessão. Pluralidades de datagramas de conteúdo 1705, 1707, e 1709 correspondem ao componente 1, componente 2, e componente 3, respectivamente. Uma pluralidade de datagramas 1711 correspondem à chave de fluxo. A rajada de fatia de tempo1701 é armazenada no buffer de período determinado 1713 antes de enviar os datagramas (pacotes) para a pilha IP 1721. O dispositivo receptor extrai primeiro as chaves (correspondentes ao datagrama 1717) para a rajada de fatia de tempo 1701 buffer de período determinado 1713. Segundo,

o dispositivo receptor instala as chaves extraídas para a base de dados da IPSec *Security Association (SA)*. Também, o dispositivo receptor extrai os datagramas restantes 1715 do buffer de período determinado e encaminha-os para a pilha IP 1721. Após decifrar, os datagramas processados são passados para as aplicações 1723 para apresentação do conteúdo de multimídia. Conseqüentemente, a pilha IP 1721 não rejeita os datagramas de conteúdo (a menos que existam datagramas de conteúdo que o dispositivo receptor não teve a chave correspondente conforme distribuída na fatia de tempo atual ou um rajada de fatia de tempo anterior). O processo é repetido para a próxima rajada de fatia de tempo recebido.

A figura 18 mostra o diagrama de fluxo 1800 para a arquitetura mostrada na figura 17 de acordo com uma incorporação da invenção. Na etapa 1801, um dispositivo de recepção recebe uma rajada de fatia de tempo sobre um canal de comunicações, por exemplo, um canal sem fio. Na etapa 1803, o dispositivo de recepção separa os componentes (por exemplo, um componente de áudio e um componente de vídeo) da rajada recebida na fatia de tempo. Na etapa 1805, o dispositivo de recepção extrai o conjunto associado de chaves de chave de fluxo. As chaves extraídas podem ser aplicadas aos datagramas de conteúdo contidos na rajada de fatia do tempo ou em subseqüentes rajada de fatia de tempo. Também, a incorporação suporta as configurações em que as chaves diferentes são usadas para datagramas diferentes na rajada de fatia de tempo. As chaves extraídas são aplicadas a uma base de dados IPSec Security Association (SA) (por exemplo, SA DB 1719 mostrado na figura 17) na etapa 1807. Na etapa 1809, os datagramas de conteúdo são extraídos de um buffer (por exemplo, buffer de período determinado 1713 do ínterim) e enviados a uma pilha de IP (por exemplo, pilha 1721) na etapa 1811. Os datagramas de conteúdo subseqüentemente são decriptografados e enviados à aplicação correspondente.

A figura 19 mostra um sistema 1900 para transferência de conteúdo protegido que suporta serviços de DVB-H IPDC (difusão de dados de IP) de acordo com a técnica anterior. O sistema 1900 fornece transferência de conteúdo protegido para os serviços de DVB-H usando IPDC como especificado do "*Interim DVB-H IP*

Datacast Specifications: IP Datacast Baseline Specification: Specification of Interface I_MT", documento A080 de DVB, Abril 2004. De acordo com esta especificação, os pares de dados de segurança associados são transmitidos em um diretório eletrônico de serviço (ESG) no carrossel 1921 de SA como arquivo de DRM protegido 1919 SA (que é fornecido pelo gerente de direitos digitais (DRM) 1909 executando a função de proteção) e o arquivo de política IPSec 1911. Porque os dados do carrossel são tipicamente atualizados não com freqüência (por exemplo, uma vez por dia) o sistema 1900 não fornece uma solução eficiente para a distribuição de chave, especialmente se uma ou mais das chaves são atualizadas ou freqüentemente muda.

O conteúdo de multimídia 1901 (que corresponde aos datagramas de IP) é cifrado pelo módulo de criptografia 1903 com chaves de IPSec 1905 e transmitido (como executado pelo sistema de transmissão 1925) como pacotes de fatia de tempo (após o encapsulamento multiprotocolo, a codificação de FEC, e formação de rajada de fatia do tempo) para o dispositivo de recepção 1926. O objeto de direitos (RO) 1923 (que é fornecido pela geração do objeto de direitos 1922) é transmitido para receber o dispositivo 1926 através de um canal de interação, no qual o dispositivo de recepção 1926 é fornecido com um meio para comunicações bidirecionais, por exemplo, funcionalidade do telefone celular. Um usuário de dispositivo de recepção1926 pode requisitar o serviço (conteúdo) e receber conseqüentemente o objeto de direitos correspondentes (RO) 1933, que permite que o usuário decifre o conteúdo do serviço requisitado. Na incorporação, o objeto de direitos 1933, tipicamente não contêm as chaves de IPSec 1905.

O dispositivo de recepção processa a rajada de fatia de tempo com o módulo de processamento 1927. Os pacotes recebidos são decifrados pelo módulo de decriptografia 1929 com uma chave fornecida pelo módulo de extração de chave 1931, de modo a obter o conteúdo 1935. As chaves são determinadas do objeto de direitos 1933. As chaves são distribuídas tipicamente em um carrossel como arquivos SA de DRM protegido. O objeto de direitos 1933 permite ao dispositivo de recepção 1926 extrair as chaves.

A figura 20 mostra um sistema 2000 que suporta os serviços de DVB-H IPDC de acordo com uma incorporação da invenção. O conteúdo de multimídia 2001 (que corresponde aos datagramas de conteúdo) é cifrado pelo módulo de criptografia 2003 aplicando as chaves 2005 de IPSec. O sistema 2025 de transmissão obtém ambos os datagramas de conteúdo cifrados do módulo de criptografia 2003 e as chaves correspondentes de DRM 2009. O sistema de transmissão 2025 forma os datagramas correspondentes que contêm as chaves correspondentes para criptografar os datagramas de conteúdo. O sistema de transmissão 2025 insere os datagramas de conteúdo cifrado e os datagramas correspondentes em uma rajada de fatia de tempo, que é transmitido para o dispositivo de recepção 2026 em um canal de comunicações. Enquanto a figura 20 não mostra explicitamente um módulo de rádio, a incorporação pode fornecer a potencialidade de sinal sem fio a fim transmitir a rajada de fatia de tempo para o dispositivo de recepção 2026 em um canal sem fio.

O dispositivo de recepção 2026 processa uma rajada de fatia de tempo, no qual os datagramas de conteúdo cifrado e os datagramas correspondentes (que contêm as chaves correspondentes que são usadas para criptografar os datagramas de conteúdo recebidos) são separados (demultiplexado) pelo módulo de processamento de rajada 2027. Na incorporação, o dispositivo de recepção 2026 compreende um receptor de banda larga para receber os sinais de DVB que incluem rajada de fatia de tempo e um transceptor para comunicações bidirecionais em uma rede sem fio. O serviço de suporte de comunicações bidirecionais requisitam por um usuário, o serviço de mensagens de OMA e a instalação do módulo de conexão e segurança. A incorporação suporta as configurações diferentes de sinal, em que as chaves são incluídas em uma chave de fluxo separada ou em que chaves são incluídas em componentes multimídia como discutido anteriormente com as figuras 4-16. O módulo de extração de chave 2031 extrai as chaves dos datagramas correspondentes a fim de decifrar os datagramas conteúdo decifrado 2035 para uma aplicação (não mostrada) de modo que o conteúdo possa ser apresentado.

Adicionalmente, o objeto de gerenciamento de direitos 2023 (conforme

determinado pelo gerador de objeto de direitos 2022) é transmitido separadamente para o dispositivo de recepção 2026 recebe o objeto de direitos 2033 para determinar se o dispositivo de recepção 2026 é permitido processar o conteúdo recebido.

A figura 21 mostra um diagrama de fluxo 2100 para transmitir dados para os serviços de DVB-H IPDC no sistema 2000 de acordo com uma incorporação da invenção. Na etapa 2101, o aparelho de transmissão (por exemplo, sistema de transmissão 2025) determina se um datagrama de conteúdo obtido deve ser incluído na rajada de fatia de tempo atual. Se não, a rajada de fatia de tempo (com os datagramas de conteúdo e chaves associadas obtidos anteriormente) é enviada para o dispositivo de recepção na etapa 2109.

Se o datagrama de conteúdo obtido for incluído na rajada da fatia de tempo atual, a etapa 2103 determina a chave correspondente e criptografa o datagrama de conteúdo com a chave na etapa 2105. Na etapa 2107, o datagrama de conteúdo cifrado e a informação de chave correspondente (que corresponde a um datagrama correspondente que pode ser incluído no componente de multimídia ou em uma chave de fluxo) é inserido na rajada de fatia de tempo atual.

A figura 22 mostra um sistema 2200 que suporta os serviços de DVB-H IPDC de acordo com uma incorporação da invenção. Na figura 22, os elementos 2201, 2203, 2205, 2222, 2223, 2227, 2229, 2231, 2233, e 2235 correspondem aos elementos 2001, 2003, 2005, 2022, 2023, 2027, 2029, 2031, 2033, e 2035, conforme mostrado na figura 20. Como com sistema 2000, o sistema 2200 transmite datagramas de conteúdo e a informação chave correspondente no mesmo rajada de fatia de tempo. A informação chave é fornecida ao sistema 2225 da transmissão pelo gerador de chave de mensagem 2206. O gerador de chave da mensagem pode adicionalmente criptografar as chaves de modo que a informação de chave cifrada é transmitida para o dispositivo de recepção 2226 pelo sistema de transmissão 2225. O DRM 2209, conjuntamente com o gerador de objeto de direitos 2222, fornece o objeto de direitos 2233 que corresponde ao serviço desejado de DVB-H IPDC para o dispositivo de recepção 2226.

Os arquivos de política de IPSec 221 (que podem conter informação associação de segurança) são transmitidos separadamente no carrossel AS 2221 do serviço (conteúdo) e mensagens de chave que são multiplexadas e transmitidas usando o fatiamento de tempo IPDC. Na incorporação, o carrossel AS 2221 é transmitido como parte do guia de serviço eletrônico. (ESG).

A figura 23 mostra um sistema 2300 que suporta serviços de DVB-H IPDC de acordo com uma incorporação da invenção. O sistema 2300 suporta o acesso condicional (CA) que pode fornecer um segundo nível de criptografia usando uma chave privativa correspondente. (como será discutido com figura 26, as chaves de IPSec podem ser cifradas pelo gerenciamento de direitos digitais (DRM) bem como por um módulo de CA.) O dispositivo de recepção 2326 compreende uma seção de receptor e uma seção de terminal. A seção de receptor executa o processamento de rajada, demultiplexação e gerenciamento de chave. A seção de receptor inclui também a instalação de conexão em CA e a decriptografia da chave. O DRM 2351 envia o pacote de instalação de conexão CA 2353 para o DRM 2314, de modo que um novo módulo de conexão novo CA é instalado no dispositivo de recepção 2326 como será discutido adicionalmente com a figura 27. A decriptografia de chave é executada em um ambiente seguro de processamento. A seção de terminal executa o processamento de decriptografia de chave além da decriptografia (que corresponde ao módulo 2329 de decriptografia) e a sintetizar do conteúdo (que corresponde ao conteúdo 2335).

A criptografia de chaves 2305, (que é usada para criptografar o conteúdo 2301, pelo módulo de criptografia 2303), é executado pelo módulo de criptografia de chave 2311. O módulo de criptografia de chave 2311compreende o módulo 2308 de CA e o DRM 2309. Assim, o módulo de criptografia de chave 2311 pode fornecer dois níveis de criptografia. Ambas as informações de chave cifrada e os datagramas de conteúdo são incluídos na mesma rajada de fatia de tempo pelo sistema de transmissão 2325.

De maneira correspondente, a criptografia da informação de chave recebida é executada pelo módulo de decriptografia de chave 2317. O módulo de criptografia

chave 2317 compreende o módulo 2315 de DRM 2314 e de CA. O módulo de decriptografia de chave 2317 executa dois níveis de decriptografia que correspondem aos dois níveis da decriptografia. A rajada que processa o módulo 2327 decifra os datagramas de conteúdo recebidos usando as chaves decifradas fornecidas pelo gerenciador de chave 2313. Os datagramas de conteúdo recebidos são decriptografados pelo módulo 2329 da seção de terminal. O gerenciador de chave 2313 recebe a informação de chave que é demultiplexada pelo módulo 2327 e envia a informação de chave ao módulo de decriptografia de chave 2317 (que é associado com um ambiente confiável) para a decriptografia de DRM e de CA.

Na incorporação, o objeto de direitos (RO) é transmitido como uma mensagem de OMA DRM 2 (de acordo com a proposta *Open Mobile Alliance Digital Rights Management Version 2.0*) do DRM 2309 para DRM 2314. O objeto de direitos é transmitido tipicamente separado das rajadas de fatia de tempo.

Figura 24 mostra o aparelho 2400 que suporta um sistema de transmissão (por exemplo, 2025, 2225, e 2325) como mostrado nas figuras 20, 22, e 23 de acordo com uma incorporação da invenção. Na incorporação, o aparelho 2400 executa as funções associadas tipicamente com uma camada de ligação (a segunda camada do modelo do protocolo OSI). O processador 2405 obtém os datagramas cifrados de um módulo de criptografia (não mostrado) através da interface de criptografia 2401 e a informação de chave correspondente de um gerador de chave (não mostrado) através da interface de chave 2403. A interface de transmissão 2407 codifica os datagramas para a correção de erro para diante no dispositivo de recepção, executa o encapsulamento multiprotocolo, e formata a rajada de fatia do tempo com os datagramas codificados. (Na incorporação, os datagramas incluem ambos os datagramas de conteúdo e os datagramas correspondentes que contêm as chaves.).

Figura 25 mostra o aparelho 2500 para um dispositivo de recepção (por exemplo, dispositivos de recepção 1926, 2026, 2226, e 2326 como mostrado nas figuras 19, 20, 22, e 23, respectivamente) que recebem uma transmissão multimídia e que aplique chaves de IPSec de acordo com uma incorporação da invenção. O

aparelho 2500 processa uma rajada de fatia do tempo (por exemplo, a rajada de fatia de tempo 2501 e 2503) a fim de extrair os datagramas de conteúdo e a chave de fluxo associada. Na incorporação mostrada na figura 25, a rajada de fatia de tempo 2501 ou o rajada de fatia de tempo 2503 tem datagramas de conteúdos (por exemplo, datagramas de conteúdos 2505, 2507, e 2509) com pacotes IP encapsulados ESP que contêm o conteúdo de serviço e os datagramas chaves correspondentes (por exemplo, datagrama correspondente 2511) compreendendo mensagens- chave de UDP. As chaves em uma mensagem-chave de UDP podem ser protegidas por DRM.

O aparelho 2500 é capaz de distinguir entre o conteúdo de serviço e as mensagens-chave. Conseqüentemente, o módulo de receptor 2551 separa datagramas de conteúdos dos datagramas chaves. Na incorporação, os datagramas chaves são dados um nível de uma prioridade mais elevada do que datagramas de conteúdo pelo aparelho transmissor (não mostrado). Na incorporação, o nível da prioridade associado com um datagrama é indicado por um campo, por exemplo, um tipo de campo de serviço (ToS) ou de um campo diferenciado dos serviços. Assim, os datagramas chaves são enviados à pilha de IP 2553 IP antes dos datagramas de conteúdo correspondentes de modo que mais tempo possa ser distribuído para a chave que processa pelo módulo de decriptografia de chave 2555. O módulo de decriptografia de chave é apresentado chaves decifradas da pilha de IP 2553 através do gerenciador de chave 2559.

As incorporações mostradas nas figuras 17 e 25 incluem as chaves na mesma rajada de fatia de tempo como o datagrama de conteúdo associado. Entretanto, em uma outra incorporação, as chaves em uma rajada de fatia de tempo são associadas com a decriptografia de datagramas de conteúdo que são contidos na rajada de fatia de tempo seguinte, assim permitindo mais tempo para processamento de chave. Outras variações são possíveis. Por exemplo, um número de chaves para uso no conteúdo de decriptografia pode ser fornecido em um único rajada de fatia de tempo e as chaves podem então ser usadas para uma pluralidade de rajadas subseqüentes de fatia do tempo.

As chaves decifradas são apresentadas para o módulo de IPSec 2557 de modo que os datagramas de conteúdo associados na pilha de IP 2553 possam ser decriptografados e apresentados ao cliente 2561.

Figura 26 mostra o aparelho 2600 que recebe uma transmissão em broadcast de multimídia e que decifra as chaves recebidas 2601 de IPSec de acordo com uma incorporação da invenção. O gerenciador de chave 2653 distribui a chave cifrada de IPSec ao servidor de DRM 2655 para decifrar um segundo nível de criptografia usando um algoritmo público de decriptografia e uma chave privativa 2603. O servidor de DRM 2655 de retorna a chave de segundo-nível decifrada 2607 ao gerenciador de chave 2653. Se o gerenciador de chave 2653 determinar que a chave esteja cifrada com uma criptografia de primeiro nível de criptografia, o gerenciador e chave 2653 distribui a chave decifrada de segundo-nível ao módulo de software de conexão 2657 de CA. O módulo conexão de CA 2657 utiliza um algoritmo secreto de decriptografia e uma chave confidencial 2605 para decifrar a chave decifrada de segundo nível 2607. Em uma incorporação da invenção, o algoritmo secreto de decriptografia corresponde a um algoritmo comum desembaralhar de DVB (CSA), que está disponível no *European Telecommunications Standards Institute* (ETSI). O módulo de software de conexão de CA 2657 retorna a chave decifrada 2609 chaves para o gerenciador de chave 2653, que envia a chave decifrada 2609 à pilha de IP 2651.

Na incorporação, o módulo de conexão de CA 2657 executa uma decriptografia em primeiro nível que é opcional e que é baseada em um método CA de operador específico que inclui uma chave privativa associada e um algoritmo associado de decriptografia. O segundo-nível de criptografia é baseado em um padrão aberto, por exemplo, OMA DRM2. Porque o primeiro nível de criptografia é opcional, o gerenciador de chave 2653 determina se um primeiro nível de criptografia foi aplicado à chave decifrada em segundo-nível 2607. Sendo assim, o gerenciador de chave 2653 distribui a chave decifrada em segundo-nível 2607 ao módulo de software de conexão CA 2657. Se não, o gerenciador de chave 2653 envia chave decifrada em segundo nível 2607 diretamente à pilha de IP 2651 porque

a chave decifrada em segundo-nível 2607 está completamente decifrada.

Na incorporação, o gerenciador de chave 2653 determina se a chave decifrada de segundo-nível 2607 foi cifrada em primeiro nível examinando um indicador associado de criptografia (não mostrado), por exemplo, um cabeçalho ou um campo de mensagem. O indicador associado de criptografia indica 'SIM' se a chave decifrada em segundo nível 2607 for cifrada em primeiro nível e 'NÃO' se a chave decifrada em segundo-nível 2607 não foi cifrada em primeiro nível. Se a chave decifrada em segundo nível 2607 for cifrada em primeiro nível, o indicador associado de criptografia não é cifrado em primeiro nível.

A figura 27 mostra o sistema 2700 para desdobrar um novo módulo de segurança de software de conexão 2701 no dispositivo de recepção 2750 de acordo com uma incorporação da invenção. O módulo de segurança de software de conexão 2701 é formatado como um pacote de instalação 2705 (por exemplo, um arquivo SIS como suportada por Symbian). O pacote de instalação 2705 é protegido (por exemplo, com OMA-DRM2) para formar ao pacote protegido 2707 e distribuído a um dispositivo de recepção usando um mecanismo de distribuição. A incorporação suporta diferentes canais de comunicações em um mecanismo de distribuição, incluindo um canal de comunicações sem fio em que o dispositivo de recepção é um terminal sem fio. O pacote protegido recebido 2707 é dirigido ao instalador 2751 da aplicação, que é uma aplicação confiável. O instalador 2751 da aplicação extrai o novo módulo de segurança de software de conexão do pacote protegido 2707 e substitui o módulo de segurança de software de conexão 2755 atual que é instalado atualmente no dispositivo de recepção 2750 com o novo módulo de segurança de software de conexão 2701. A fim de extrair o novo módulo de segurança de software de conexão 2701, o dispositivo de recepção 2750 recebe o objeto de direitos 2703 que é processado por DRM 2753. Conseqüentemente, o DRM 2753 indica ao instalador 2751 da aplicação que a recolocação do módulo do software da segurança de conexão está permitida.

Nas incorporações da invenção, as configurações de componentes como mostradas nas figuras 3-16 podem ser incorporadas nos sistemas como mostrado

nas figuras 20, 22, e 23.

Métodos e aparelho para fornecer direitos sobre o fluxo de conteúdos de granulosidade fina.

Enquanto a discussão acima fornece os detalhes a respeito das incorporações de métodos e os aparelhos para o uso em fornecer o conteúdo em fluxo continuo que pode ser usado com os métodos e o aparelho discutidos abaixo, os outros métodos e aparelho podem também ser usados.

