INSTITUTO NACIONAL
DA PROPRIEDADE INDUSTRIAL

(11) Número de Publicação: **PT 1576818 E**

(51) Classificação Internacional:
H04N 7/16 (2006.01) ***H04N 7/167*** (2006.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2003.12.01**

(30) Prioridade(s): **2002.12.03 CH 0204402**

(43) Data de publicação do pedido: **2005.09.21**

(45) Data e BPI da concessão: **2006.11.02**
002/2007

(73) Titular(es):
NAGRACARD SA
22, ROUTE DE GENEVE CH-1033 CHESEAUX-SUR-LAUSANNE CH

(72) Inventor(es):
OLIVIER BRIQUE CH
CHRISTOPHE GOGNIAT CH

(74) Mandatário:
VÍTOR LUÍS RIBEIRO CARDOSO
LARGO DE SÃO DOMINGOS, Nº1 2910-092 SETÚBAL PT

(54) Epígrafe: **MÉTODO DE GESTÃO PARA A VISUALIZAÇÃO DAS DESCRIÇÕES DOS EVENTOS COM ACESSO CONDICIONAL**

(57) Resumo:
MÉTODO DE GESTÃO PARA A VISUALIZAÇÃO DAS DESCRIÇÕES DOS EVENTOS COM ACESSO CONDICIONAL

DESCRIÇÃO

MÉTODO DE GESTÃO PARA A VISUALIZAÇÃO DAS DESCRIÇÕES DOS EVENTOS COM ACESSO CONDICIONAL

A presente invenção refere-se a um método de gestão para a visualização das descrições dos eventos com acesso condicional, em particular para a televisão por assinatura.

Nos sistemas com acesso condicional, em particular no âmbito da televisão digital por assinatura, um fluxo de dados digitais é transmitido ao televisor. Este fluxo está encriptado para poder controlar a utilização e para definir as condições para essa utilização. Esta encriptação é realizada graças às palavras de controlo (*Control Words*) as quais são mudadas a intervalos regulares (normalmente entre 5 e 30 segundos) para dissuadir qualquer tipo de ataque que tente encontrar essa palavra de controlo.

Para que o receptor possa descodificar o fluxo encriptado com estas palavras de controlo, estas últimas são enviadas independentemente do fluxo em mensagens de controlo (ECM) encriptadas por uma chave própria do sistema de transmissão entre um centro de gestão e um módulo de segurança da unidade do utilizador. De facto, as operações de segurança são efectuadas num módulo de segurança (SC) que habitualmente está realizado com a forma de um cartão inteligente, considerado inviolável. Este módulo pode ser do tipo amovível ou pode estar directamente integrado no receptor.

No momento da descodificação de uma mensagem de controlo (ECM), no módulo de segurança (SC) é verificado, se há o direito para aceder ao fluxo considerado. Este direito pode

ser gerido pelas mensagens de autorização (EMM) que carregam este direito no módulo de segurança. Outras possibilidades são igualmente possíveis como por exemplo o envio de chaves de descodificação.

Para a exposição à continuação, chamar-se-á "evento" a um conteúdo de vídeo, áudio (por exemplo MP3) ou dados (por exemplo um programa de jogo) que de acordo com o método conhecido está encriptado pelas palavras de controlo, podendo cada evento estar encriptado por uma ou várias palavras de controlo, tendo cada um deles um período determinado de validade.

A contabilização da utilização destes eventos está actualmente baseada no princípio da assinatura, da compra de eventos ou do pagamento por unidade de tempo.

A assinatura permite definir um direito associado a um ou vários canais de difusão que transmitem estes eventos e permite ao utilizador obter estes canais descodificados se o direito está presente no seu módulo de segurança.

Paralelamente, é possível definir os direitos próprios de um evento, como por exemplo um filme ou um jogo de futebol. O utilizador pode adquirir esse direito (compra por exemplo) e esse evento será especificamente gerido por esse direito. Este método é conhecido sob a denominação "*pay-per-view*" (PPV, pagar para ver).

