



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

(11) PI 0206703-0 B1

(22) Data do Depósito: 13/11/2002

(45) Data de Concessão: 03/05/2016
(RPI 2365)



(54) Título: MÉTODO PARA PROVER CONFIANÇA VERIFICÁVEL AUTOMATICAMENTE EM UM PROCESSO DE RESOLUÇÃO DE CONTEÚDO, E, DISPOSITIVO (PDR)

(51) Int.Cl.: H04N 7/173

(30) Prioridade Unionista: 18/10/2002 EP 02257275.4, 27/11/2001 EP 01309950.2

(73) Titular(es): TP VISION HOLDING B.V.

(72) Inventor(es): FRANCISCUS L. A. J. KAMPERMAN, ALEXIS S. R. ASHLEY, PIM T. TUYLS

“MÉTODO PARA PROVER CONFIANÇA VERIFICÁVEL AUTOMATICAMENTE EM UM PROCESSO DE RESOLUÇÃO DE CONTEÚDO, E, DISPOSITIVO (PDR)”

5 A invenção relaciona-se a um processo de resolução de conteúdo no qual um identificador de referência de conteúdo (CRID) identificando um item de conteúdo que é resolvido usando uma gravação de autoridade de resolução (RAR) para obter um localizador identificando uma localização onde o item de conteúdo pode ser obtido.

10 À medida que o número de canais disponíveis para espectadores de televisão tem aumentado, juntamente com a diversidade de conteúdo de programação disponível em tais canais, tem se tornado crescentemente desafiador para espectadores de televisão identificar programas de televisão de interesse. Historicamente, espectadores de televisão identificam programas de televisão de interesse analisando guias de
15 programas de televisão impressos. Como o número de programas de televisão tem aumentado, tem se tornado crescentemente difícil identificar efetivamente programas de televisão desejáveis usando tais guias impressos.

Mais recentemente, guias de programas de televisão tornaram-se disponíveis em formato eletrônico, freqüentemente referidos como guias de
20 programas eletrônicos (EPG). Como guias de programas de televisão impressos, os EPG apresentam visões gerais do conteúdo disponível que podem ser navegadas pelo usuário. O conteúdo de termo geral compreende tipicamente coisas como música, canções, filmes, programas de televisão, imagens e similares, mas também podem se referir a cenas individuais,
25 objetos MPEG-4 e assim por diante.

O EPG compila a visão geral a partir de metadados que acompanham os itens de conteúdo individual. Metadados para itens de conteúdo são disponíveis a partir de uma variedade de fontes. Metadados podem ser incluídos com um fluxo de radiodifusão, por exemplo, como

tabelas MPEG-2, ou transferidos de bases de dados externas. Por exemplo, um receptor de televisão ou Gravador Digital Pessoal pode ser provido de uma conexão à Internet, que permite que o dispositivo acesse metadados tornados disponíveis através da “World-Wide Web”.

5 Os metadados geralmente compreendem informações tais como título, artista, gênero e assim por diante, e podem também conter um identificador de referência de conteúdo único (CRID), algumas vezes também chamado identificador de referência de conteúdo. Usando o CRID, cada item de conteúdo individual pode ser identificado univocamente. Adicionalmente, usando o CRID, informação adicional pode ser recuperada de uma base de dados. Por exemplo, um usuário pode selecionar um item de conteúdo que deseja ver a partir do EPG, embora a hora e local da radiodifusão ainda não sejam conhecidos. Usando o CRID, o sistema pode então recuperar a hora e local da radiodifusão do item de conteúdo quando esta informação se torna disponível. O CRID não é restrito a transmissões de radiodifusão de conteúdo. Poderia também se referir a uma localização na Internet, ou a qualquer outra fonte. A finalidade da resolução de conteúdo é permitir a aquisição de uma instância específica de um item específico de conteúdo. Por exemplo, um usuário pode desejar gravar um episódio de uma série de televisão, mas ele não sabe necessariamente quando e onde aquele episódio se tornará disponível. Ele pode então usar seu gravador digital pessoal (PDR) ou dispositivo similar para entrar com uma referência do episódio ou série, por meio do CRID. Notar que um CRID pode se referir a uma série inteira ou a um episódio individual desta.