O controle dos direitos para o fluxo continuo de conteúdo é um tanto difícil porque há uma quantidade limitada de largura de faixa disponível. Uma solução natural para o problema deve criar de maneira normal os RO's com os períodos de validade muito curtos, contendo possivelmente a mesma chave de serviço, mas com direitos diferentes de uso. Isto pode ser incômodo na prática embora, porque as chaves de serviço mudam muito menos freqüentemente do que, por exemplo, programas de televisão em um canal de televisão. Como uma outra solução, os RO's ou expressões de direitos poderiam ser distribuídas em KSMs. Enviando RO's completos freqüentemente no KSM consumiria uma pequena largura de faixa, entretanto, como deve ser dirigido a cada assinante (ou a um grupo de assinantes) individualmente, de modo que somente aqueles que pagaram os direitos. Mesmo se os direitos são os mesmos a todos os assinantes, e o acesso ao KSM está limitado por outros meios de modo que o KSM necessite conter somente a parte de expressão dos direitos de um RO, a expressão própria dos direitos pode requerer um número considerável de bits, particularmente se for usada uma Linguagem de Expressão de Direitos e do tipo XML. As soluções típicas para este problema envolvem vários métodos de compressão para binarizar a expressão dos direitos, ou para limitar os direitos possíveis a alguns casos predeterminados ("uso indica"). Entretanto, estas soluções potenciais não fornecem adequadamente RIs com um controle suficientemente refinado em uma largura de faixa em uma maneira amigável de modo a ser prática para a adoção.

Olhando primeiro para a figura 28, um exemplo da técnica anterior é fornecido. O conteúdo é cifrado com uma chave de conteúdo (CK) e fornecido ao um

receptor (não mostrado). O receptor obtém separadamente a RO 2860 que inclui o CK ao juntamente com um conjunto de direitos de uso. O conteúdo cifrado recebido pode então ser visto ou de outro modo usado como fornecido par no RO de acordo com o os direitos de uso obtidos. Entretanto, este método da técnica anterior não particularmente adequado para conteúdo de fluxo continuo.

Voltando à figura 29, é mostrado um aspecto ilustrativo da presente invenção. O conteúdo de fluxo continuo é fornecido a um transmissor de broadcast e é cifrado no dispositivo de criptografia 2915 usando TK 2925. O receptor (não mostrado) é fornecido com o SK 2950 através de um KSM 2940, o KSM 2940 sendo formado pela criptografia 2930 usando o SK 2950 juntamente com TK 2925. A chave de fluxo, que fornece o KSM, é anunciada aos usuários com endereço IP e número de porta. Como o TK 2925 é cifrado com SK 2950, o dispositivo usa RO 2960, que contém o SK 2950, para decifrar o KSM 2940 de modo a ser capaz de decifrar o conteúdo de fluxo continuo 2910. Além do fornecimento do SK 2950, o RO 2960 também fornece os direitos de uso 2965.

Tipicamente, o TK mudará periodicamente. A figura 31 fornece um exemplo deste. Como observado, o TK muda diversas vezes enquanto o SK for válido. Na prática, o número de mudanças no TK pode ser muito mais elevado. Quando o TK muda, um KSM novo 2940 (figura 29) é fornecido ao receptor com o TK novo cifrado pela mesma SK 2950. Assim, quando a SK 2950 permanecer o mesmo, o RO 2960 permitirá que o receptor decifre o conteúdo de fluxo continuo. Quando o SK muda, entretanto, um RO novo é necessário de modo que o KSMs enviado ao dispositivo possa ser decifrado e o conteúdo de fluxo continuo ser usado conforme permitido. Geralmente, os RO's comprados de RIs devem ter períodos relativamente longos de validade para tornar o mecanismo de DRM praticável. Em uma incorporação, uma vez que um RO principal é obtido, o RO secundário pode também ser obtido. Como discutido acima em referência às chaves nas figuras 4-16, em uma incorporação da invenção os TKs são distribuídos no KSM antes de seu período de validade de modo que o usuário (dispositivo) possa decifrar a combinação de chave(s) e bits antes que o conteúdo de fluxo continuo real (ou o segmento dele) seja recebido. Do mesmo

modo, o RO pode ser adquirido antes do período de validade.

Como observado acima, os direitos são expressos tipicamente em REL. Para dirigir-se à introdução de direitos do uso em uma solução amigável de largura de faixa que fornece a precisão suficiente de controle, uma nova variável REL chamada categoria de programa pode ser usada. A variável de categoria de programa pode ser pequena, por exemplo, 2 bits, enquanto que fornece o uso suficiente de controle de direitos para algumas aplicações. Usando três ou o mais bits, entretanto, fornece o controle refinado e podem conseqüentemente ser desejável. O tamanho da variável, entretanto, é um tanto dependente do método de separação. Em algumas incorporações da invenção, em vez de usar uma variável separada, a informação de categoria de programa é embutida em ou concatenada com algum outro identificador, tal como o identificador do conteúdo, do programa ou do serviço.

Olhando a figura 30, os vários provedores de conteúdo (PC) fornecem o conteúdo a um radiodifusor. Além disso, vário RIs comunicam-se com o radiodifusor, para determinar as categorias de programa ou para fornecer as categorias de programa, como será discutido abaixo. Deve-se notar que o RIs e o CPs podem ou não ser as mesmas entidades. O conteúdo é cifrado e transmitido então aos receptores. Deve-se notar que a criptografia de conteúdo pode ser feita pelo provedor de conteúdo ou pelo radiodifusor e pelas chaves de criptografia são distribuídas conformemente entre quem criptografa e o editor de direitos (RI).

Por exemplo, considere um serviço de broadcast e um dispositivo. De um RI particular, o dispositivo obtém um RO de um RI particular para acessar um certo conteúdo, e há uma descrição de REL dos direitos de uso para o conteúdo no RO. Enquanto a descrição for estática para o período da validade, o REL pode conter os direitos do uso que são condicionais à variável da categoria de programa REL. Assim, a medida que KSM's mudam o valor da variável da categoria de programa REL, os direitos de uso (condicional) atualmente podem de fato mudar.

O valor da variável da categoria de programa pode ser derivado do KSM's de serviço de transmissão em questão em duas maneiras alternativas, discutidas abaixo. Desde que KSM's são enviados muito freqüentemente, as mudanças de

valor da variável da categoria de programa REL e daqui as mudanças nos direitos de uso atualmente eficazes podem ser muito refinadas em tempo. Para conservar a largura de banda de broadcast, contudo, a quantidade de dados novos adicionados ao KSM's para indicar a variável de categoria de programa REL é, de preferência, minimizada.

Antes de discutir como as categorias de programa podem ser fornecidas ao receptor, a figura 32 mostra um exemplo de várias partes do conteúdo. Por exemplo, o conteúdo de fluxo continuo 3210 pode incluir uma categoria 3215 de notícias, uma categoria 3217 de esportes, uma categoria de documentário 3219 e uma categoria 3221 de filme. A categoria de notícias pode adicionalmente ser dividida em categorias de n 3215-1, 3215-2..., 3215-n. Estas categorias podem, por exemplo, mas sem limitação, representar manchetes, a notícia doméstica, a notícia estrangeira, etc... Similarmente, as categorias 3217 de esportes podem também ainda ser divididas em categorias tais como destaques, escores, a transmissão ao vivo, etc... Alternativamente, as categorias não podem ter qualquer coisa para fazer com o tipo de conteúdo, mas são definidas simplesmente para cada um conjunto diferente de direitos diferentes de uso. Por exemplo, as categorias podem ser 'altamente restritas', 'um tanto restritas', 'normal' e 'liberal', refletindo as permissões dadas ao usuário.

Abaixo estão dois métodos possíveis de prover KSM, a diferença mais significativa é a necessária interação entre o radiodifusor e os RI's. Deve ser observado que alguma combinação dos dois métodos pode ser usada.

Olhando o primeiro método de determinar a categoria de programa para o REL, em um aspecto da invenção, o radiodifusor "classifica" o conteúdo de fluxo continuo em categorias diferentes. Por exemplo, o número da categoria do programa pode ser relativamente pequeno, como 4 categorias diferentes, ou pode ser relativamente grande, como 256 categorias diferentes de programa. Naturalmente, os bits adicionais serão necessitados como o número de aumentos das categorias do programa, assim dois bits podem fornecer a informação a respeito de quatro categorias do programa quando 8 bits forem necessários fornecer 256 categorias de

programa. Por exemplo, em um serviço portátil da transmissão de televisão, cada programa de televisão é categorizado em um número de categorias de programa, que podem incluir a notícia, shows de valor baixo (iv), shows de valor alto (hv), esportes de Iv, esportes de hv, filmes velhos, filmes novos, etc. Os RIs não podem influenciar as categorias (ajustado pelo radiodifusor e comum a todo o RIs)5, mas podem livremente usar a faixa de valor variável (por exemplo, de 0... 255) de categoria de programa amplo REL de programa em seus direitos de uso expressos em REL no RO que fornecem ao dispositivo. Tipicamente, entretanto, um número menor, tal como 12-16 categorias de programa serão mais práticas. Nenhuma comunicação extra entre o radiodifusor e o RIs é preciso. Cada um de tais segmentos de programa pode ser associado a um conjunto de direitos de uso (no relatório da invenção: a categoria de programa) incluindo 'representação ao vivo', 'o armazenamento e a exposição por 48 horas, 'armazenamento e exposição indefinidamente', 'retransmissão e cópia (encaminhamento) indefinidamente' ou alguns outros tipos similares.

Assim, o RO pode incluir os direitos condicionais expressos em REL que dependem do valor da categoria de programa. Assim, um usuário pôde comprar direitos completos tais que o RO fornece os direitos permissíveis máximos para o conteúdo. Alternativamente, o usuário pode selecionar um RO livre promocional que forneça direitos muito mais limitados e pode somente permitir a exposição das partes do conteúdo de fluxo continuo. Periodicamente o RO será atualizado porque o SK muda assim os direitos do uso podem variar de RO para RO. O usuário recebe o um ou mais RO quando requisitar / comprar / assinar / renovar o serviço ou as partes dele. Em uma incorporação da invenção o usuário pode primeiramente receber um RO 'principal ' e promover o RO 'secundário' pode ser adquirido ou criado mais tarde. Se o usuário não requisitar (comprar / assinar) o segmento de programa que está sendo recebido, o usuário é informado naquele ('você não tem direitos a este segmento de programa/ (programa)) e/ou é informado como comprar os direitos.

Em um outro aspecto da invenção, como mostrado em figura 33, o RIs

ajustaram as categorias e as comunicou ao radiodifusor, que põe então as categorias no KSMs. Desde que haja RIs múltiplos, pode ser útil limitar o número dos bits que são permitidos por RI a dois bits. Em tal caso, a faixa de categoria de programa poderia ser 0... 3. Que a faixa, entretanto, seria específica de RI, e poderia conseqüentemente relacionar-se diretamente com os direitos do uso de uma parte particular do conteúdo de fluxo continuo (melhor que tipo de conteúdo de fluxo continuo dentro uma forma mais genérica). Em tal caso, forneça ao invés de então um único RO, quatro que o RO pode ser fornecido, cada um com um conjunto de direitos de uso configurados pelo RI.

No mecanismo de RO que está sendo usado na figura 33, deve haver meios de indicar que valor de categoria se refere a que RI, preferivelmente sem usar as identidades de RI (que são maiores de dois bits). Em uma incorporação, cada KSM 3340 contem um vetor de valores de categoria de N (para algum N) onde cada valor de categoria pode ser dois bits. Em uma outra incorporação da invenção, os valores de categoria podem ser mais de dois bits. Os RO's forneceu ao que receptor contem um conteúdo de RI na faixa 1... N de modo que o valor da categoria em cada um do RI_1 com RI-N correspondesse a um conjunto de RO. Ainda em outras incorporações da invenção um ou mais bit ou as combinações dos bits dentro de KSM podem ser usados para valores da categoria. Quando o KSM puder incluir o vetor, outros formatos e protocolos podem ser usados para fornecer o valor da categoria associado com o RI. Além disso, em uma incorporação o número bits e/ou de combinações de bit dentro do vetor podem ser reservados para o uso futuro.

Em uma outra incorporação da invenção, um número bits e/ou de combinações de bit no KSM, que pode ou não pode ter sido reservado para outras finalidades, podem ser traçados aos valores da categoria ou ser interpretados como valores da categoria. Além, determinadas posições dentro do KSM poderiam ser usadas fornecer uma indicação a respeito de se um tipo de programa poderia ser visto. Um RO poderia determinar o que o valor da categoria baseasse no valor da categoria fornecido pelo KSM e olha então o lugar apropriado no KSM para determinar que direito do uso existiu, como se o conteúdo poderia ser indicado.

Porque cada RO poderia ser configurado para olhar em posições diferentes com o KSM para determinar os direitos do uso, o controle individualizado que pode variar com cada KSM poderia prontamente ser fornecido.

Como mostrado, o usuário recebeu neste caso quatro ROs, cada um com uma classe dos direitos do usuário. A vantagem de usar classes dos direitos do uso é que o número e o tamanho totais de objetos dos direitos podem ser menores do que no exemplo de um conjunto completo do RO se os direitos do uso forem oferecidos comprando no nível de segmentos de programa. Quando o usuário recebe o KSM que carrega o TK real, a combinação de bit na posição que corresponde à posição RI #1 permite que o usuário selecione o RO que corresponde a sua compra. Para o exemplo que um valor de O em RI #1 indicaria ROI, um valor de 1 indicaria R02, um valor de 2 indicaria que R03 e um valor de 3 indicariam o R04. Enquanto o TKs pode ser mudado do segmento de programa ao segmento de programa, o usuário pode usar seus direitos na maneira que requisitou (comprou). Deve-se notar que o usuário 'está escutando' o KSM que lhe foi anunciado (endereço IPe o número da porta).

Por exemplo, em um serviço portátil da radiodifusão de televisão, baseado em esquemas de programa de televisão, RIs escolhe uma das 4 categorias para cada programa, as comunica ao radiodifusor, e o radiodifusor a seguir inclui as categorias nos KSMs. Para um RI, as quatro categorias podem ser 1) interpretação ao vivo reservado somente, 2) armazenamento e para replay permitido 48 horas, 3) armazenamento e para replay reservado indefinidamente e 4) o armazenamento, replay e copia a outros dispositivos permitidos indefinidamente. Este exemplo, entretanto, é meramente ilustrativo e outras combinações da direito do uso podem ser fornecidas.

Na situação acima todos os compradores do conjunto de RO's do RI podem ter o mesmo conjunto de direitos. Por exemplo, um RI#J no KSM 3340 pode corresponder a um negocio de pacote particular enquanto um segundo RI#J+1 pode corresponder a um negócio de pacote diferente. Deve ser observado, entretanto, que a categoria de programa para cada RI é particular para o TK, assim o mesmo

conjunto de RO's pode fornecer diferentes direitos de uso para diferentes TKs, e adicionalmente, diferentes conjuntos de ROs podem fornecer diferentes conjuntos e/ou combinações de direitos de uso.

Assim, para um conjunto de ROs o ROI pode fornecer ver somente os direitos de uso enquanto um outro conjunto de ROs o ROI pode fornecer para deslocamento de tempo.

Ainda, em ambas as soluções, deve-se recordar que a condicionalidade com base nas categorias somente complementa o uso total de direitos no RO, fazendo-o mais dinâmico: muitos direitos de uso são prováveis ser incondicionais e assim não dependentes do valor da variável de categoria REL de programa. Do mesmo modo, em ambas as soluções, melhor que em fornecer a condicionalidade dentro dos direitos de uso de um único RO, a informação de categoria de programa enviada no KSM pode alternativamente ser usada para selecionar um conjunto de ROs completo, ou possivelmente um dos diversos RO secundário relacionado ao mesmo RO principal.

Assim, os aspectos da presente invenção fornecem uma maneira de largura de banda eficiente de distribuir os direitos aplicáveis a todos os assinantes, mas que podem variar o período de programa por programa e de período de tempo por período de tempo, enquanto ainda permitir a magnificência total do REL para definir aqueles direitos para cada categoria de programa. A invenção pode ser aplicada aos serviços de IPDC sobre DVB-T, DVB-H, MediaFLO, radiodifusão de OMA e outros sistemas.

Como pode ser apreciado por alguém versado na técnica, um sistema computadorizado com um meio legível por computador associado que contém instruções para controlar o sistema computadorizado pode ser utilizado para executar as incorporações exemplares que são aqui reveladas. O sistema computadorizado pode incluir pelo menos um computador tal como um microprocessador, um processador do sinal digital, e um circuito eletrônico periférico associado.

Quando a invenção foi descrita com respeito aos exemplos específicos

incluindo modalidades presentemente preferidas de realizar a invenção, aqueles versados na técnica apreciarão que há umas variações e umas permutações numerosas dos sistemas e das técnicas acima descritos que caem dentro do espírito e do escopo da invenção como determinado nas reivindicações apensas.

REIVINDICAÇÕES

1. Método para transmitir um fluxo de dados para o dispositivo, o método é **CARACTERIZADO** pelo fato de que compreende:

(a) transmitir o conteúdo streaming cifrado com a chave de tráfego;

(b) transmitir a mensagem de fluxo de chave cifrada com a chave de serviço, a mensagem de fluxo de chave incluindo a chave de tráfego; e

(c) prover os primeiros direitos do objeto com a chave de serviço, desse modo a chave de serviço permite a decifragem da mensagem de fluxo de chave e a mensagem de fluxo de chave permite a decifragem do conteúdo streaming.

2. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que (b) compreende:

(i) transmitir o primeiro valor de categoria de programa.

3. Método de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que (b) também compreende:

(ii) transmitir o segundo valor de categoria de programa, onde o primeiro valor de categoria é associado com o primeiro emissor de direitos e o segundo valor da categoria de programa é associado com o segundo emissor de direitos.

4. Método de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que o primeiro valor de categoria de programa e o segundo valor de categoria de programa são fornecidos no vetor, o primeiro e o segundo valores de categoria de programa respectivamente compreendem a primeira e a segunda posição no vetor.

5. Método de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que o primeiro e o segundo valores de categoria de programa são expressos com dois ou mais bits.

6. Método de acordo com a reivindicação 5, **CARACTERIZADO**

pelo fato de que também compreende:

(d) prover o segundo objeto de direitos, o terceiro objetos de direitos e o quarto objeto de direitos, onde o primeiro, o segundo, o terceiro de o quarto objetos de direitos formam um grupo de objetos de direitos.

7. Método de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que ao menos um dos primeiro e segundo valores de categoria de programa corresponde a um dos primeiro, segundo, terceiro e quarto objetos de direitos.

8. Método de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que o primeiro objeto de direitos inclui uma pluralidade de direitos de uso associados com uma pluralidade de valores de programa, desse modo o primeiro valor de programa transmitido corresponde a um de uma pluralidade de direitos de uso.

9. Método de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que também compreende:

(d) trocar a chave de tráfego; e

(e) repetir (a) e (b).

10. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 1.

11. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 2.

12. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 7.

13. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 8.

14. Dispositivo de leitura de computador **CARACTERIZADO**

pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 9.

15. Método para receber um fluxo de dados de um sistema de comunicação durante a sessão de multimídia, o método é **CARACTERIZADO** pelo fato de que compreende:

(a) receber um fluxo de dados cifrado, o fluxo de dados cifrado pela chave de tráfego;

(b) receber uma mensagem de fluxo de chave cifrada, a mensagem de fluxo de chave cifrada incluindo a chave de tráfego; e

(c) usar a chave de tráfego para decifrar o fluxo de dados.

16. Método de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que (c) compreende:

(d) decifrar a mensagem de fluxo de chave com a chave de serviço.

17. Método de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que também compreende:

(e) obter o objeto de direitos, o objeto de direitos incluindo a chave de serviço; e

(f) usar o fluxo de dados.

18. Método de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que (b) compreende:

(i) receber um valor variável de categoria de programa.

19. Método de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que (f) compreende:

(i) exibir o fluxo de dados.

20. Método de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que (f) compreende:

(i) armazenar o fluxo de dados.

21. Método de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o uso do fluxo de dados é controlado

pelo direito de uso associado com os direitos do objeto.

22. Método de acordo com a reivindicação 16, **CARACTERIZADO** pelo fato de que também compreende:

(e) repetir (a), (b), (c) e (d) após as mudanças da chave de tráfego.

23. Método de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o objeto de direitos também inclui o direito de uso associado com o valor variável da categoria de programa incluído na mensagem de fluxo de chave e (f) é controlado pelo direito de uso.

24. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 15.

25. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 16.

26. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 17.

27. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 18.

28. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 22.

29. Dispositivo de leitura de computador **CARACTERIZADO** pelo fato de que possui instruções executáveis de computador para executar os passos descritos na reivindicação 23.

30. Método para obter o fluxo de dados do sistema de comunicação, o método é **CARACTERIZADO** pelo fato de que compreende:

(a) receber o fluxo de conteúdo cifrado com a chave de tráfego;

(b) receber a chave de tráfego e o primeiro valor variável de categoria de programa cifrado pela chave de serviço;

(c) obter os direitos do objeto com a chave de serviço; e

(d) usar as chaves para decifrar o fluxo de conteúdo.

31. Método de acordo com a reivindicação 30, **CARACTERIZADO** pelo fato de que também compreende:

(e) usar o fluxo de conteúdo de acordo com o primeiro direito de uso no objeto de direitos que é associado com o valor variável de categoria de programa.

32. Método de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que também compreende:

(f) repetir (a) e (b) quando a chave de tráfego muda.

33. Método de acordo com a reivindicação 32, **CARACTERIZADO** pelo fato de que (b) também compreende:

(ii) receber o segundo valor variável de categoria de programa, o segundo valor variável de categoria de programa associado com o segundo direito de uso no objeto de direitos.

34. Método para transmitir os dados streaming para o receptor, o método é **CARACTERIZADO** pelo fato de que compreende:

(a) prover o objeto de direitos, o objeto de direitos incluindo a chave de serviço;

(b) transmitir a mensagem de fluxo de chave cifrada com a chave de serviço, a mensagem de fluxo de serviço incluindo a chave de tráfego; e

(c) transmitir o fluxo de dados, o fluxo de dados sendo cifrado com a chave de tráfego, onde a mensagem de fluxo de chave cifrada é transmitida antes da transmissão do fluxo de dados.