Uma mensagem de controlo (ECM) não contém unicamente a palavra de controlo, mas também as condições em que esta deve ser reenviada ao receptor/descodificador. No momento da descodificação das palavras de controlo, verificar-se-á se um

direito associado às condições de acesso enunciadas na mensagem está presente no módulo de segurança.

A palavra de controlo só é devolvida à unidade de utilizador quando a comparação é positiva. Esta palavra de controlo está contida numa mensagem de controlo ECM que está encriptada por uma chave de transmissão.

Para que o direito esteja presente no módulo de segurança, habitualmente este é carregado neste módulo por uma mensagem de autorização (EMM) que, por razões de segurança, habitualmente está encriptada com uma chave diferente chamada chave de direito (RK).

Segundo uma forma conhecida de difusão de televisão por assinatura, os três elementos seguintes são necessários para descodificar um evento num momento dado:

- os dados relativos ao evento encriptado por uma ou várias palavras de controlo (CW),

- a ou as mensagens de controlo ECM que contêm as palavras de controlo (CW) e as condições de acesso (AC),

- o direito correspondente memorizado no módulo de segurança que permite verificar as ditas condições de acesso.

Quando é desejável que o utilizador visualize os canais ou serviços ou os eventos a que ele acedeu, da mesma maneira a aqueles para os quais pode conseguir os direitos, os princípios descritos acima são igualmente utilizados. Para isso, é utilizada uma guia electrónica (EPG = *Electronic Program Guide*) e são assinalados, por exemplo a verde, os

eventos ou canais para os quais os direitos já tinham sido adquiridos e a vermelho aqueles que ainda não têm os direitos adquiridos.

Quando a caracterização dos direitos é simples, por exemplo quando o utilizador subscreveu certos serviços predefinidos por um determinado período, é fácil gerar uma EPG que considere estes direitos. Inversamente, quando é desejável gerir direitos mais complexos, realizar ofertas promocionais ou utilizar condições que não foram previstas na assinatura, os sistemas actuais não permitem gerir facilmente estes elementos.

O Pedido de Patente WO 97/42762 descreve um sistema de acesso às informações, que particularmente pode ser utilizado no âmbito da televisão por assinatura. Neste sistema, as mensagens de autorização são enviadas aos descodificadores dos utilizadores. Estas mensagens contêm, de forma habitual, os direitos de acesso aos eventos de televisão por assinatura. Estas contêm também apontadores que indicam uma posição de memória que permitem obter informações adicionais. Estas informações adicionais podem em particular ser informações que não estão codificadas e que se referem aos eventos em si mesmos ou a programas. Estas informações estão ligadas ao descodificador e habitualmente pode-se aceder a elas sem a necessidade de as descodificar. Estas não estão contidas nas mensagens de autorização.

Este sistema não permite gerir os aspectos da segurança ligados aos dados complementares e não permite gerir as condições de acesso variáveis em função dos direitos existentes para cada utilizador, estas condições de acesso por princípio devem ser protegidas.

A presente invenção se propõe paliar os inconvenientes dos dispositivos do estado da técnica anterior realizando um dispositivo no qual é possível gerir os direitos complexos oferecendo portanto uma grande flexibilidade de utilização a um difusor.