PI0612027-0

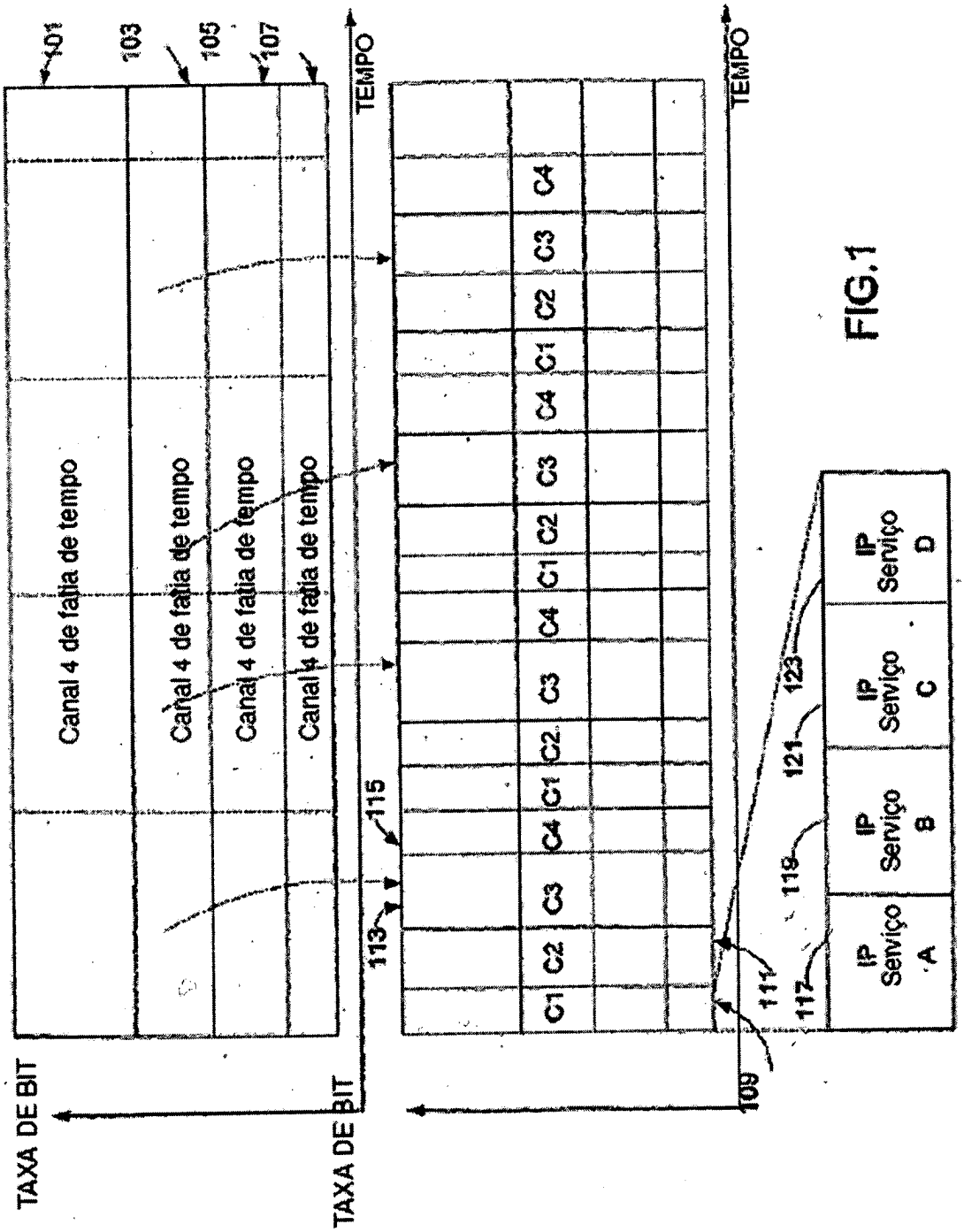


FIG.1

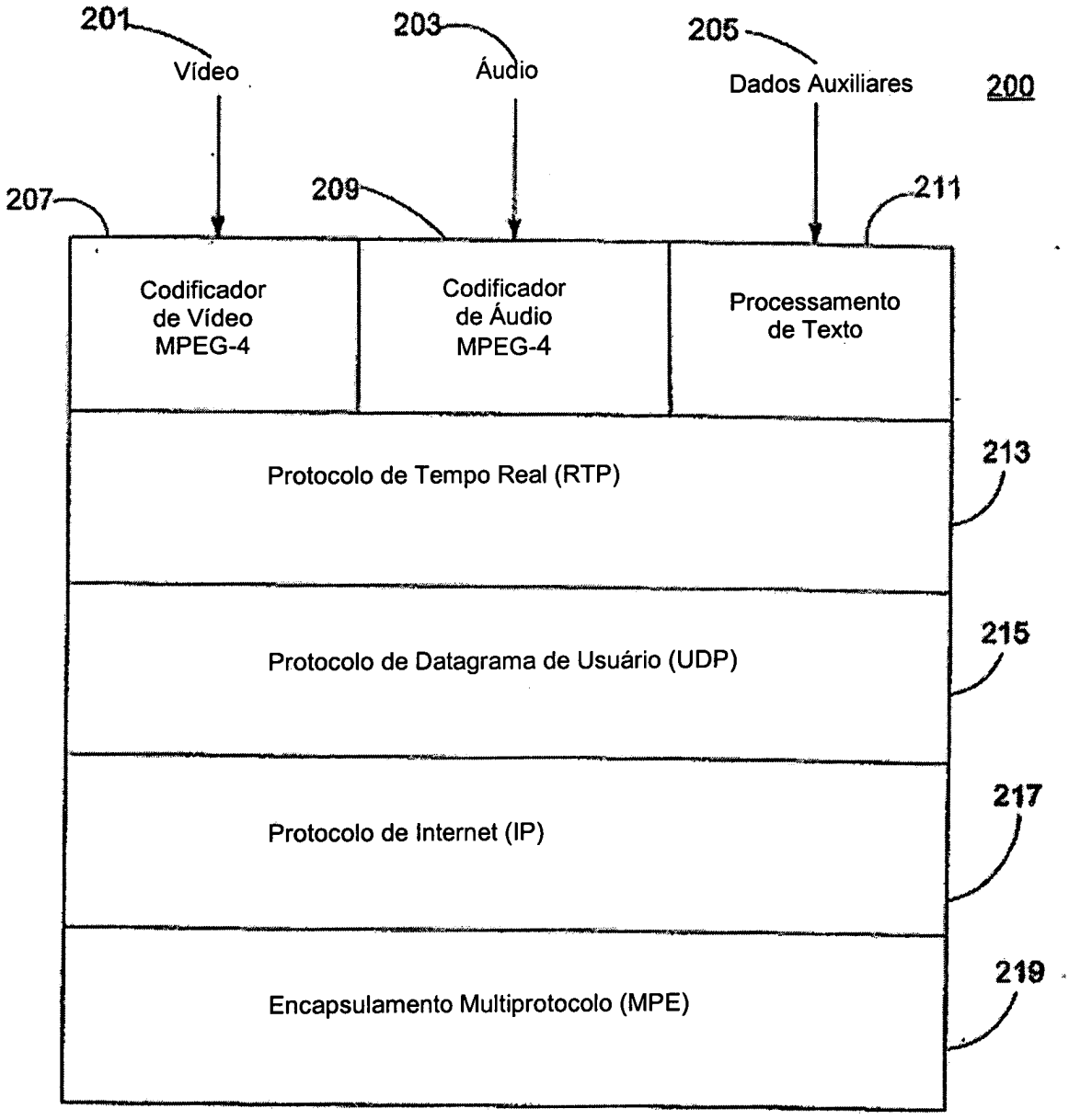

201
Vídeo
203
Áudio
205
Dados Auxiliares
200
207
209
211
Codificador de Vídeo MPEG-4
Codificador de Áudio MPEG-4
Processamento de Texto
213
Protocolo de Tempo Real (RTP)
215
Protocolo de Datagrama de Usuário (UDP)
217
Protocolo de Internet (IP)
219
Encapsulamento Multiprotocolo (MPE)

FIG. 2

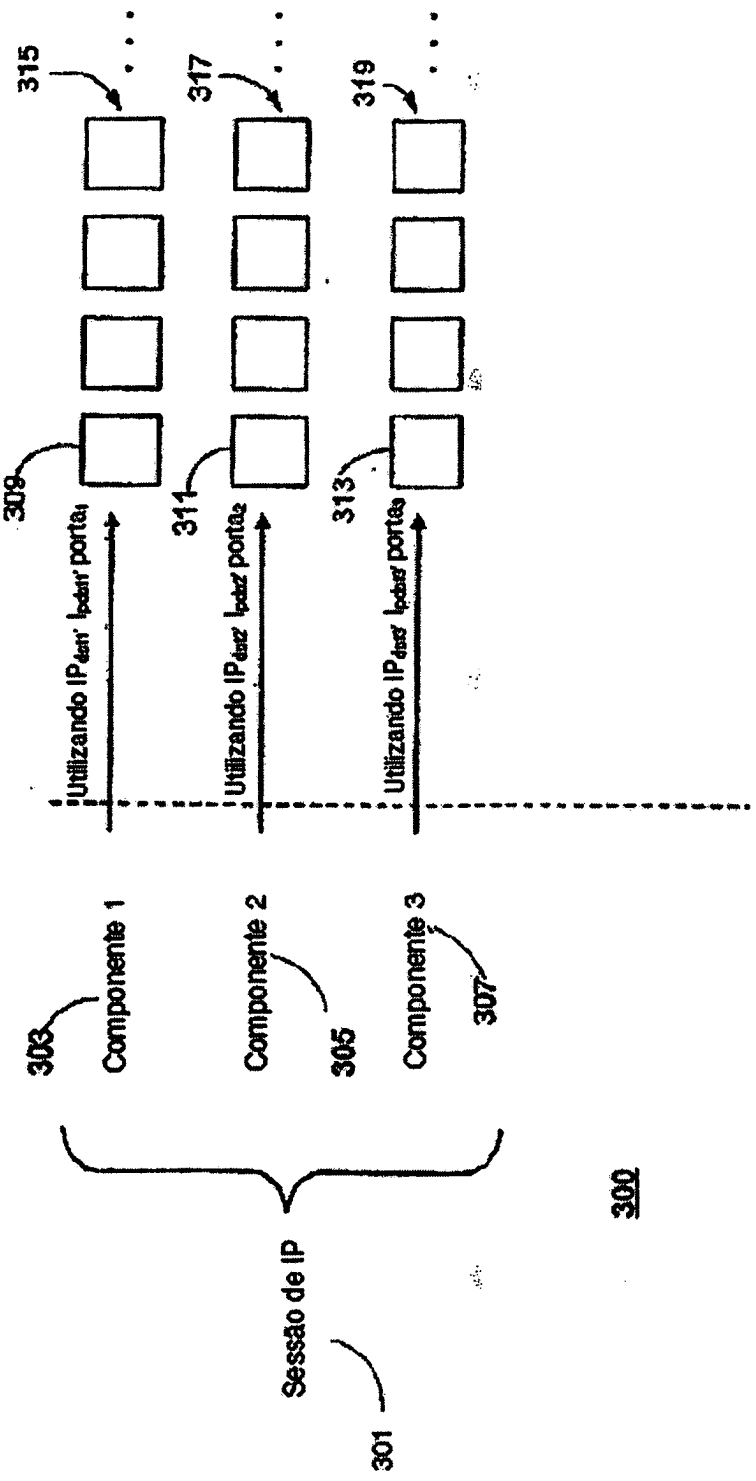

315
317
319
309
311
313
Utilizando IP dest1 porta1
Utilizando IP dest2 porta2
Utilizando IP dest3 porta3
Componente 1
Componente 2
Componente 3
303
305
307
Sessão de IP
301
300
Transmitido com um fluxo de pacotes

FIG. 3

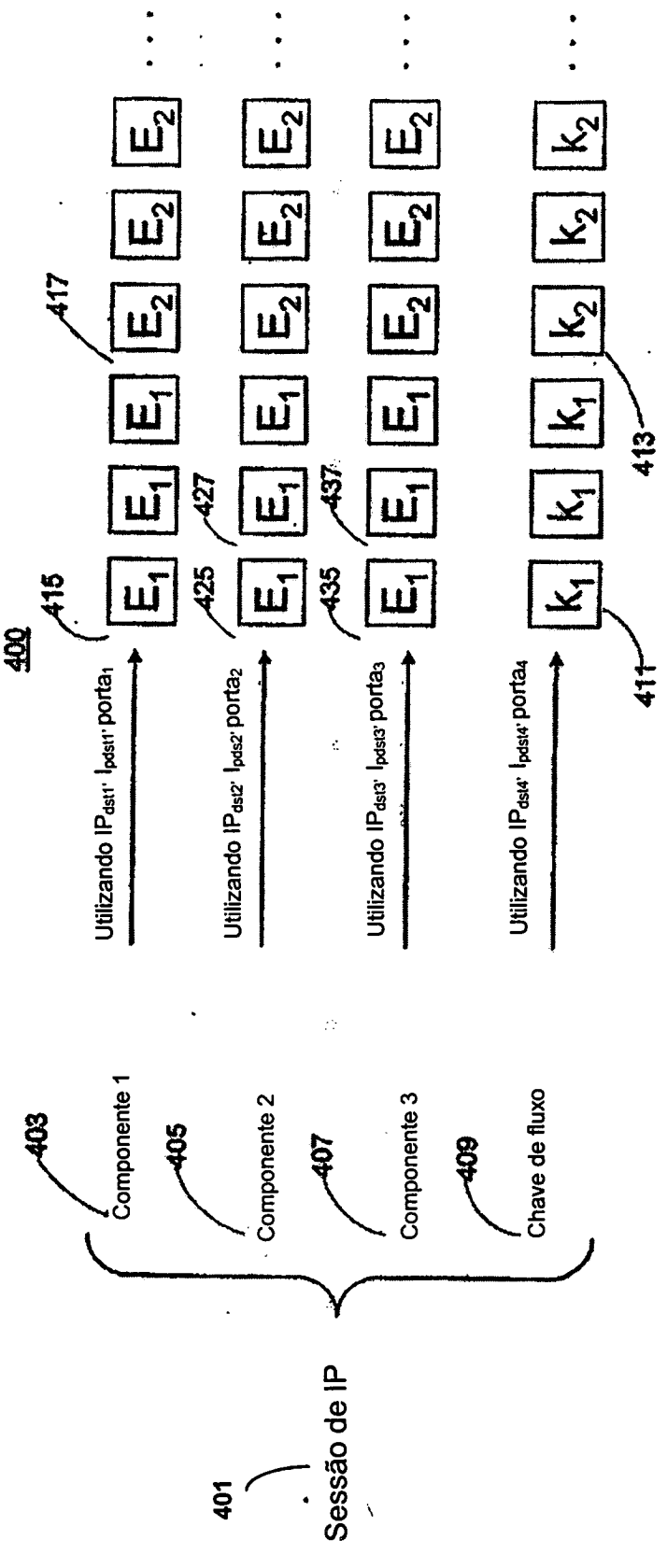

400
401
Sessão de IP
403
Componente 1
405
Componente 2
407
Componente 3
409
Chave de fluxo
411
413
415
417
425
427
435
437
Utilizando IPdst1, Ipds1, porta1
Utilizando IPdst2, Ipds2, porta2
Utilizando IPdst3, Ipdst3, porta3
Utilizando IPdst4, Ipdst4, porta4
E1
E2
K1
K2

FIG. 4

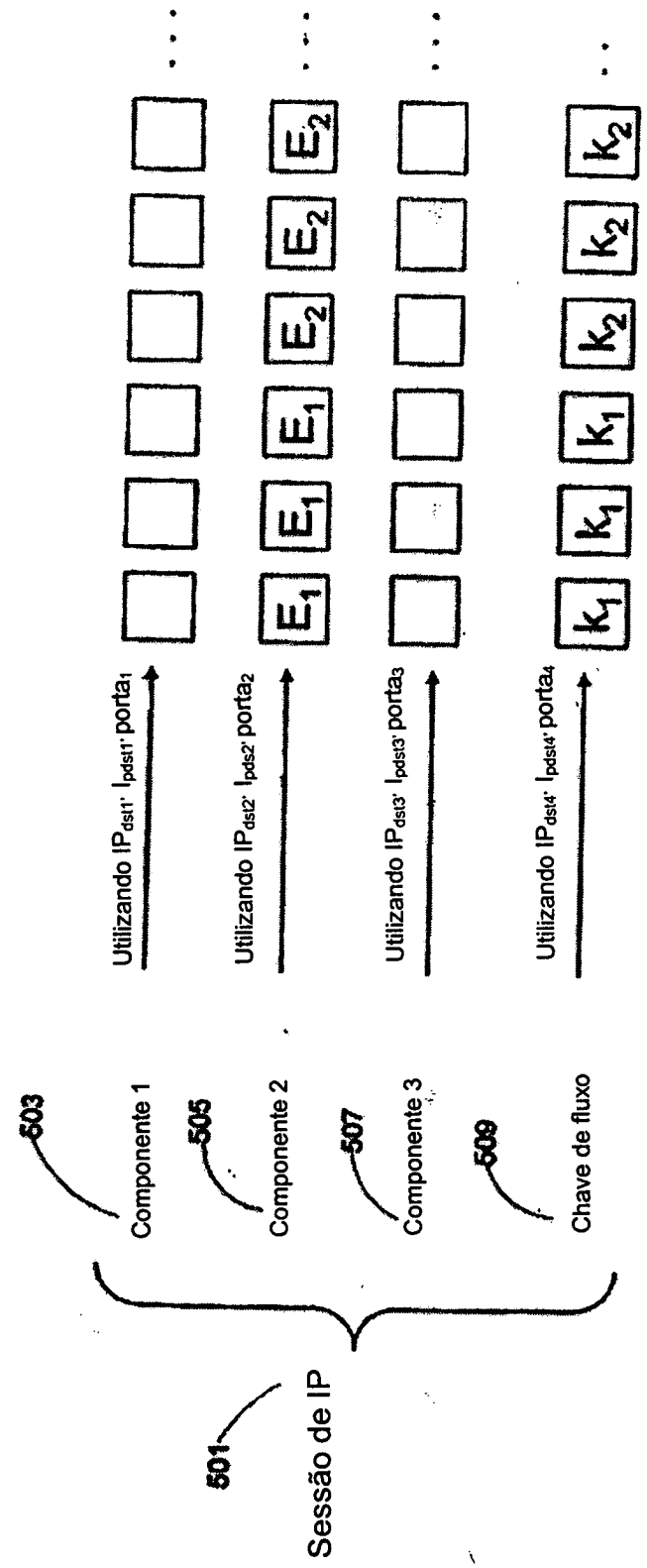

500
Utilizando IP_{dst1}, I_{pdst1}, $porta_1$
Utilizando IP_{dst2}, I_{pds2}, $porta_2$
Utilizando IP_{dst3}, I_{pdst3}, $porta_3$
Utilizando IP_{dst4}, I_{pdst4}, $porta_4$
503
Componente 1
505
Componente 2
507
Componente 3
509
Chave de fluxo
501
Sessão de IP

FIG. 5

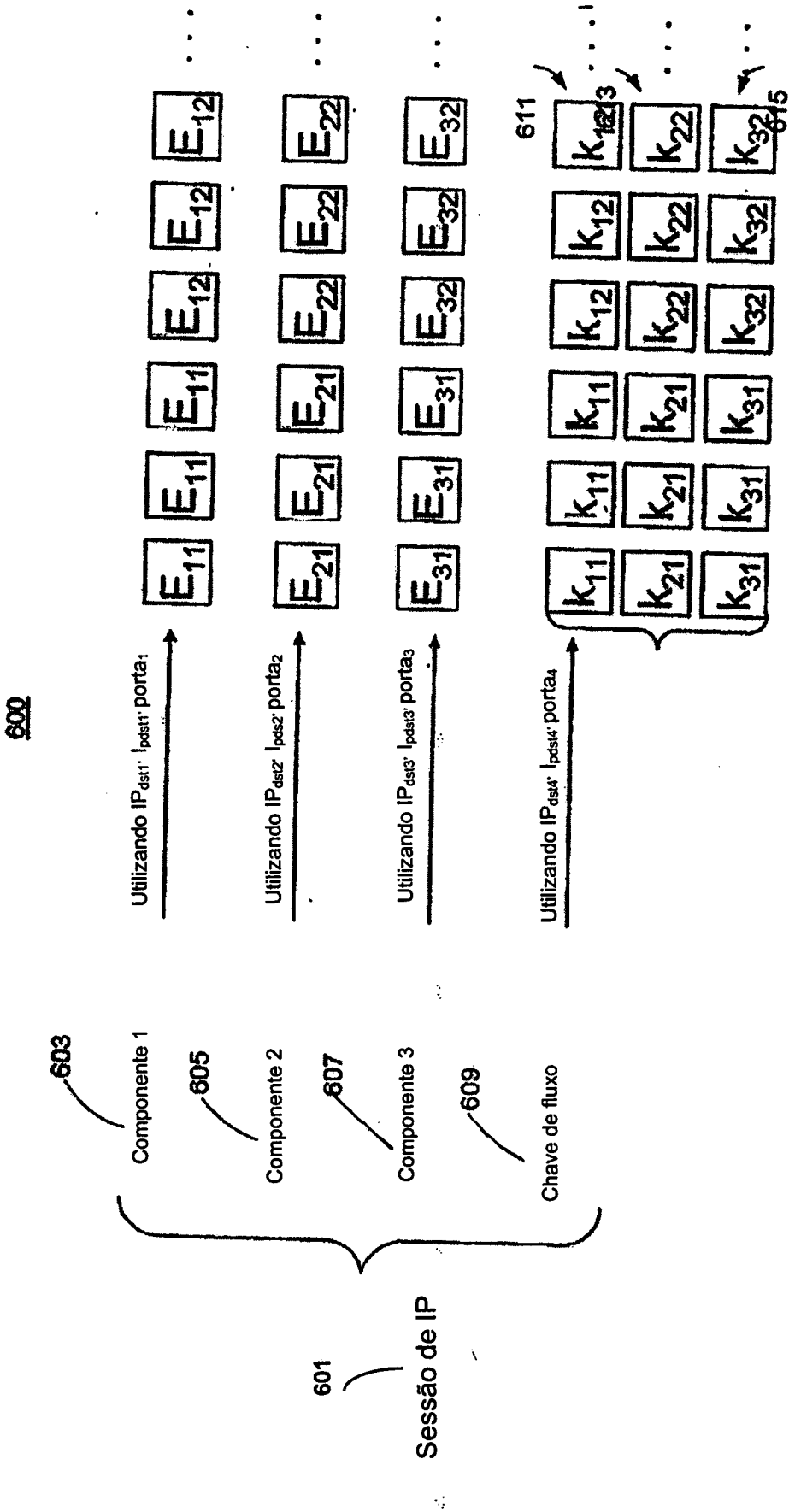

600
Sessão de IP
601
Componente 1
603
Componente 2
605
Componente 3
607
Chave de fluxo
609
611
Utilizando IPdst1, Ipds1, porta1
Utilizando IPdst2, Ipds2, porta2
Utilizando IPdst3, Ipds3, porta3
Utilizando IPdst4, Ipds4, porta4
E11
E12
E21
E22
E31
E32
K11
K12
K21
K22
K31
K32