Este objectivo é obtido por um processo de gestão da visualização das descrições dos eventos com acesso condicional, que compreende as seguintes etapas:

- o envio de dados que formam uma guia electrónica de programas (EPG), a um descodificador (STB), sendo esta guia electrónica destinada à visualização dos eventos que serão difundidos, estes dados compreendem, para cada evento, pelo menos um identificador, dados de texto e um bloco condicional que inclui as condições requeridas para aceder a esse evento,

- o envio de pelo menos uma mensagem de autorização (EMM) a um módulo de segurança (SC) associado ao descodificador, definindo esta mensagem os direitos de acesso a um evento;

caracterizado por o método incluir ainda as seguintes etapas:

- o envio ao dito módulo de segurança (SC), do bloco condicional (PECM),

- o tratamento, no módulo de segurança, da condição de acesso contida no dito bloco condicional (PECM), e

- o reenvio pelo módulo de segurança de uma mensagem que indica, em função da condição de acesso para cada evento e dos direitos de acesso contidos no módulo de segurança, se o

direito para cada evento está presente ou não no módulo de segurança, e

- por a condição de acesso contida no bloco condicional (PECM) ser expressa com a forma de uma operação (Op) descrita por uma petição numa linguagem estruturada.

A presente invenção e as suas vantagens serão melhor entendidas com referência à descrição de uma forma específica de a realizar e em relação aos desenhos anexos, em que:

- a figura 1 ilustra esquematicamente um forma de realizar a uma guia electrónica EPG de acordo com a técnica anterior;

- a figura 2 ilustra esquematicamente o conteúdo da mensagem de controlo ECM utilizado na forma de realização da figura 1;

- a figura 3 ilustra o conteúdo de uma mensagem de controlo ECM de acordo com a presente invenção;

- a figura 4 ilustra o conteúdo de um bloco condicional utilizado no sistema de acordo com a invenção; e

- a figura 5 representa um modo de realizar uma guia electrónica EPG de acordo com a invenção.

As figuras 1 e 2 descrevem os sistemas conhecidos da técnica anterior. Nestes sistemas, os dados que compõe a guia electrónica de programa EPG são transmitidos por um canal de serviço e estes estão compostos por informações horárias e de texto, como particularmente o título do evento, a descrição e eventualmente comentários.

Os dados da EPG contêm igualmente o serviço ao qual este evento está ligado relacionado com o direito de acesso, estando por exemplo os serviços indicados de S1 a S48.

Paralelamente, o evento difundido está acompanhado pelas mensagens de controlo ECM que contêm um certo número de campos pré-definidos, que na figura 2 têm os números referências de 11 a 14, como particularmente o identificador do evento (campo 13), o serviço ao qual está ligado (campo 14), a palavra de controlo CW (campo 11), a hora e a data da difusão (campo 12) e eventualmente, um crédito associado ao evento. Graças a esta estrutura pré-determinada por campos, a estrutura da mensagem está definida de maneira a que por exemplo no campo 14, sempre se vá a encontrar o número de um serviço SID.

Este serviço é inicializado por uma mensagem de autorização EMM que tem como objectivo definir um bloco de assinatura no módulo de segurança SC, contendo este bloco entre outros o período de validade de este serviço.

Para visualizar a guia electrónica EPG no televisor de um utilizador, o descodificador STB lê os direitos contidos no módulo de segurança SC isto é os blocos anteriormente definidos. Mais precisamente, determina, de acordo com estes direitos, a lista dos serviços disponíveis assim como a duração ou a data de validade de cada serviço. O descodificador dispõe portanto, por uma parte, de uma base de dados proveniente do módulo de segurança e que contém a lista dos serviços disponíveis com o seu período de validade assim como uma base de dados destinada ao EPG, que contém a lista dos eventos, o serviço ao qual está ligado e a data da difusão.

Para cada evento, o descodificador pode portanto verificar se o módulo de segurança dispõe do direito para o serviço considerado e se esse direito será válido no momento da difusão do evento. Em função da resposta desta comparação, o evento será mostrado na EPG, por exemplo a vermelho se o direito não está adquirido e a verde se esse direito foi adquirido e portanto está presente no módulo de segurança.

Na figura 1, um "Yes" é mostrado na última coluna da EPG em relação ao evento considerado se o direito para este evento está adquirido e um "No" no caso contrário.