FIG. 6

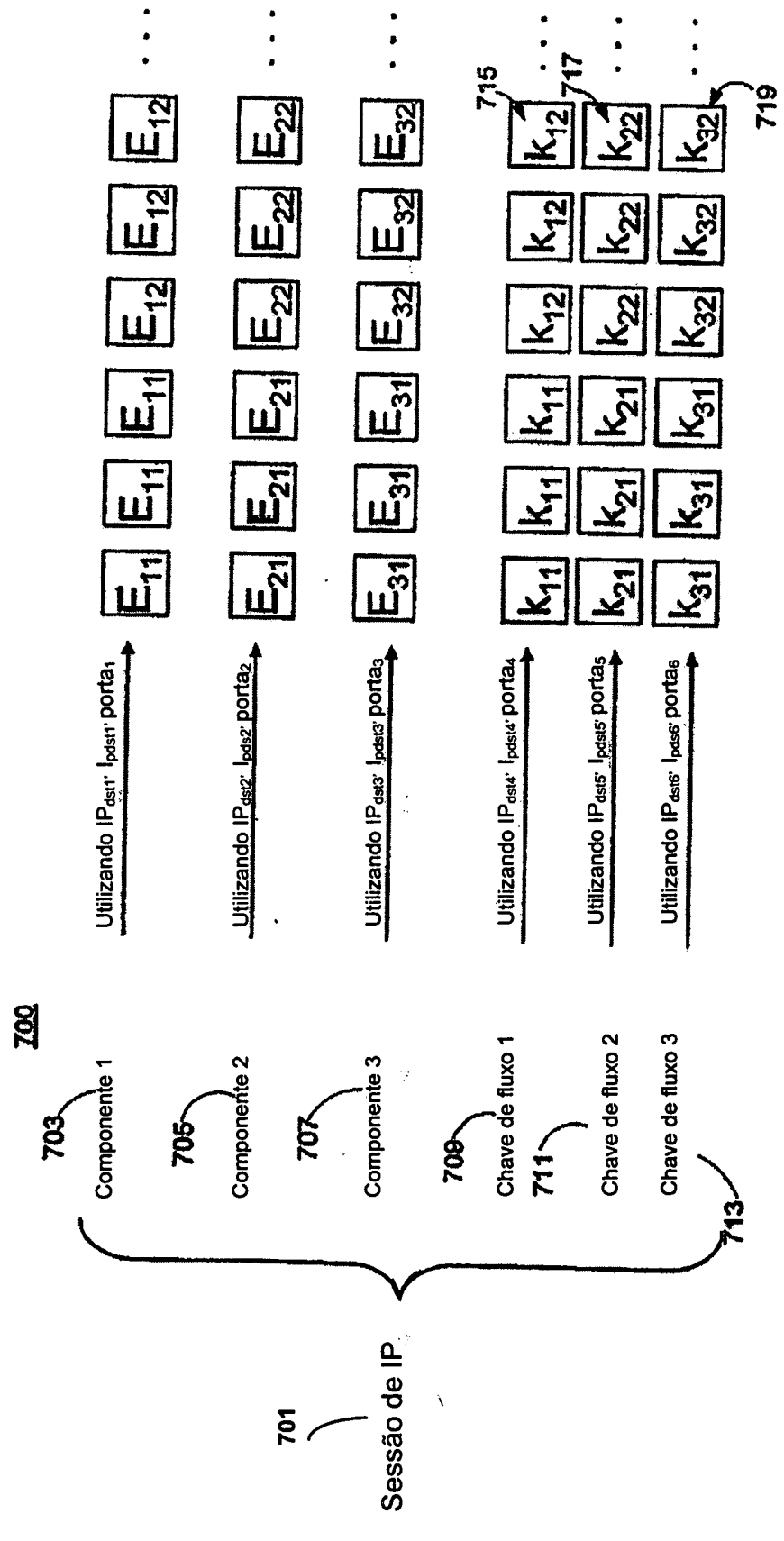

700
703
Componente 1
705
Componente 2
707
Componente 3
709
Chave de fluxo 1
711
Chave de fluxo 2
Chave de fluxo 3
713
Sessão de IP
701
Utilizando IPdst1, Ipds1, porta1
Utilizando IPdst2, Ipds2, porta2
Utilizando IPdst3, Ipdst3, porta3
Utilizando IPdst4, Ipdst4, porta4
Utilizando IPdst5, Ipdst5, porta5
Utilizando IPdst6, Ipds6, porta6
E11
E21
E31
E12
E22
E32
K11
K21
K31
K12
K22
K32
715
717
719

FIG. 7

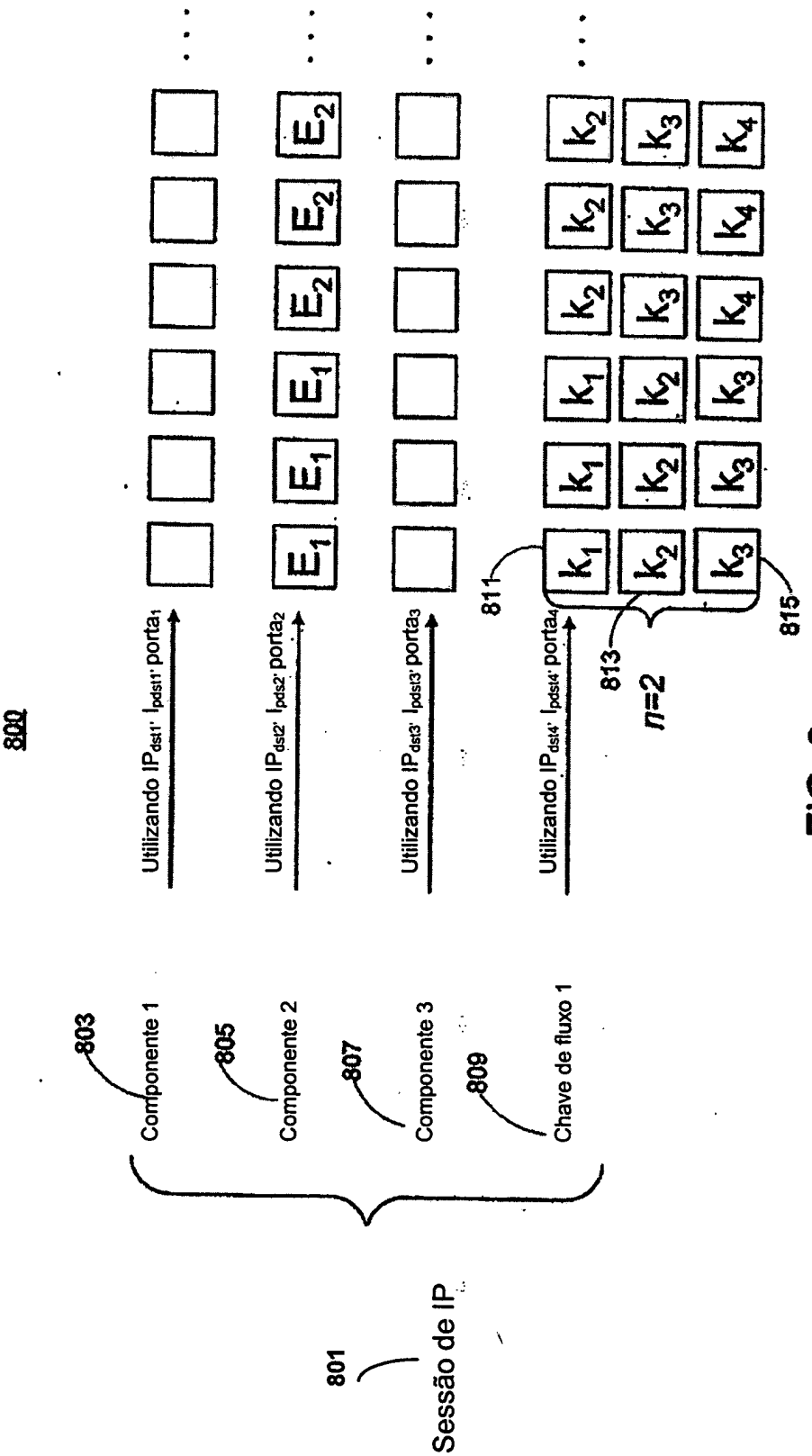

800
Componente 1
Componente 2
Componente 3
Chave de fluxo 1
803
805
807
809
801
Sessão de IP
Utilizando IPdst1, Ipdst1, porta1
Utilizando IPdst2, Ipdst2, porta2
Utilizando IPdst3, Ipdst3, porta3
Utilizando IPdst4, Ipdst4, porta4
E1
E2
K1
K2
K3
K4
811
813
815
n=2

FIG. 8

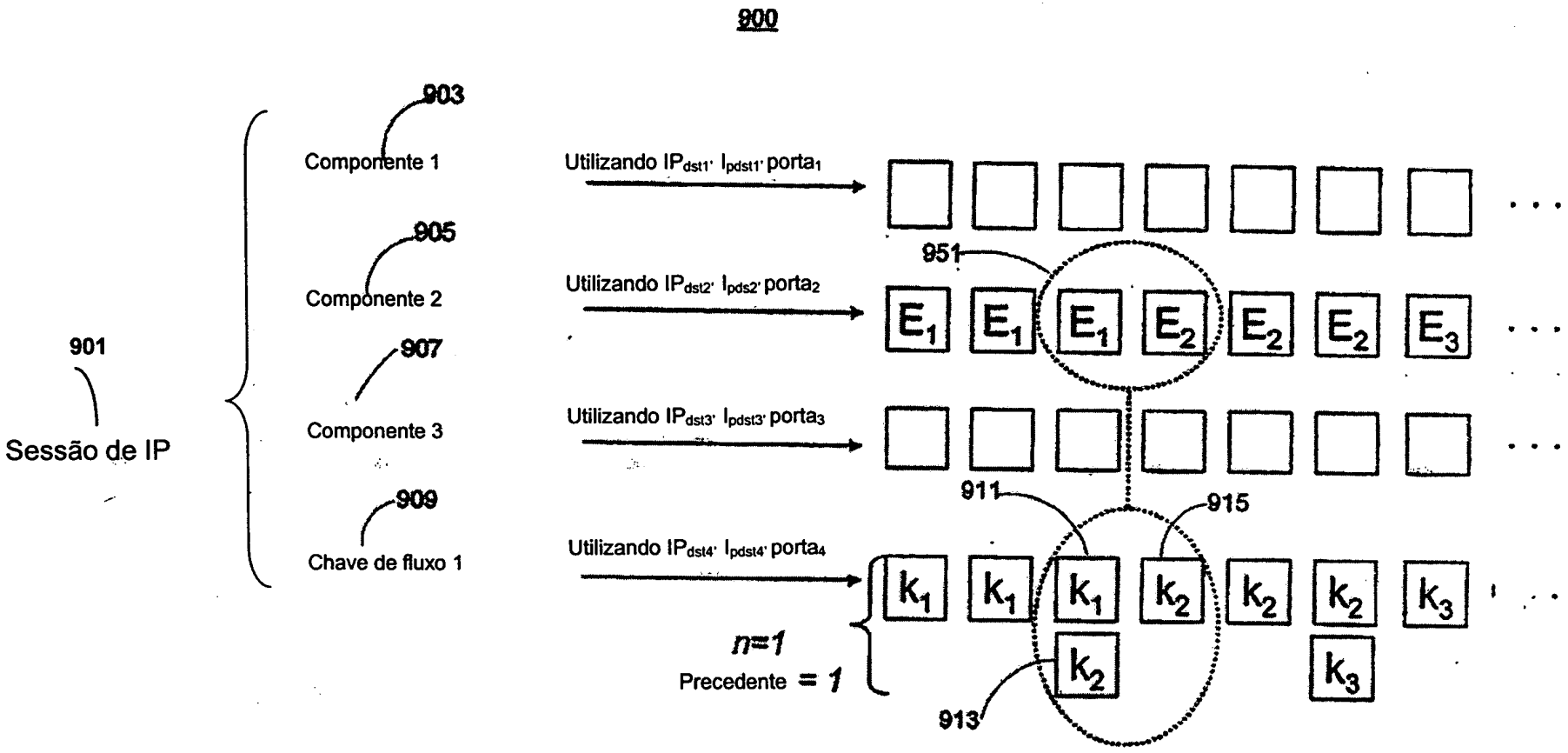

900
901
Sessão de IP
903
Componente 1
905
Componente 2
907
Componente 3
909
Chave de fluxo 1
Utilizando IP$_{dst1}$, I$_{pdst1}$, porta$_1$
Utilizando IP$_{dst2}$, I$_{pds2}$, porta$_2$
Utilizando IP$_{dst3}$, I$_{pdst3}$, porta$_3$
Utilizando IP$_{dst4}$, I$_{pdst4}$, porta$_4$
951
911
915
913
n=1
Precedente = 1

FIG. 9

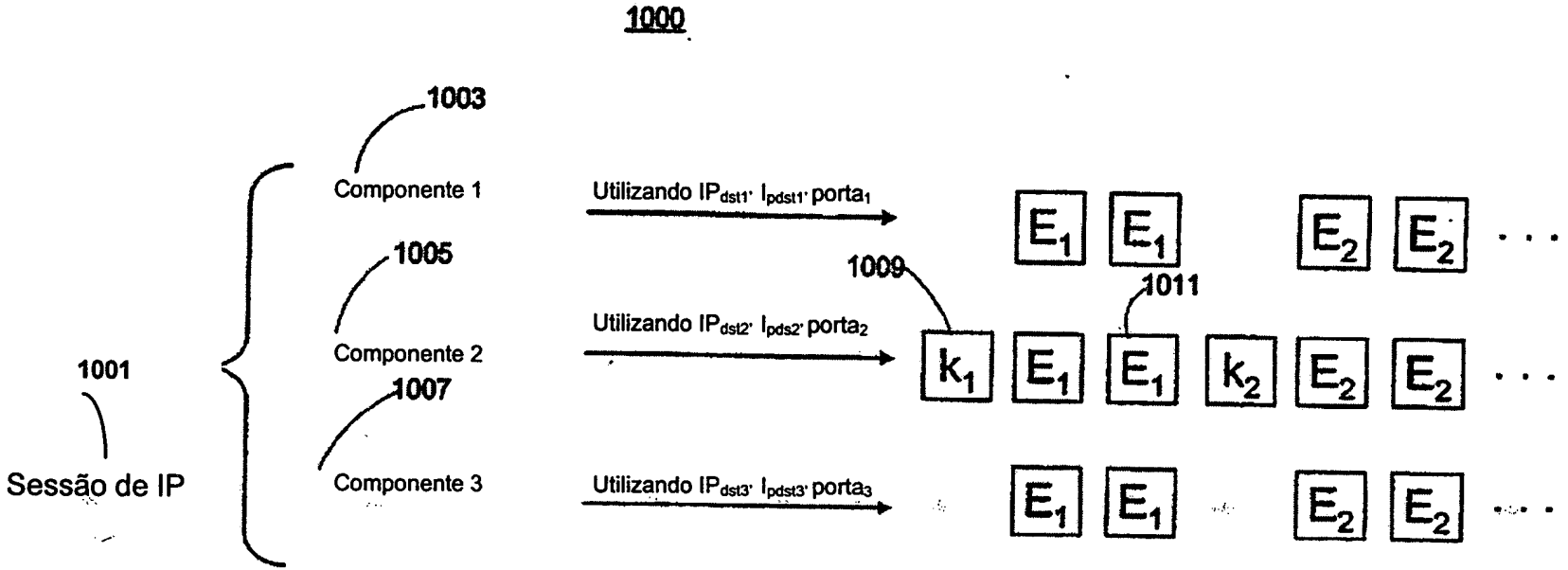

1000
1003
Componente 1
1005
Componente 2
1007
Componente 3
1001
Sessão de IP
Utilizando IP_{dst1}, I_{pdst1}, $porta_1$
Utilizando IP_{dst2}, I_{pds2}, $porta_2$
Utilizando IP_{dst3}, I_{pdst3}, $porta_3$
1009
1011
k_1
k_2
E_1
E_2

FIG. 10

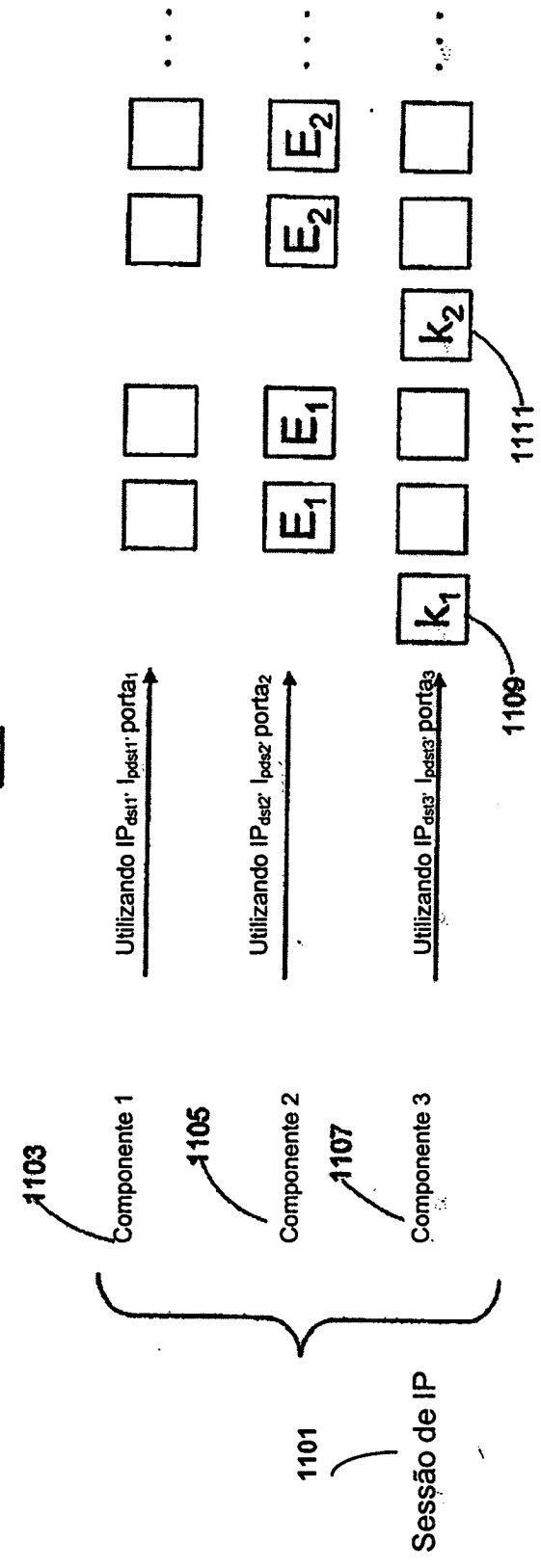

1100
Utilizando IP_{dst1}, l_{pdst1}, $porta_1$
Utilizando IP_{dst2}, l_{pdst2}, $porta_2$
Utilizando IP_{dst3}, l_{pdst3}, $porta_3$
E_1
E_2
k_1
k_2
1109
1111
1103
Componente 1
1105
Componente 2
1107
Componente 3
1101
Sessão de IP

FIG. 11

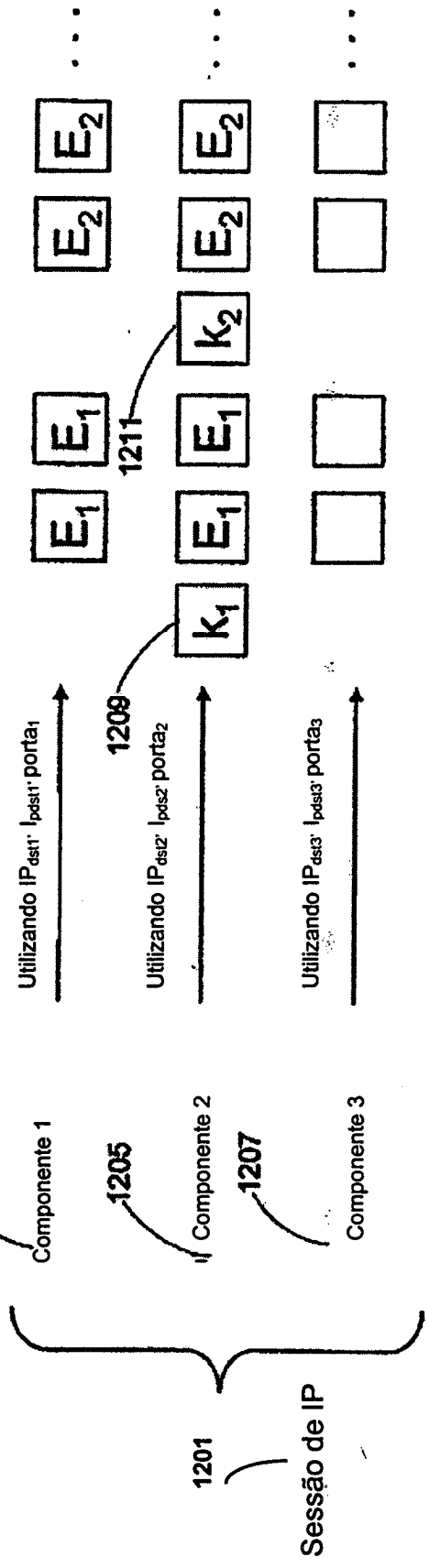

1200
1201
Sessão de IP
1203
Componente 1
1205
Componente 2
1207
Componente 3
Utilizando IPdst1, Idst1, porta1
Utilizando IPdst2, Idst2, porta2
Utilizando IPdst3, Idst3, porta3
1209
1211
E1
E2
K1
K2

FIG. 12

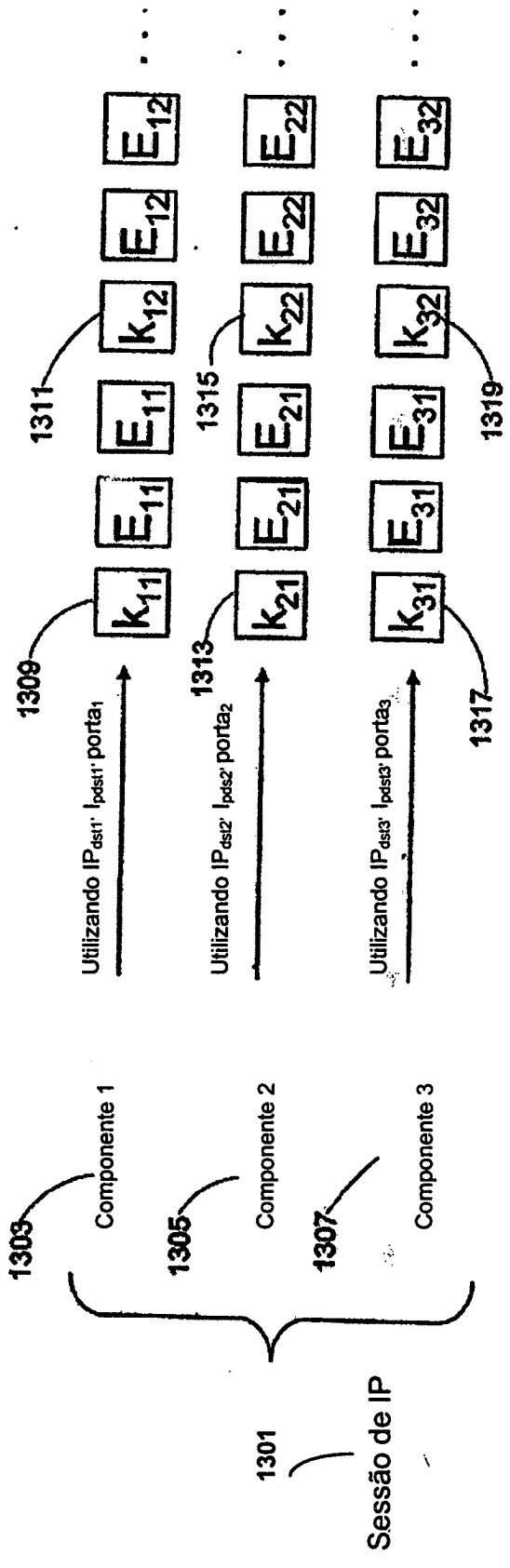

1300
1309
1313
1317
1311
1315
1319
Utilizando IP_{dst1}, I_{pdst1}, $porta_1$
Utilizando IP_{dst2}, I_{pdst2}, $porta_2$
Utilizando IP_{dst3}, I_{pdst3}, $porta_3$
k_{11} E_{11} E_{11} k_{12} E_{12} E_{12} ...
k_{21} E_{21} E_{21} k_{22} E_{22} E_{22} ...
k_{31} E_{31} E_{31} k_{32} E_{32} E_{32} ...
1303
Componente 1
1305
Componente 2
1307
Componente 3
1301
Sessão de IP

FIG. 13

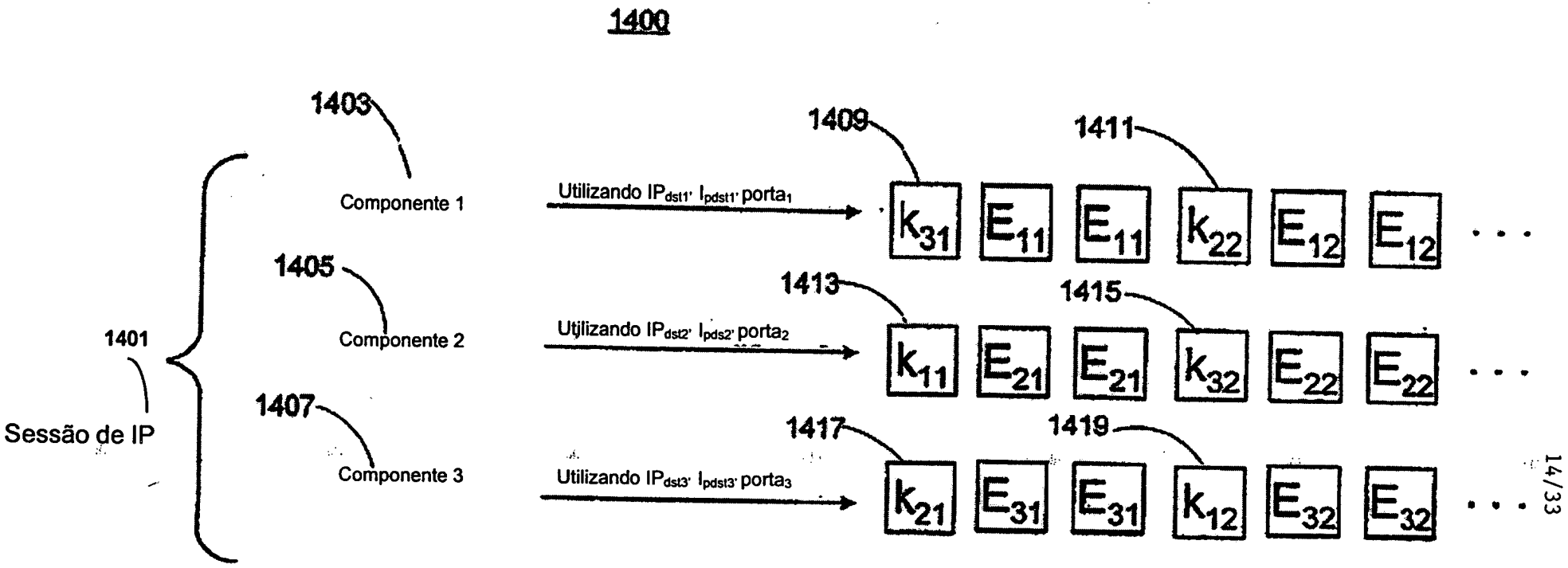

1400
1403
Componente 1
1405
Componente 2
1407
Componente 3
1401
Sessão de IP
1409
1411
1413
1415
1417
1419
Utilizando IPdst1, Ipdst1, porta1
Utilizando IPdst2, Ipdst2, porta2
Utilizando IPdst3, Ipdst3, porta3
k31 E11 E11 k22 E12 E12
k11 E21 E21 k32 E22 E22
k21 E31 E31 k12 E32 E32

FIG. 14

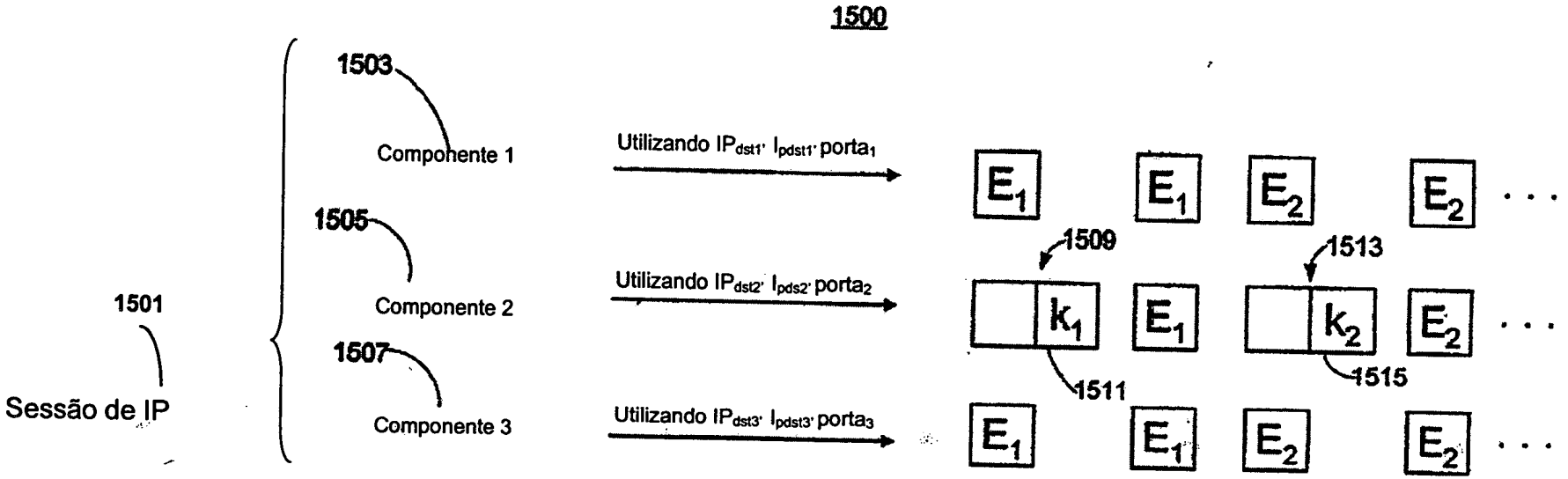

1500
1501
Sessão de IP
1503
Componente 1
1505
Componente 2
1507
Componente 3
Utilizando IPdst1, Ipdst1, porta1
Utilizando IPdst2, Ipdds2, porta2
Utilizando IPdst3, Ipdst3, porta3
E1
E1
E2
E2
1509
1513
k1
E1
k2
E2
1511
1515
E1
E1
E2
E2

FIG. 15

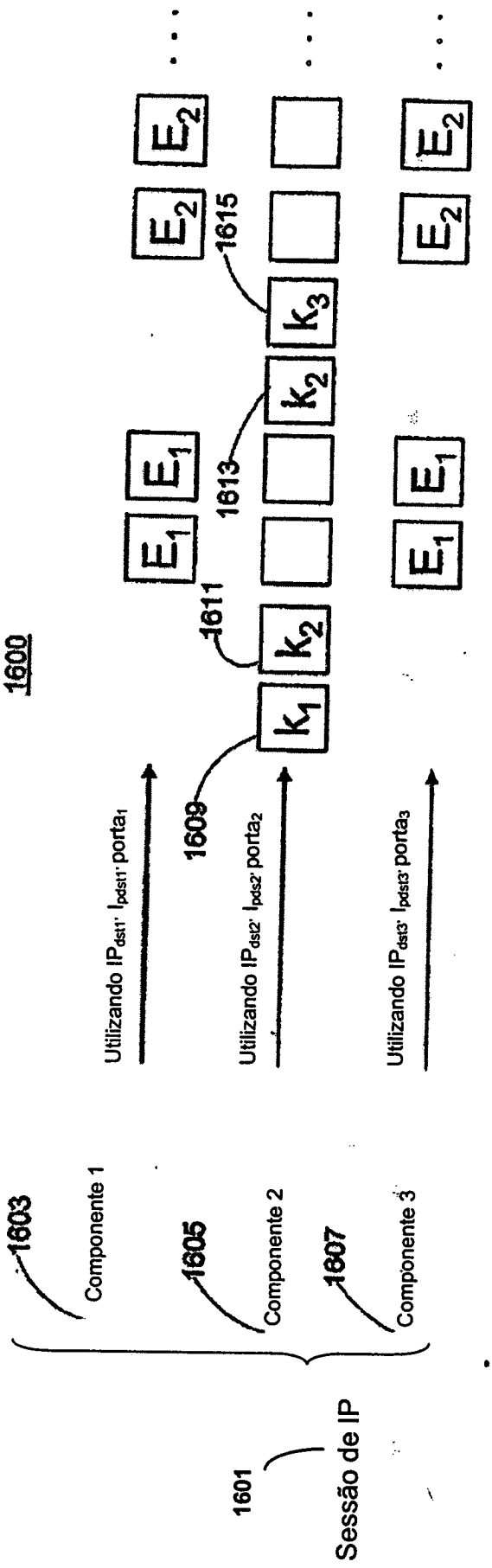

1600
1601
Sessão de IP
1603
Componente 1
1605
Componente 2
1607
Componente 3
Utilizando IP$_{dst1}$, I$_{pdst1}$, porta$_1$
Utilizando IP$_{dst2}$, I$_{pdst2}$, porta$_2$
Utilizando IP$_{dst3}$, I$_{pdst3}$, porta$_3$
1609
1611
1613
1615
E$_1$
E$_2$
k$_1$
k$_2$
k$_3$

FIG. 16

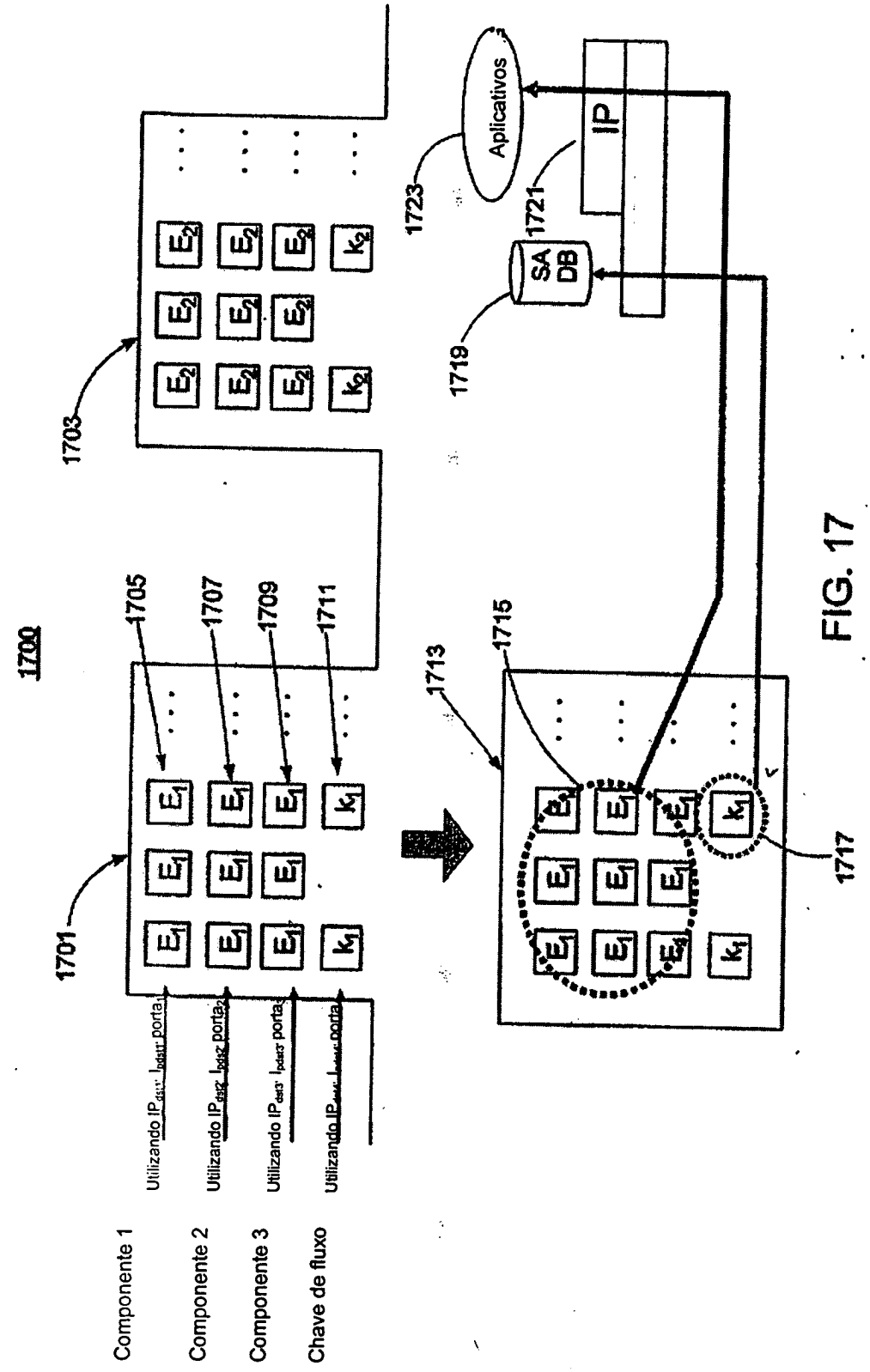

1700
1701
1703
1705
1707
1709
1711
1713
1715
1717
1719
1721
1723
SA DB
IP
Aplicativos
Componente 1
Componente 2
Componente 3
Chave de fluxo
Utilizando IP
porta

FIG. 17

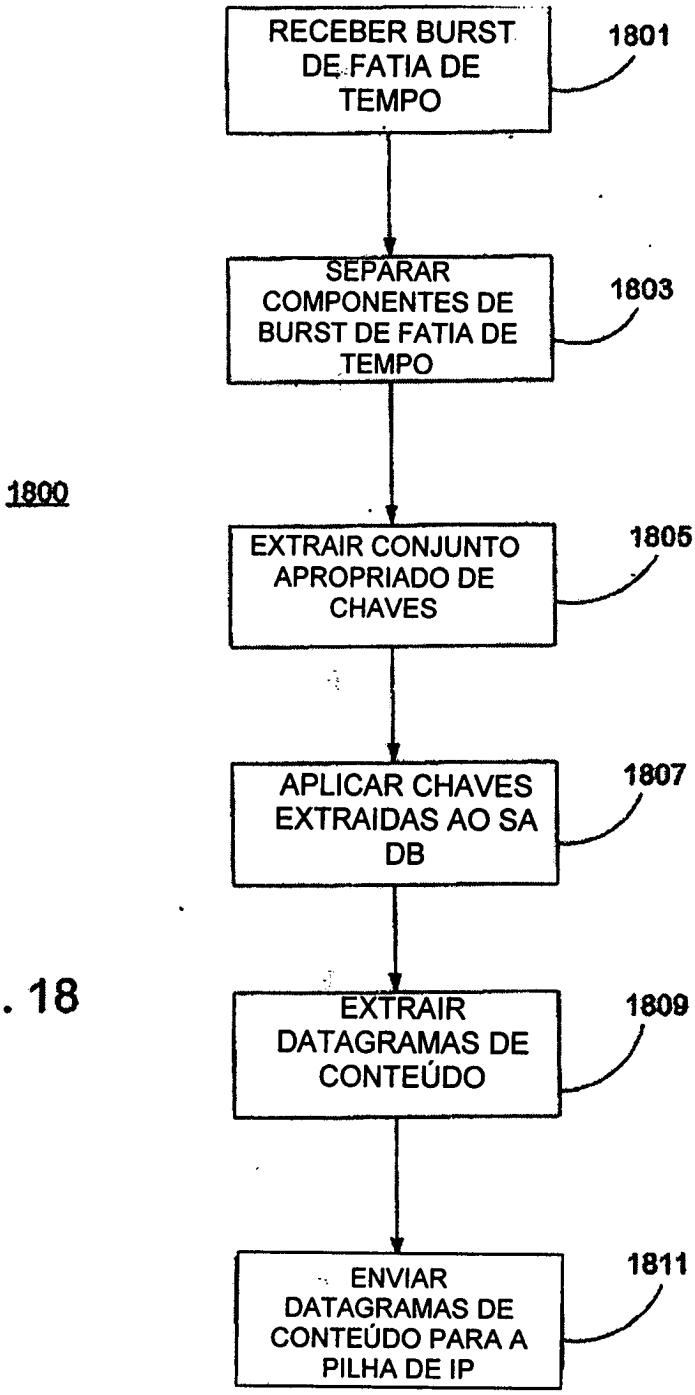

1800
RECEBER BURST DE FATIA DE TEMPO
1801
SEPARAR COMPONENTES DE BURST DE FATIA DE TEMPO
1803
EXTRAIR CONJUNTO APROPRIADO DE CHAVES
1805
APLICAR CHAVES EXTRAIDAS AO SA DB
1807
EXTRAIR DATAGRAMAS DE CONTEÚDO
1809
ENVIAR DATAGRAMAS DE CONTEÚDO PARA A PILHA DE IP
1811