No momento da difusão de um evento, as mensagens de controlo ECM, que contêm as palavras de controlo CW e associadas a este evento, são tratadas no módulo de segurança para verificar a existência dos direitos associados a esse evento. Se os direitos estão presentes, cada mensagem de controlo ECM é tratada para extrair as palavras de controlo CW nela contida. Esta palavra de controlo é então enviada ao descodificador que descodifica os dados que tinham sido encriptados com esta palavra de controlo específica.

Este modo de realização funciona perfeitamente quando as condições são simples, por exemplo quando o utilizador tem uma assinatura para um conjunto de serviços. Neste caso, o descodificador compara o conteúdo dos campos pré-definidos nas informações que compõe o EPG com o conteúdo da memória do módulo de segurança e obtém uma resposta directamente explorável.

Quando é desejável propor ofertas promocionais de forma particular, pode ser necessário definir condições complexas, para as quais uma estrutura fixa com os campos pré-definidos

não se considera adaptada. Um exemplo de uma oferta promocional deste tipo consiste em permitir um livre acesso a um conjunto de canais, no dia do aniversário de cada assinante. Com um sistema convencional, esta oferta pode ser proposta, mas ao preço de uma grande complexidade. De facto, para permitir isto, é necessário criar direitos complementares, mais precisamente 365 blocos de assinatura, correspondendo cada um a um dia do ano. Estes direitos são geridos como os outros direitos, o que significa que são transmitidos pelas mensagens de autorização EMM. Estas mensagens devem ser enviadas de maneira repetitiva a todos os beneficiários, para assegurar que os direitos foram bem recebidos.

Com a recepção desta mensagem, um novo bloco de assinatura é criado no módulo de segurança para esta única utilização. Deve ser assinalado que estas mensagens vão abranger uma largura de faixa e meios criptográficos em particular porque o nível da encriptação destas mensagens é elevado.

Outro exemplo de oferta promocional consiste em facturar um evento dado segundo várias diferentes quantidades em função do tipo de assinatura subscrita. O titular de uma assinatura de canal temático desportivo pode por exemplo pagar um jogo de futebol a um determinado preço, enquanto que as pessoas que não têm este tipo de assinatura deverão pagar outro montante para este mesmo jogo. Neste estado, não é possível gerir este tipo de regras porque a identificação do evento é rigorosamente igual para todos os utilizadores, enquanto que as condições de acesso para este evento dependem do evento e dos parâmetros próprios do utilizador.

Actualmente, segundo o estado da técnica, a solução consistiria em enviar uma mensagem de autorização EMM própria de cada utilizador com o montante do evento considerando as suas condições específicas. Pode-se facilmente imaginar a quantidade de mensagens a transmitir para satisfazer todos os utilizadores.

De maneira mais geral, para poder aplicar as condições particulares para um evento particular, é necessário que estas condições tenham sido previamente previstas na assinatura dos utilizadores implicados. Se este não é o caso, a gestão dos casos particulares pode resultar difícil ao mesmo impossível. Em todos os casos, para gerar os direitos particulares no módulo de segurança, é necessário enviar as mensagens de autorização EMM, a uma frequência suficiente para assegurar que a maioria dos utilizadores tenha recebido bem os direitos que lhe estão destinados.

Este modo de realização é pouco cómodo porque satura a memória de maneira importante e porque o tráfico das mensagens de autorização EMM utiliza inutilmente a largura de faixa disponível.

Na figura 3 que descreve um modo de realização da invenção, a mensagem de controlo ECM não contém um dado numa posição de memória pré-definida, mas sim uma operação Op. Esta está escrita em forma de petição, utilizando por exemplo um linguagem sintáctica como aquela conhecido com o acrónimo SQL (*Structured Query Language*, linguagem de consulta estruturada).