FIG. 18

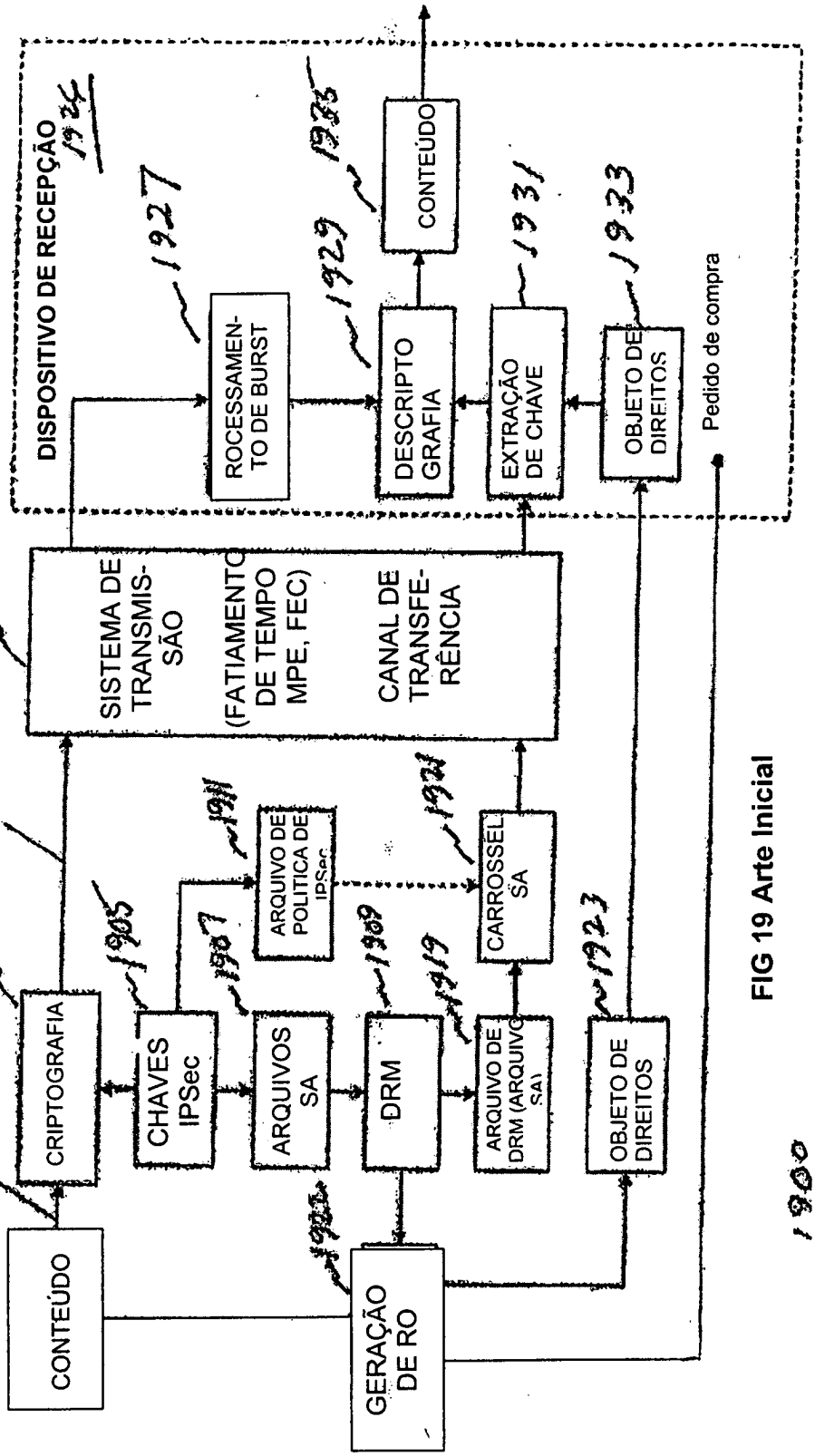


FIG 19 Arte Inicial

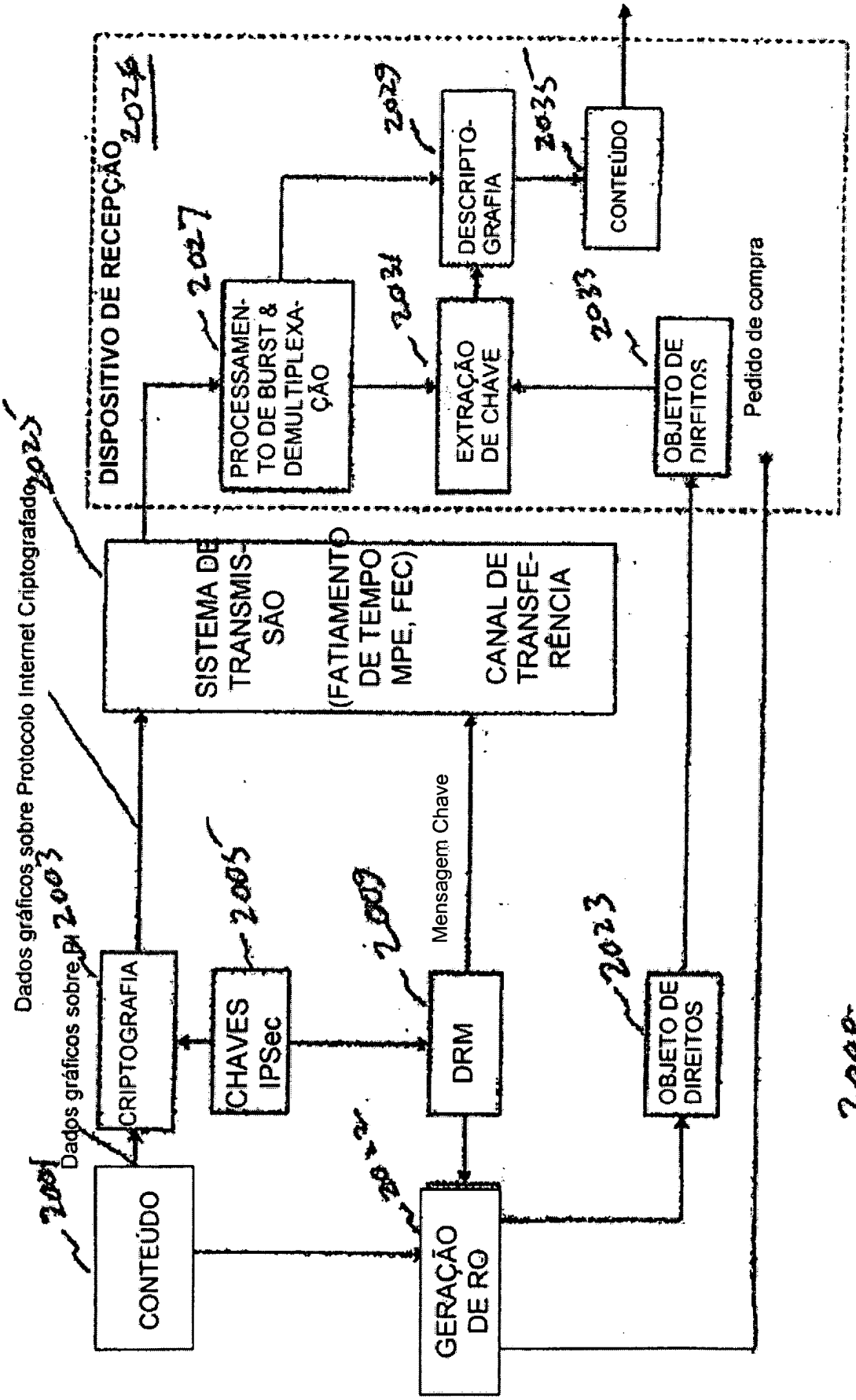

2000
2001
CONTEÚDO
Dados gráficos sobre
2003
CRIPTOGRAFIA
Dados gráficos sobre Protocolo Internet Criptografado
2002
2005
CHAVES IPSec
2009
DRM
Mensagem Chave
2023
OBJETO DE DIREITOS
GERAÇÃO DE RO
SISTEMA DE TRANSMISSÃO
(FATIAMENTO DE TEMPO MPE, FEC)
CANAL DE TRANSFERÊNCIA
DISPOSITIVO DE RECEPÇÃO
2026
2027
PROCESSAMENTO DE BURST & DEMULTIPLEXAÇÃO
2029
DESCRIPTOGRAFIA
2031
EXTRAÇÃO DE CHAVE
2033
OBJETO DE DIREITOS
2035
CONTEÚDO
Pedido de compra

FIG. 20

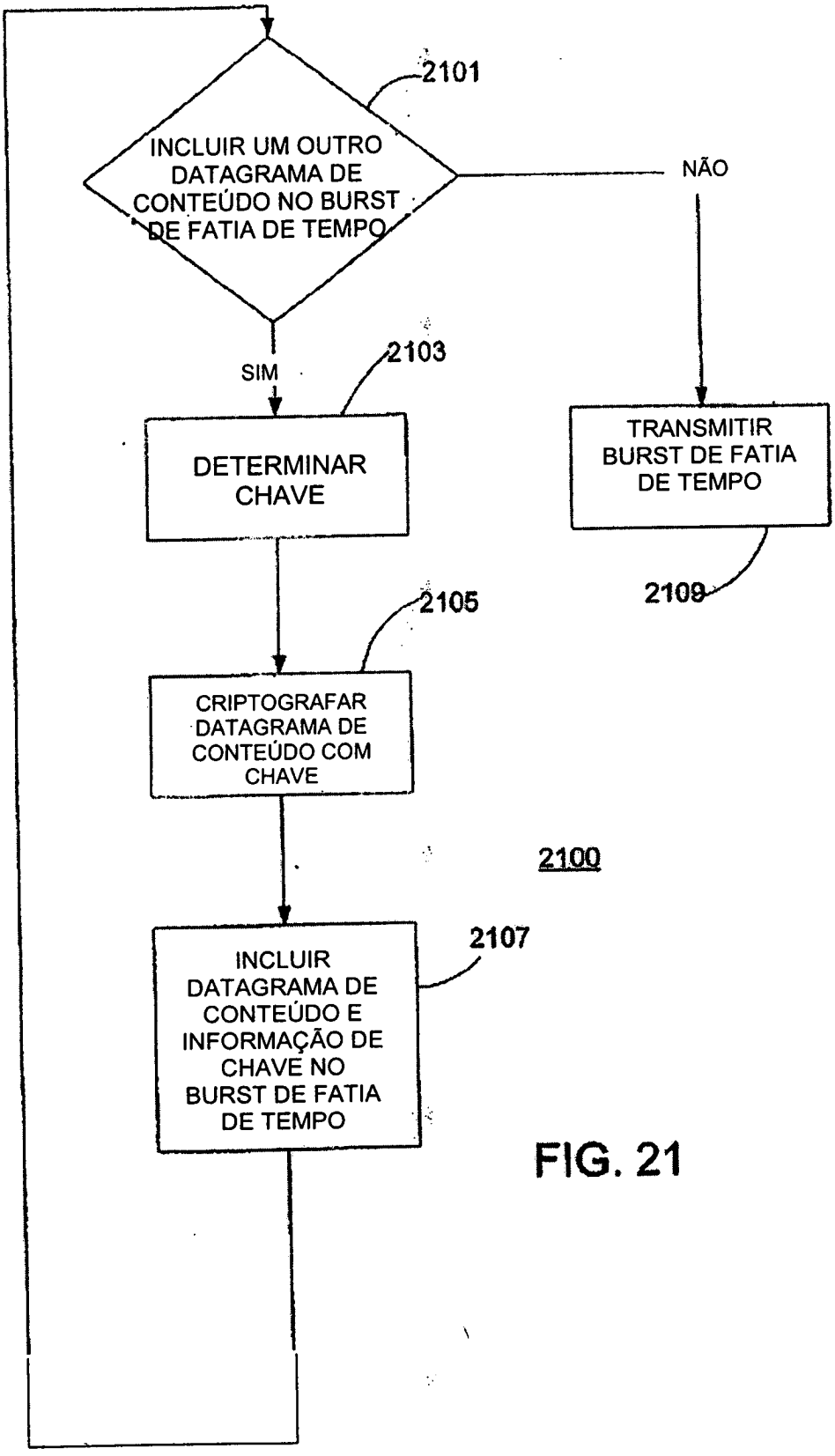

2101
INCLUIR UM OUTRO DATAGRAMA DE CONTEÚDO NO BURST DE FATIA DE TEMPO
NÃO
SIM
2103
DETERMINAR CHAVE
TRANSMITIR BURST DE FATIA DE TEMPO
2109
2105
CRIPTOGRAFAR DATAGRAMA DE CONTEÚDO COM CHAVE
2100
2107
INCLUIR DATAGRAMA DE CONTEÚDO E INFORMAÇÃO DE CHAVE NO BURST DE FATIA DE TEMPO

FIG. 21

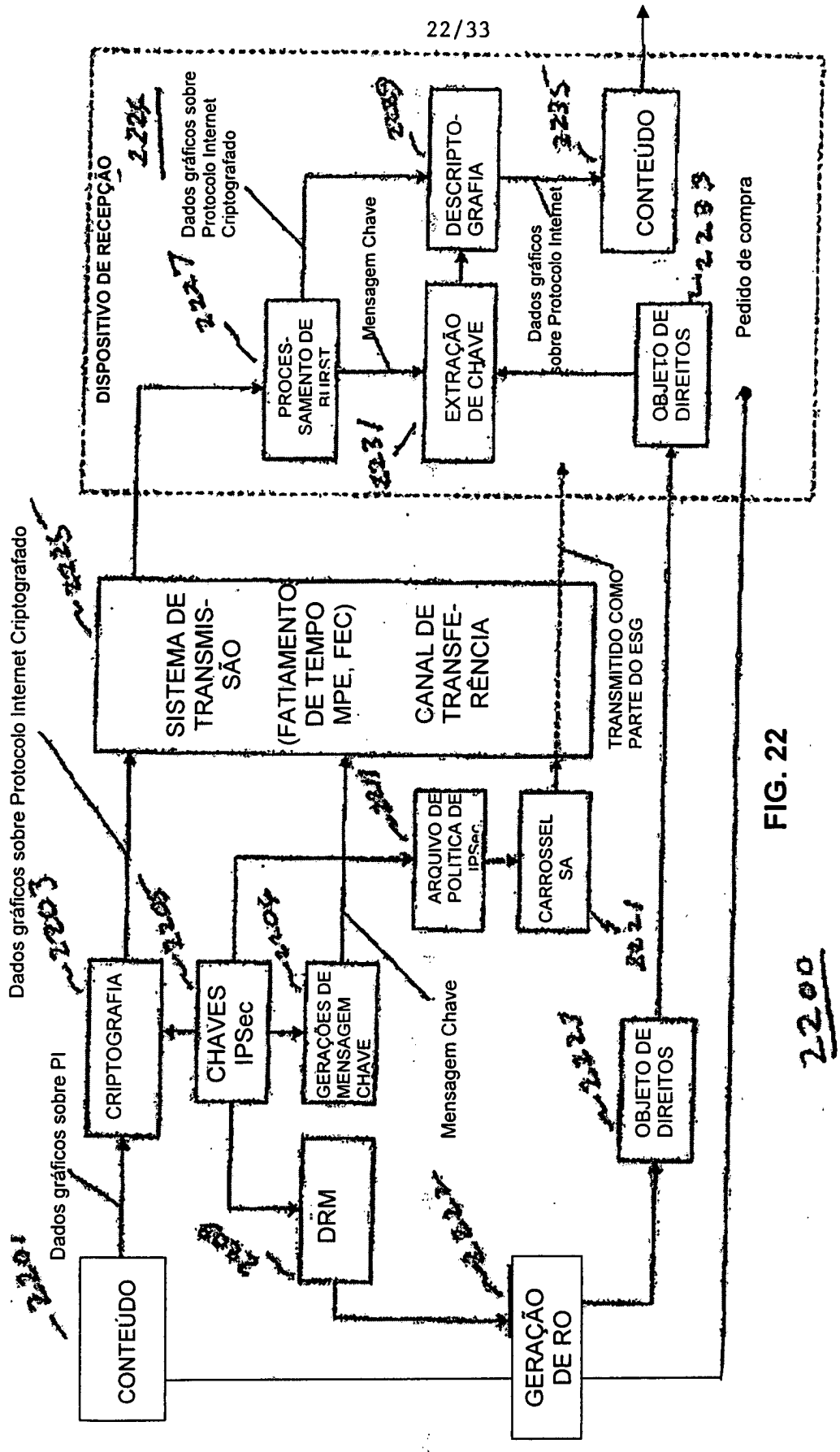

2200
2201
CONTEÚDO
Dados gráficos sobre PI
2203
CRIPTOGRAFIA
Dados gráficos sobre Protocolo Internet Criptografado
2205
CHAVES IPSec
2207
GERAÇÕES DE MENSAGEM CHAVE
Mensagem Chave
2209
DRM
2211
ARQUIVO DE POLITICA DE IPSec
2213
CARROSSEL SA
2215
SISTEMA DE TRANSMISSÃO
(FATIAMENTO DE TEMPO MPE, FEC)
CANAL DE TRANSFERÊNCIA
TRANSMITIDO COMO PARTE DO ESG
2217
OBJETO DE DIREITOS
2219
GERAÇÃO DE RO
2221
OBJETO DE DIREITOS
2223
DISPOSITIVO DE RECEPÇÃO
2225
PROCESSAMENTO DE BURST
Dados gráficos sobre Protocolo Internet Criptografado
2227
EXTRAÇÃO DE CHAVE
2229
Mensagem Chave
DESCRIPTOGRAFIA
2231
Dados gráficos sobre Protocolo Internet
2233
CONTEÚDO
2235
OBJETO DE DIREITOS
2237
Pedido de compra

FIG. 22

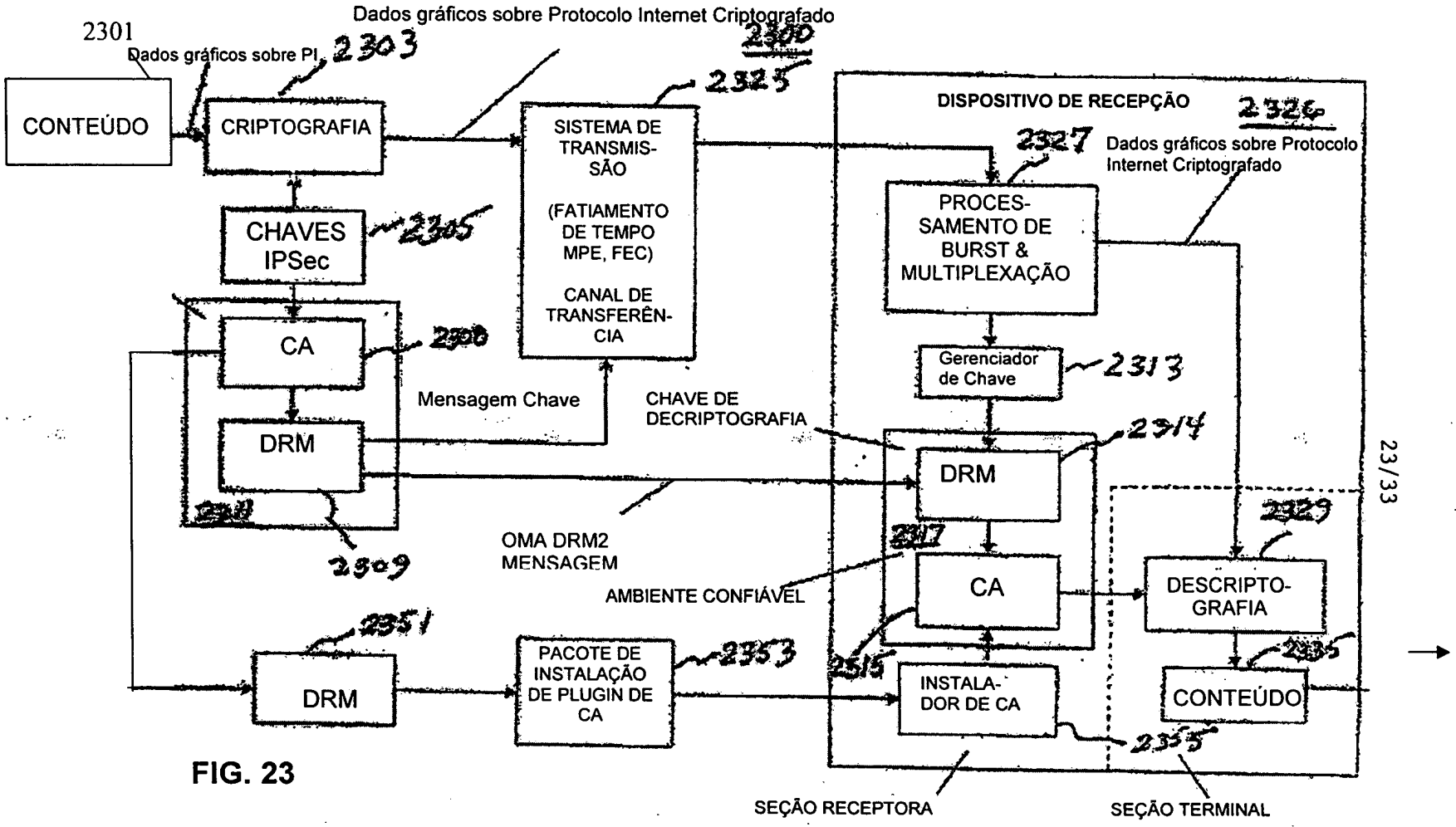

2301
Dados gráficos sobre Protocolo Internet Criptografado
Dados gráficos sobre PI
2303
2300
2325
CONTEÚDO
CRIPTOGRAFIA
SISTEMA DE TRANSMIS-SÃO
(FATIAMENTO DE TEMPO MPE, FEC)
CANAL DE TRANSFERÊN-CIA
DISPOSITIVO DE RECEPÇÃO
2326
2327
Dados gráficos sobre Protocolo Internet Criptografado
PROCES-SAMENTO DE BURST & MULTIPLEXAÇÃO
CHAVES IPSec
2305
CA
2306
Gerenciador de Chave
2313
Mensagem Chave
CHAVE DE DECRIPTOGRAFIA
DRM
2314
DRM
2309
OMA DRM2 MENSAGEM
2329
2317
AMBIENTE CONFIÁVEL
CA
DESCRIPTO-GRAFIA
2351
2353
2315
2335
DRM
PACOTE DE INSTALAÇÃO DE PLUGIN DE CA
INSTALA-DOR DE CA
CONTEÚDO
2355
SEÇÃO RECEPTORA
SEÇÃO TERMINAL

FIG. 23

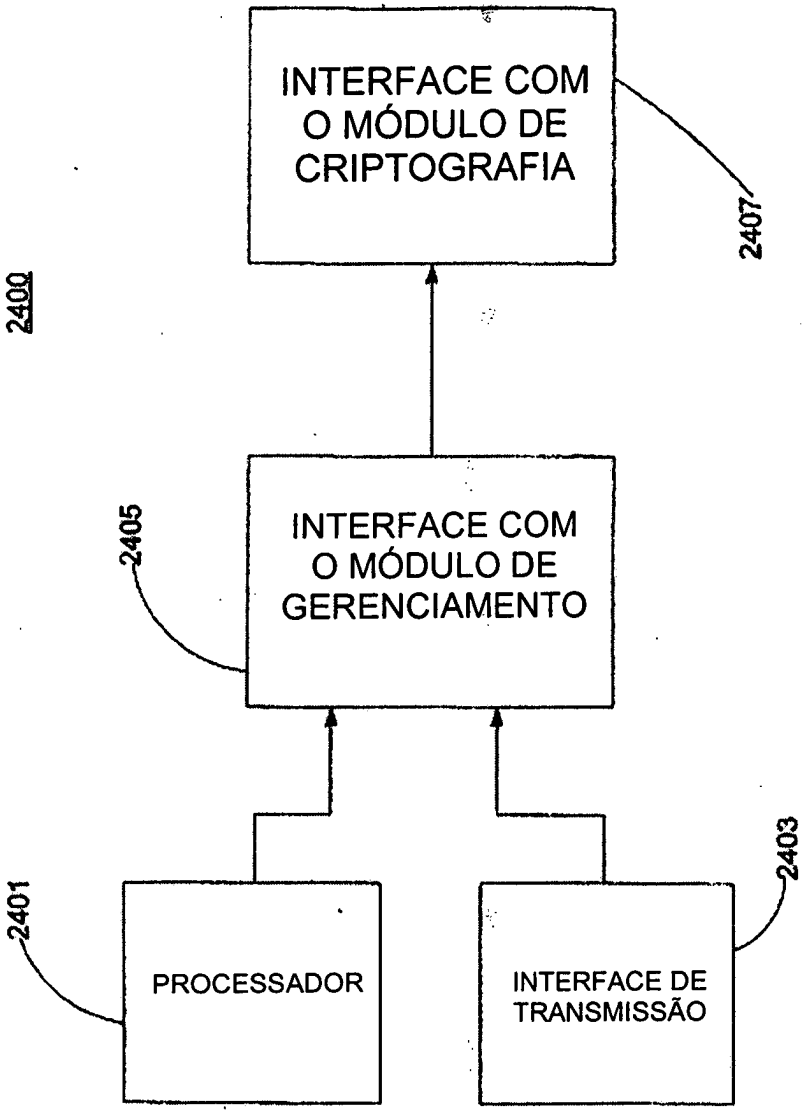

2400
INTERFACE COM O MÓDULO DE CRIPTOGRAFIA
2407
INTERFACE COM O MÓDULO DE GERENCIAMENTO
2405
PROCESSADOR
2401
INTERFACE DE TRANSMISSÃO
2403

FIG. 24

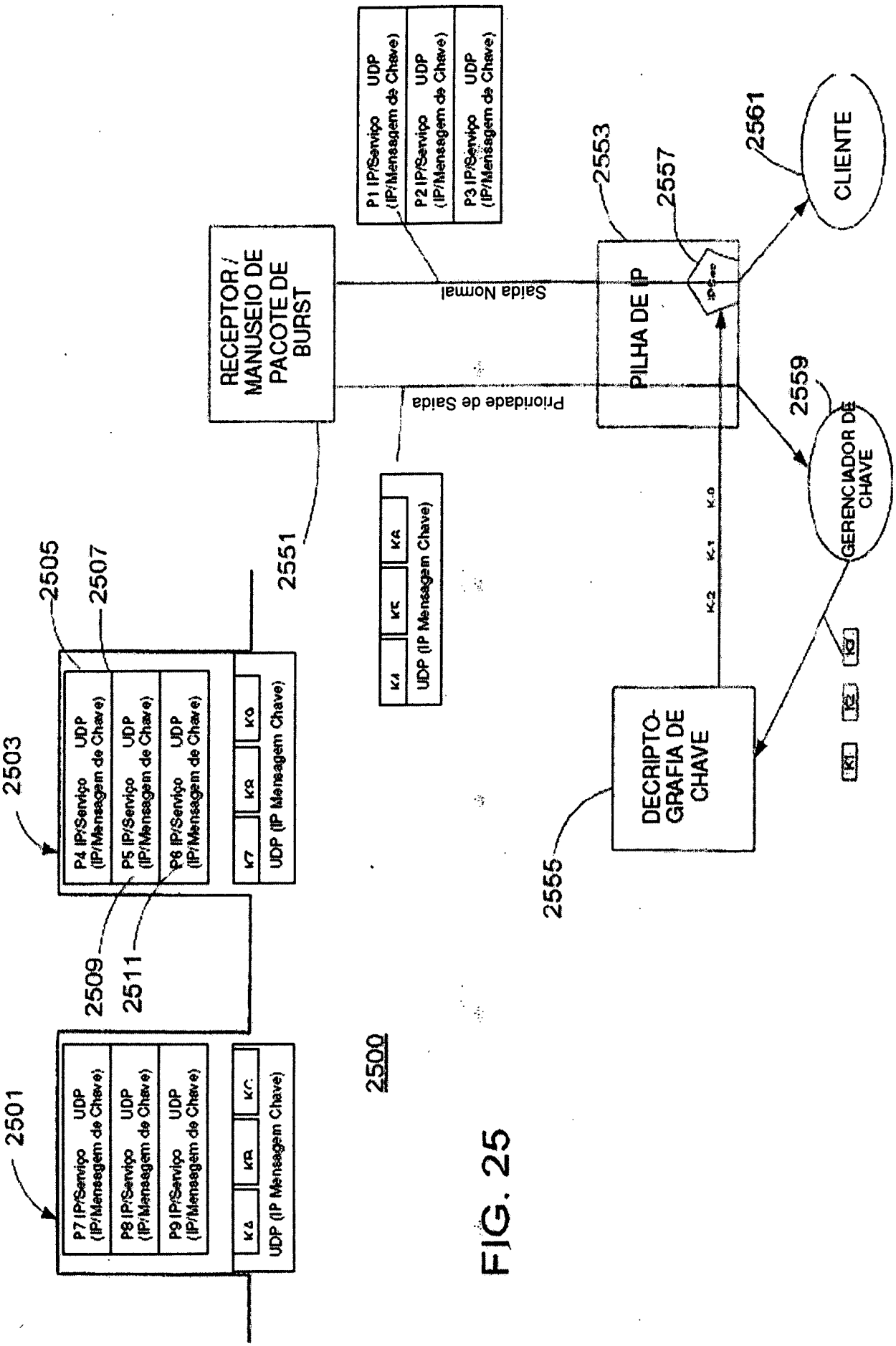

2500
2501
2503
2505
2507
2509
2511
2551
2553
2555
2557
2559
2561
P7 IP/Serviço UDP (IP/Mensagem de Chave)
P8 IP/Serviço UDP (IP/Mensagem de Chave)
P9 IP/Serviço UDP (IP/Mensagem de Chave)
UDP (IP Mensagem Chave)
P4 IP/Serviço UDP (IP/Mensagem de Chave)
P5 IP/Serviço UDP (IP/Mensagem de Chave)
P6 IP/Serviço UDP (IP/Mensagem de Chave)
UDP (IP Mensagem Chave)
P1 IP/Serviço UDP (IP/Mensagem de Chave)
P2 IP/Serviço UDP (IP/Mensagem de Chave)
P3 IP/Serviço UDP (IP/Mensagem de Chave)
UDP (IP Mensagem Chave)
RECEPTOR / MANUSEIO DE PACOTE DE BURST
Saída Normal
Prioridade de Saída
PILHA DE IP
CLIENTE
GERENCIADOR DE CHAVE
DECRIPTO-GRAFIA DE CHAVE
K-0
K-1
K-2

FIG. 25

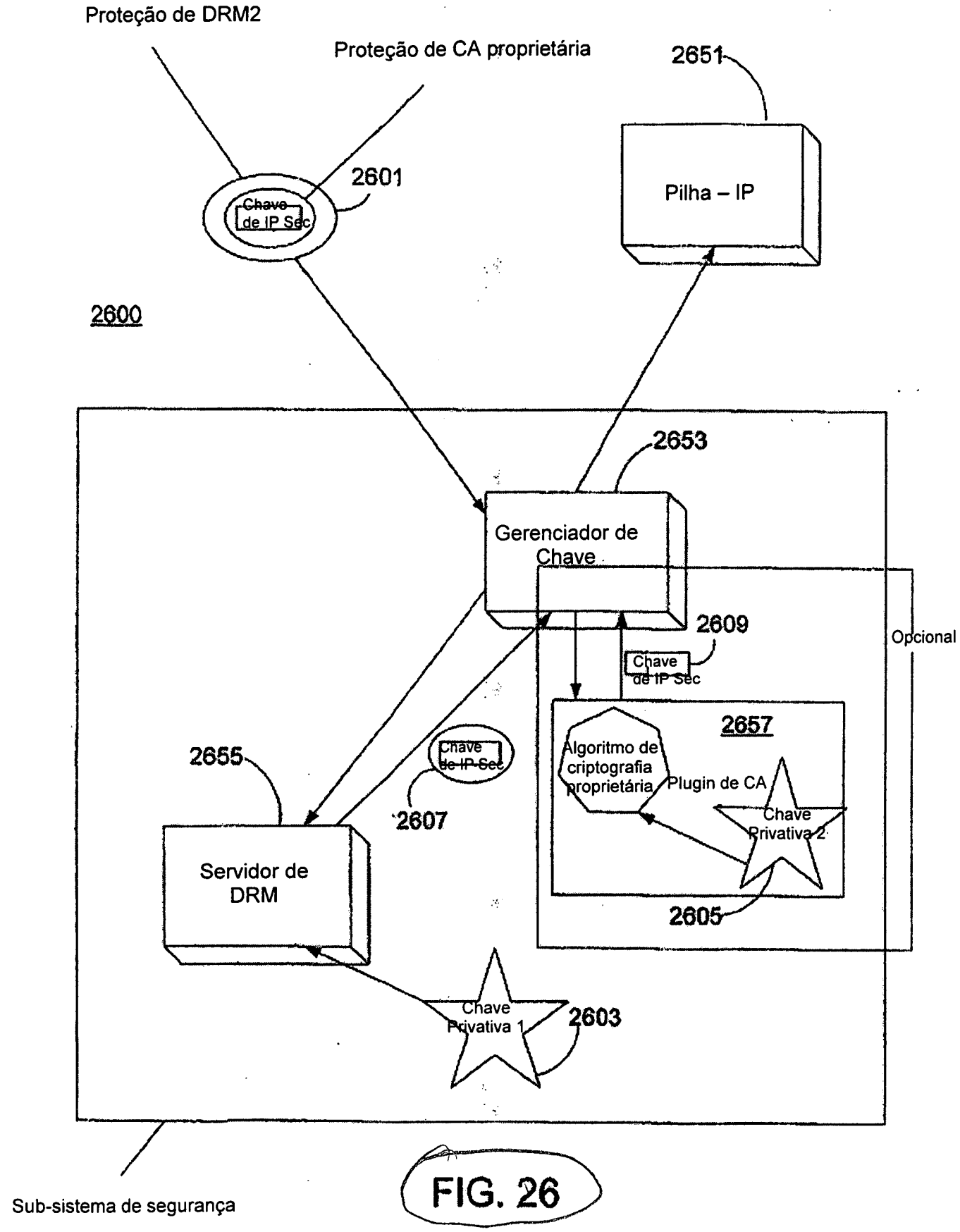

Proteção de DRM2
Proteção de CA proprietária
2651
2601
Chave de IP Sec
Pilha – IP
2600
2653
Gerenciador de Chave
2609
Opcional
Chave de IP Sec
2657
Algoritmo de criptografia proprietária
Plugin de CA
Chave Privativa 2
2655
Chave de IP Sec
2607
Servidor de DRM
2605
Chave Privativa 1
2603
Sub-sistema de segurança

FIG. 26

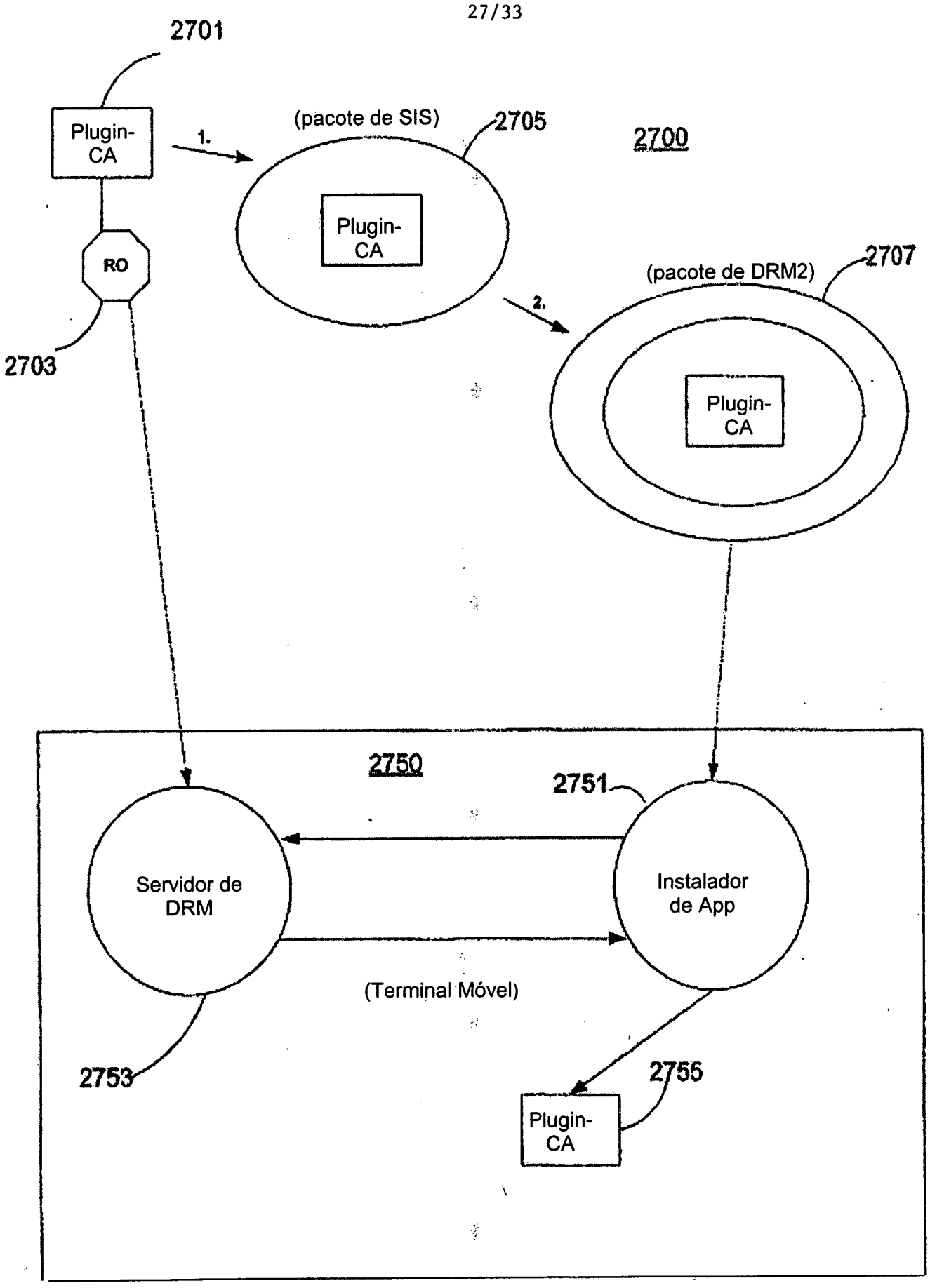

2701
Plugin-CA
1.
(pacote de SIS)
2705
2700
Plugin-CA
RO
2703
2707
(pacote de DRM2)
2.
Plugin-CA
2750
2751
Servidor de DRM
Instalador de App
(Terminal Móvel)
2753
2755
Plugin-CA