A presente invenção é particularmente vantajosa em relação aos sistemas conhecidos pelo estado da técnica anterior

porque as condições definidas pelos pedidos do tipo SQL podem em qualquer momento ser imaginadas, modificadas ou utilizadas de maneira muito flexível. O facto de franquear os campos de dados pré-definidos nas mensagens de controlo ECM abre uma via a combinações que não tinham sido pensada no momento do arranque do sistema e que portanto não estavam previstas na assinatura dos utilizadores.

Esta gestão simplificada tem como consequência o facto de permitir propor ofertas muito diversificadas, inclusive para um número muito restrito de pessoas. Portanto é possível gerar ofertas muito determinadas que se aproximem o mais possível das perspectivas de marketing da empresa.

No momento do tratamento de uma mensagem de controlo ECM deste tipo, a operação Op é tratada pelo motor SQL do módulo de segurança SC e do resultado dependerá o reenvio ou não da palavra de controlo CW contida nessa mesma mensagem.

Da mesma maneira que para as mensagens de controlo ECM, está igualmente previsto, no âmbito da invenção, substituir os campos de uma mensagem de autorização EMM por um pedido de tipo SQL.

Os dados memorizados no módulo de segurança, que definem os blocos de assinatura, ficam invariáveis, variando apenas as operações sobre estes dados.

A título de exemplo, um pedido deste tipo poderia ser:

- Serviço S22 válido ou data aniversário = 10 de Outubro.

Outro exemplo de pedido complexo para uma compra impulsiva poderia ser:

- Se o módulo de segurança contém os direitos para os serviços S1, S8 e S12, deduzir um valor de 4 USD para o evento Ev 1, do contrário, deduzir um valor de 5 USD para este evento.

Nesta forma de realizar a invenção, o descodificador STB não está habilitado para tratar um pedido complexo em linguagem SQL, fundamentalmente por razões de segurança.

No âmbito desta invenção, a solução consiste em modificar os dados transmitidos ao EPG, esta modificação consiste em incluir nestes dados um novo bloco que é uma cópia parcial da mensagem de controlo ECM que será transmitido com o evento considerado.

Este bloco denominado bloco condicional (PECM) compreenderá pelo menos o mesma pedido SQL que a mensagem de controlo do qual está derivado. De acordo com a implementação escolhida, os outros campos como por exemplo a palavra de controlo poderão ser eliminados. É evidente que as mensagens de controlo ECM são transmitidas no momento em que o evento é visualizado pelo utilizador, já que estas contêm as palavras de controlo CW. Inversamente, os blocos condicionais devem ser previamente enviados já que estes são utilizados para formar a EPG que permite ao utilizador visualizar antecipadamente, os direitos que já tinha adquirido e aqueles que pode adquirir.

No momento da recepção destes dados pela EPG, este bloco PECM será transmitido ao módulo de segurança, o qual é capaz de

tratar os pedidos complexas, particularmente em linguagem SQL.

Este bloco PECM está ilustrado na figura 4. O módulo de segurança tratará este bloco condicional de maneira convencional e poderá extrair a petição SQL. As condições definidas nesta pedido são analisados no módulo de segurança e o resultado da petição é retransmitido ao descodificador STB. Graças a este resultado, a EPG pode ser apresentada de acordo com o anteriormente explicado, com referência à descrição do estado da técnica anterior.

Este método está representado esquematicamente pela figura 5. De maneira mais detalhada, os dados que permitem formar a EPG são transmitidos ao descodificador STB. Um bloco condicional PECM, que contém, em forma de petição SQL, a operação que permite definir as condições de acesso, é formado e depois é transmitido ao módulo de segurança SC. Este módulo trata a petição SQL. As condições da petição SQL são comparadas com os direitos inscritos no módulo de segurança, o qual permite determinar para que os eventos estão adquiridos ou podem ser adquiridos os direitos. Estes direitos disponíveis estão associados aos dados da EPG. A lista dos eventos é apresentada a continuação no televisor do utilizador, distinguindo, para cada evento se o módulo de segurança dispõe dos direitos ou não.

Lisboa, 29 de Janeiro de 2007

REIVINDICAÇÕES

1. Um método de gestão para a visualização das descrições de eventos com acesso condicional, que compreende as seguintes etapas:

- o envio dos dados que formam uma guia electrónica de programas (EPG), a um descodificador (STB), estando esta guia electrónica destinada à visualização dos eventos que serão difundidos, estes dados têm, para cada evento, pelo menos um identificador, dados de texto e um bloco condicional que inclui as condições requeridas para o acesso a este evento,

- enviar pelo menos uma mensagem de autorização (EMM) a um módulo de segurança (SC) associada ao descodificador, definindo esta mensagem os direitos de acesso a um evento;

caracterizado por o método compreender também as seguintes etapas:

- enviar ao dito módulo de segurança (SC), o bloco condicional (PECM),

- tratar no módulo de segurança, a condição de acesso contida no dito bloco condicional (PECM), e

- reenviar pelo módulo de segurança uma mensagem que indica, em função da condição de acesso para cada evento e dos direitos de acesso contidos no módulo de segurança, se o direito está presente ou não para cada evento no módulo de segurança, e

por a condição de acesso contida no bloco condicional (PECM) ser expressa em forma de uma operação (Op) descrita por uma petição numa linguagem estruturada.

2. Um método de gestão de acordo com reivindicação 1, caracterizada por a petição estar escrita em linguagem SQL (*Structured Query Language*, linguagem de consulta estruturada).

3. Um método de gestão de acordo com a reivindicação 1, caracterizado por um evento estar encriptado pelo menos por uma palavra de controlo (CW), estas palavras de controlo (CW) serem transmitidas ao descodificador (STB) na forma de uma mensagem de controlo (ECM) encriptada que inclui igualmente as condições de acesso, consistindo este método em transmitir no bloco condicional (PECM) toda ou parte da mensagem de controlo (ECM).

4. Um método de gestão de acordo com a reivindicação 3, caracterizado por o bloco condicional (PECM) incluir unicamente os dados relativos às condições de acesso contidas nas mensagens de controlo (ECM).

5. Um método de gestão de acordo com a reivindicação 4, caracterizada por os ditos dados relativos às condições de acesso serem enviadas encriptados ao bloco condicional (PECM).

6. Um método de gestão de acordo com a reivindicação 4, caracterizado por os ditos dados relativos às condições de acesso estarem descodificados no bloco condicional (PECM).