FIG. 27

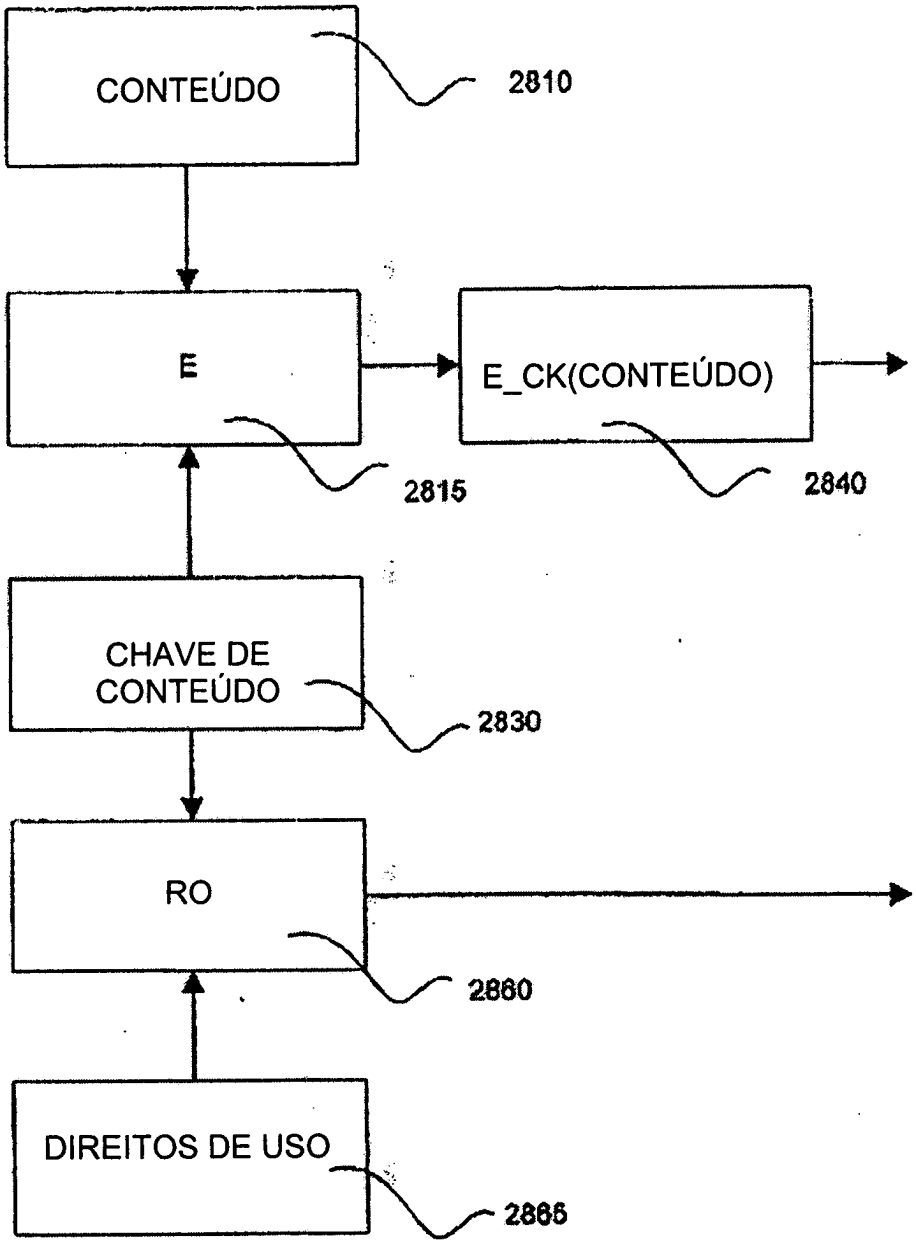

CONTEÚDO
2810
E
E_CK(CONTEÚDO)
2815
2840
CHAVE DE CONTEÚDO
2830
RO
2860
DIREITOS DE USO
2865

FIG. 28

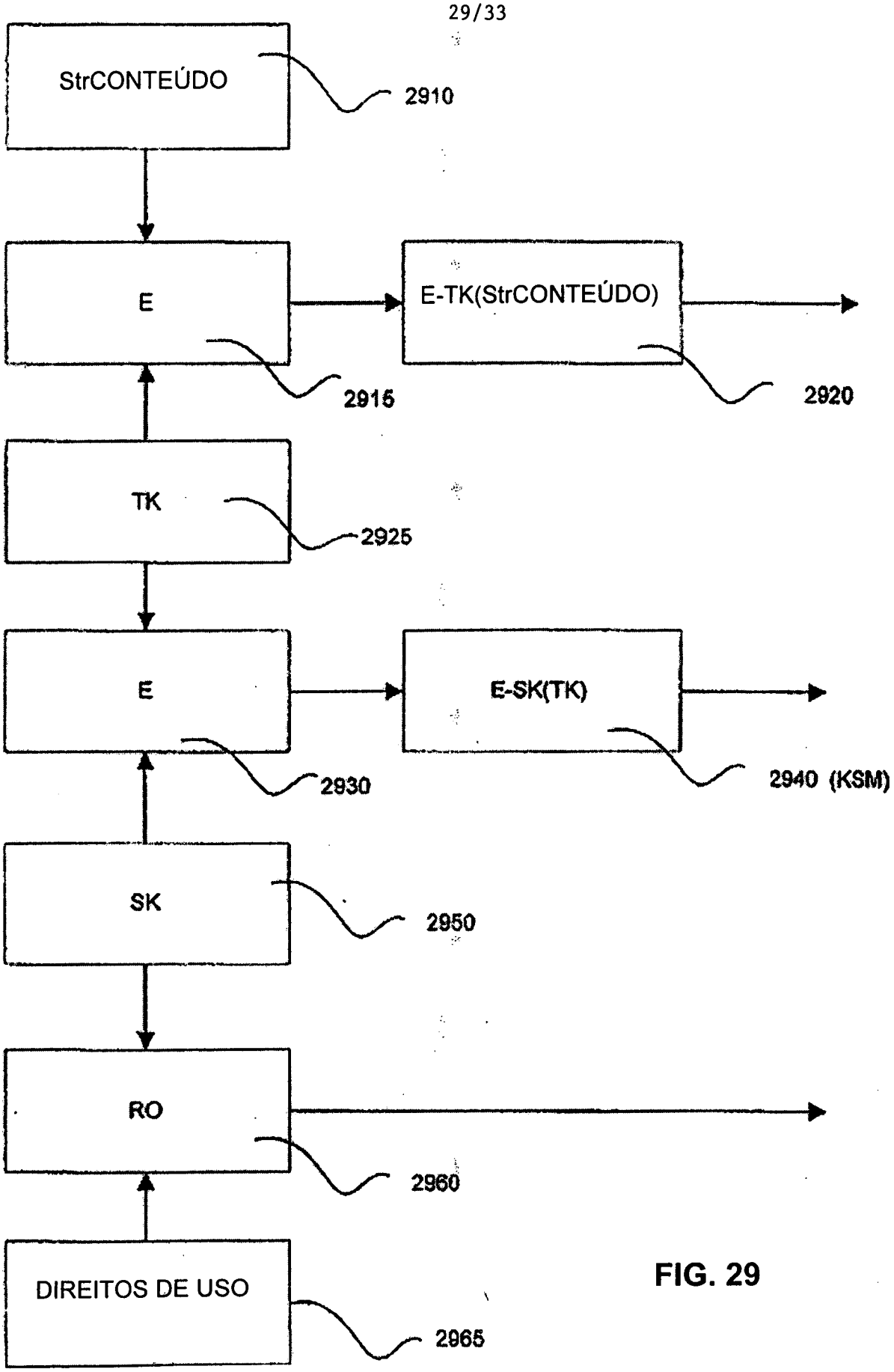

StrCONTEÚDO
2910
E
E-TK(StrCONTEÚDO)
2915
2920
TK
2925
E
E-SK(TK)
2930
2940 (KSM)
SK
2950
RO
2960
DIREITOS DE USO
2965

FIG. 29

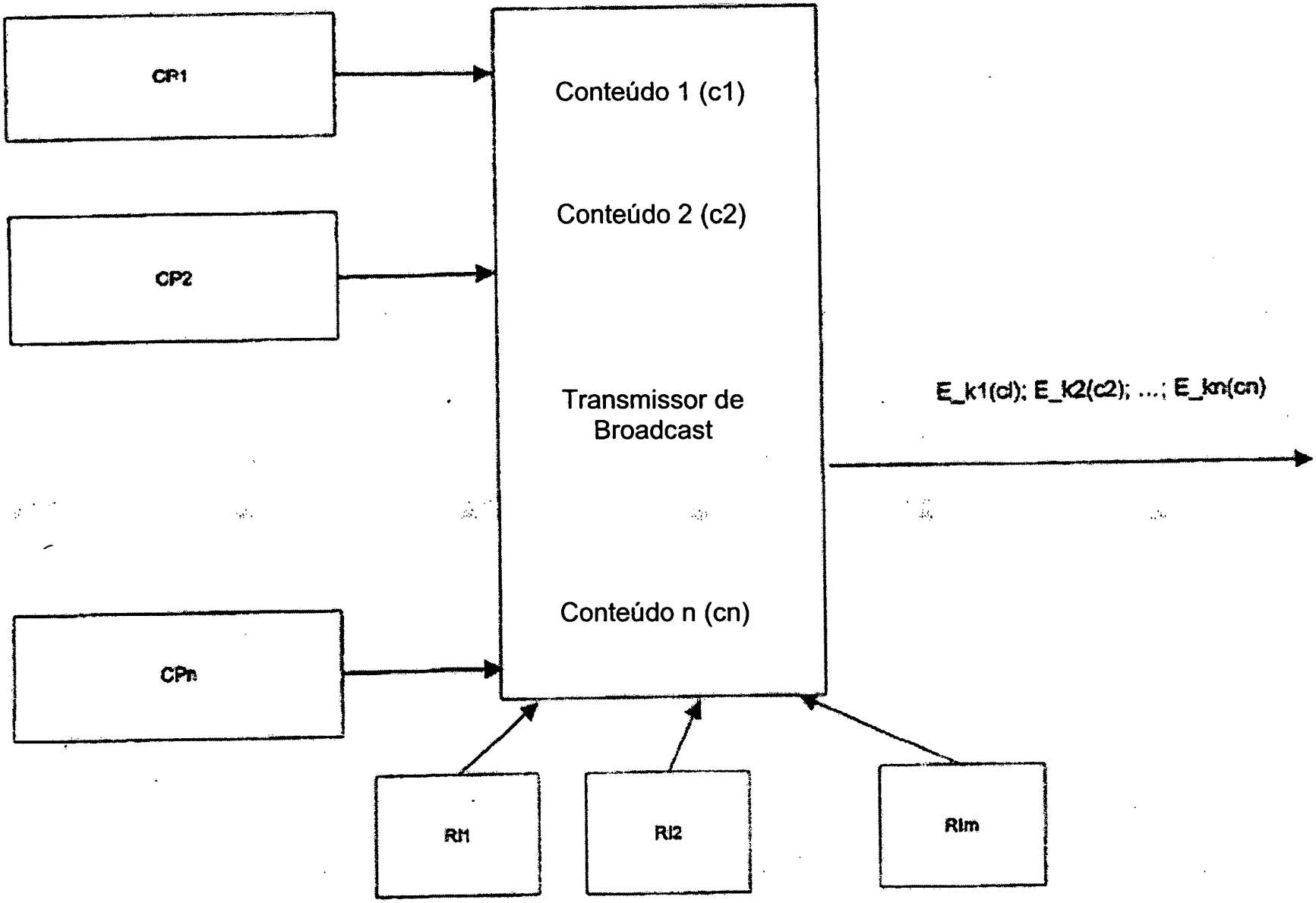

CP1
CP2
CPn
Conteúdo 1 (c1)
Conteúdo 2 (c2)
Transmissor de Broadcast
Conteúdo n (cn)
E_k1(c1); E_k2(c2); ...; E_kn(cn)
RM
RI2
RIm

FIG. 30

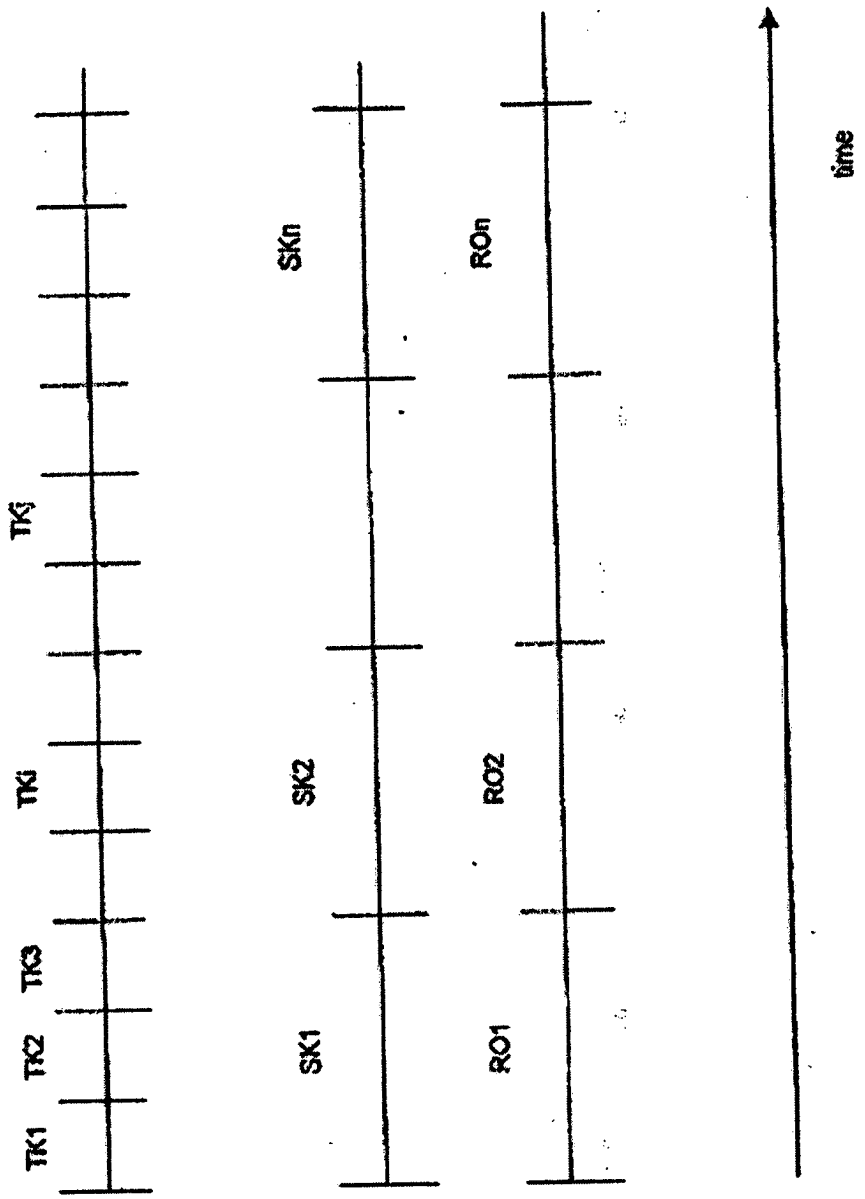
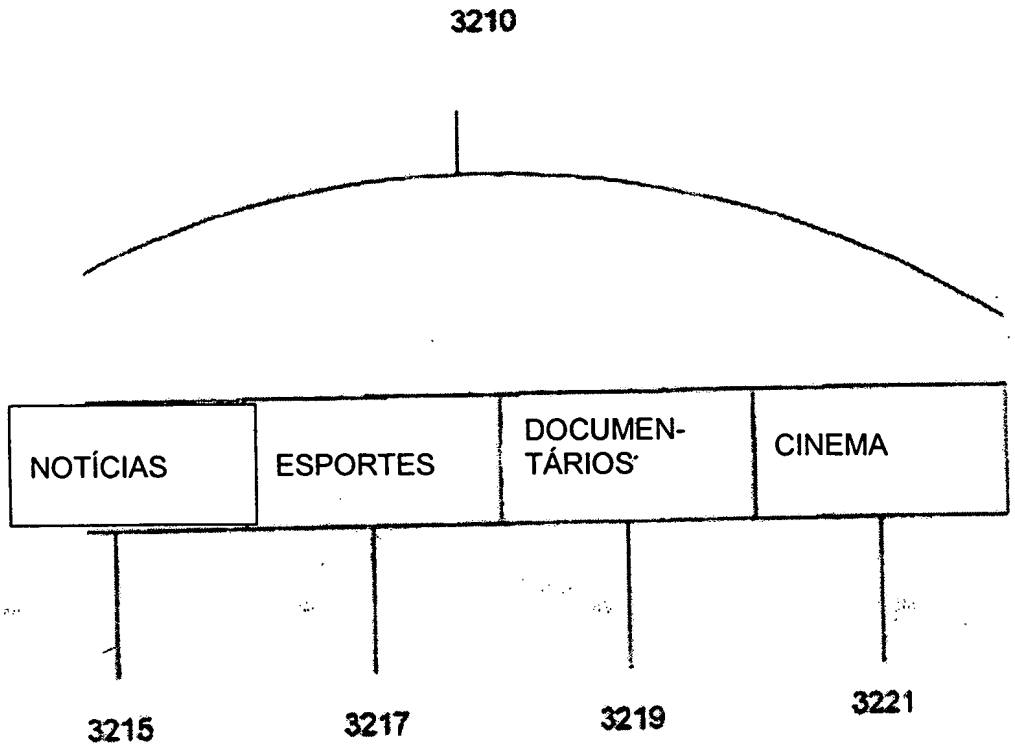


FIG. 31


3210
NOTÍCIAS
ESPORTES
DOCUMEN-
TÁRIOS
CINEMA
3215
3217
3219
3221

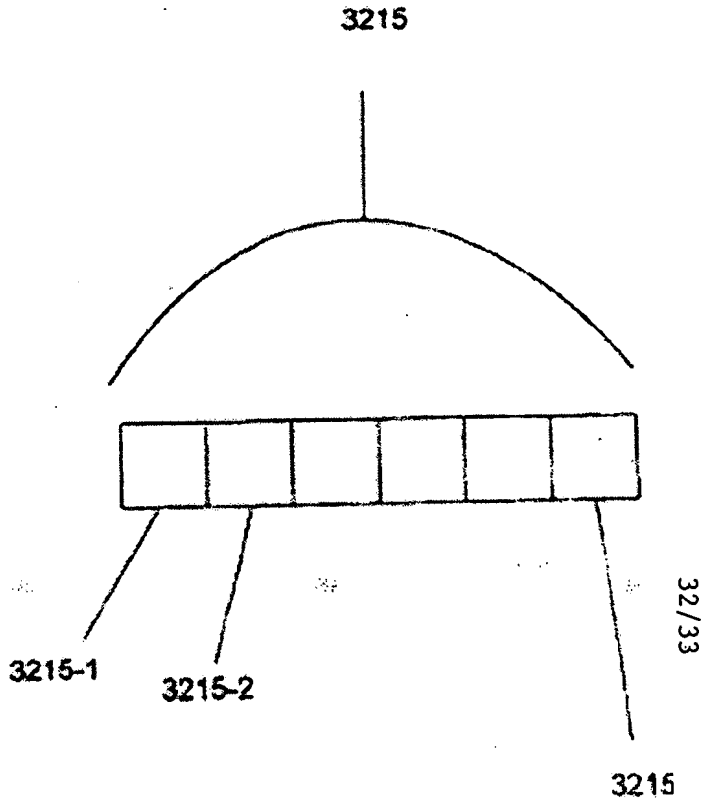

3215
3215-1
3215-2
3215

FIG. 32

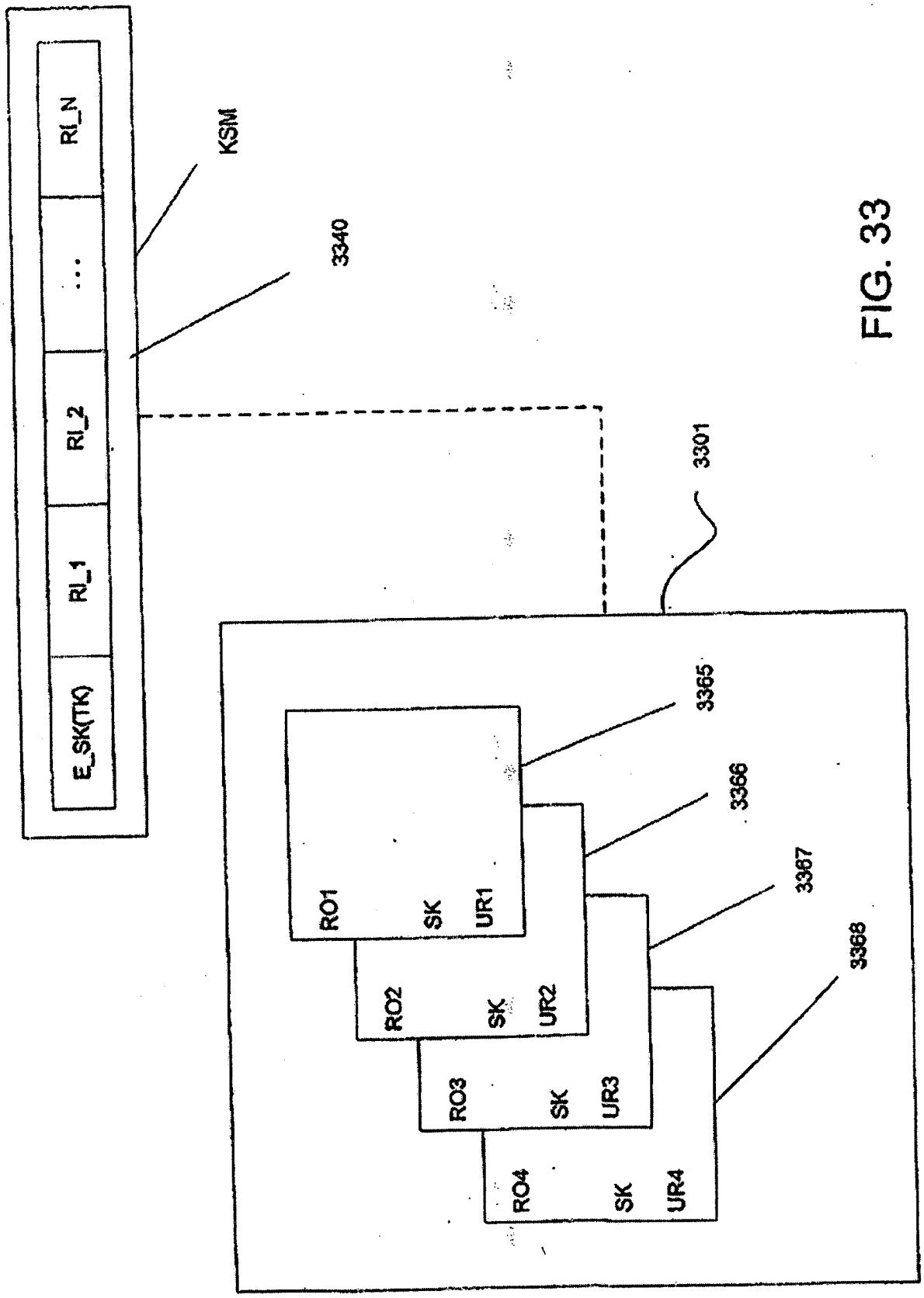

KSM
3340
E_SK(TK)
RI_1
RI_2
...
RI_N
3301
3365
3366
3367
3368
RO1
SK
UR1
RO2
SK
UR2
RO3
SK
UR3
RO4
SK
UR4

FIG. 33

 PI0612027-0

RESUMO

"MÉTODO PARA TRANSMITIR UM FLUXO DE DADOS PARA O DISPOSITIVO, DISPOSITIVO DE LEITURA DE COMPUTADOR, MÉTODO PARA RECEBER UM FLUXO DE DADOS DE UM SISTEMA DE COMUNICAÇÃO DURANTE A SESSÃO DE MULTIMÍDIA, MÉTODO PARA OBTER O FLUXO DE DADOS DO SISTEMA DE COMUNICAÇÃO, E, MÉTODO PARA TRANSMITIR OS DADOS STREAMING PARA O RECEPTOR."

A presente invenção provê métodos, aparelhos, e sistemas para entregar o conteúdo streaming protegido para o dispositivo de recepção. Em um aspecto da presente invenção, um radio difusor provê o conteúdo streaming. Para assegurar os visualizadores são autorizados apropriadamente, o conteúdo streaming é cifrado com a chave de tráfego. A chave de tráfego é fornecida para os usuários através da mensagem de fluxo da chave, que é cifrada com a tecla de serviço. O usuário obtém ao menos um objeto de direito dos emissores de direito e ao menos um objeto de direito inclui a chave de serviço, de forma que o conteúdo streaming possa ser usado. Ao menos um objeto de direito também contêm a informação considerando os direitos de uso que podem ser configurados pelo emissor de direitos de forma que, dependendo do usuário e/ou do dispositivo de recepção, diferentes direitos podem estar disponíveis. A mensagem de fluxo de chave pode incluir um valor variável de categoria de programa que indica o tipo de conteúdo e em conjunção com os direitos do objeto, determina quais direitos de uso existem para o conteúdo streaming.