Lisboa, 29 de Janeiro de 2007

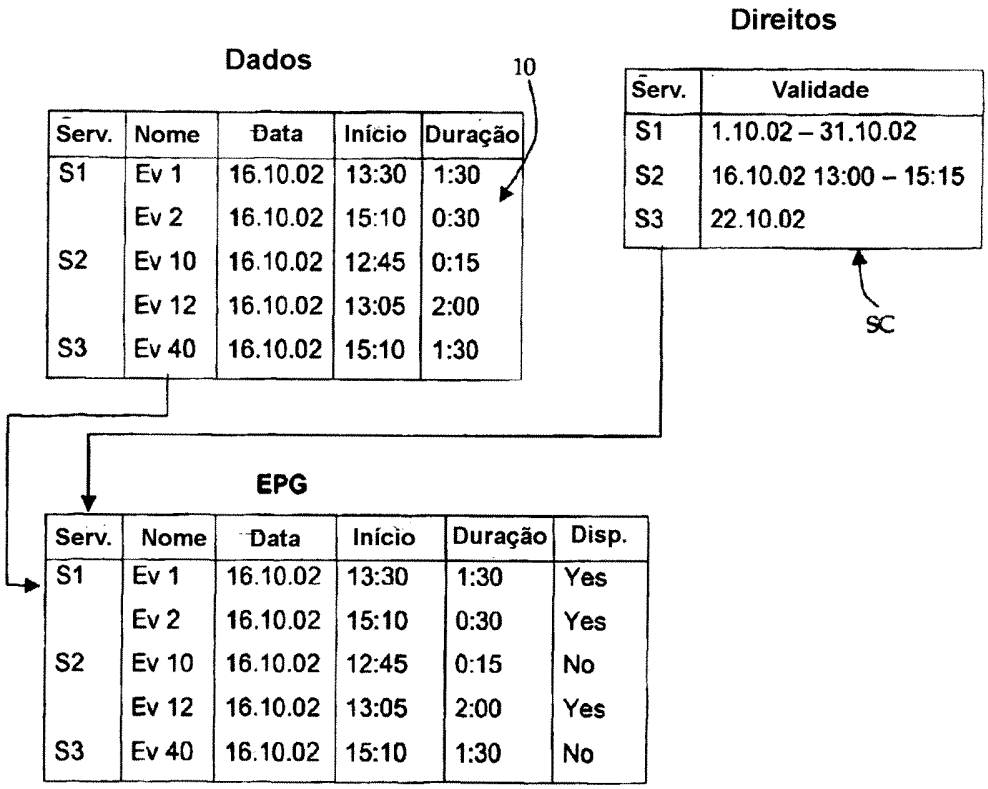

FIG. 1

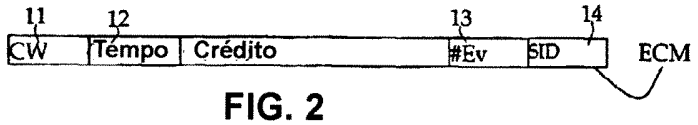

FIG. 2

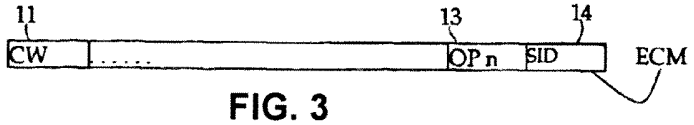

FIG. 3

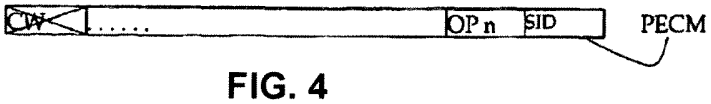

FIG. 4

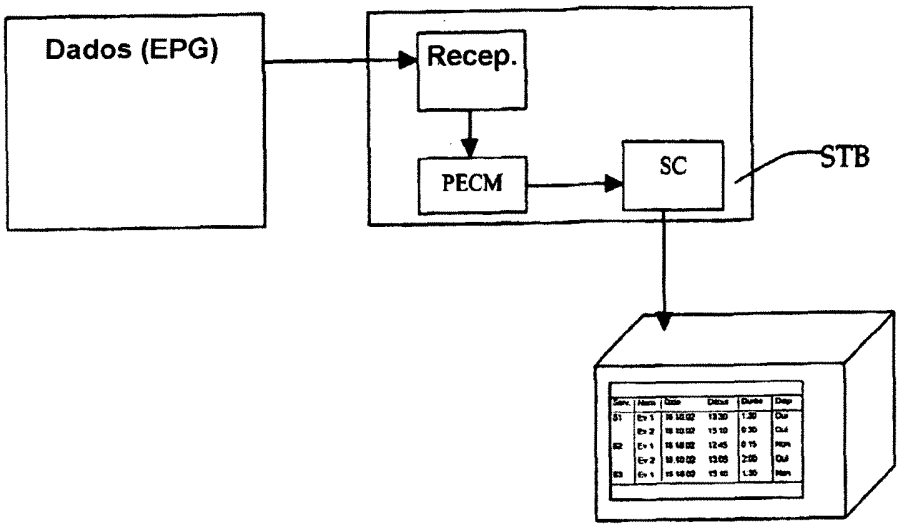

FIG. 5