25 Tendo recebido um CRID para um item de conteúdo, o PDR tenta obter a localização do item de conteúdo. Esta informação é chamada de localizador e contém a data, hora e canal no qual o item de conteúdo será radiofundido. O usuário entretanto, não precisa se preocupar com isto. Uma vez que o PDR tem obtido o localizador do item de conteúdo, o PDR aguarda

a data e horário especificado e então grava o episódio enquanto este é radiofundido no canal especificado. Naturalmente, se o localizador indica uma localização na Internet ou similar, o PDR pode simplesmente recuperar o conteúdo a partir da localização indicada tão logo este se torne disponível.

- 5 O corpo de padronização TV a Qualquer Tempo (“TV-Anytime”) provê um ID de Referência de Conteúdo padronizado. Ver TV-Anytime Forum, www.tv-anytime.org, Specification Series: S-4, on Content Referencing (Normative), Document SP004V11, 14 de Abril de 2001.

10 A sintaxe do CRID conforme usada pela TV a Qualquer Tempo é conforme segue:

CRID: //<authority>/<data>

- 15 O campo <authority> indica o corpo que criou o CRID. Uma autoridade proverá também a capacidade do CRID ser resolvido em localizadores ou outros CRID. Um localizador é o nome para localizações no tempo e espaço do conteúdo. O campo <data> é um cadeia de formato livre que é conforme à definição dos Identificadores de Recurso Uniforme (URI) conforme dado na RFC 2396. Esta cadeia deveria ser significativa para a autoridade dada pelo campo <authority>.

- 20 O CRID é usado para resolução de localização, que pode ser definida como o processo de traduzir um CRID em outros CRID ou localizadores. Por exemplo, um CRID para uma série de TV inteira poderia ser traduzido em uma série de CRID para os episódios individuais daquela série. A resolução de localização pode ser feita no dispositivo de gravação (tipicamente um Gravador Digital Pessoal ou PDR) ou remotamente. Um provedor de resolução efetua resolução de localização. Os provedores de resolução usam gravações de autoridade de resolução (RAR) para serem identificados e localizados. Uma RAR inclui pelo menos um campo
- 25 <authority>, correspondendo a um corpo que cria os CRID.

Uma RAR também contém uma URL e o nome do provedor

de resolução. A URL aponta para a localização onde a informação de resolução pode ser encontrada. O nome do provedor de resolução contém o nome do corpo que está provendo resolução de localização. Estas RAR são tornadas disponíveis para os PDR.

5 Usando a abordagem acima, qualquer um conhecendo a localização do conteúdo poderia atuar como um provedor de resolução.

É um objetivo da invenção restringir o processo de resolução do conteúdo acima de tal modo que certas entidades designadas podem participar.

10 Este objetivo é alcançado de acordo com a invenção, em um método compreendendo aplicar uma medida a pelo menos um dos CRID, as RAR e o localizador provendo integridade e autenticação de origem.

Provedores de conteúdo e serviço podem desejar que somente provedores de resolução autorizados efetuem resolução de conteúdo para seu
15 conteúdo, por exemplo, para ser capaz de proteger sua reputação. Por outro lado, para consumidores e PDR é importante ser capaz de se apoiar e confiar na autoridade do CRID e provedor de resolução, de tal modo que se possa obter o conteúdo correto. Então, os inventores verificaram que é desejável reforçar a abordagem acima, de modo que, a confiança verificável
20 automaticamente pode ser introduzida no processo de resolução de conteúdo. Esta proteção preferivelmente envolve autenticação de origem de dados e proteção de integridade, mas pode também envolver proteção contra acesso não autorizado, ou manutenção de confidencialidade.

Se uma terceira parte pode mudar os metadados ou tabela
25 CRID, pode fazer com que o PDR grave outras informações do que foi pretendido, incluindo comerciais, trailers ou mesmo outro conteúdo. Isto é muito aborrecido para um usuário e pode diminuir a confiança que o usuário tem no sistema. Para evitar isto, o PDR pode desejar verificar se o conteúdo vem de uma fonte acreditada. Se os dados podem ser autenticados para

originar de uma fonte mesmo quando são distribuídos usando canais diferentes, o PDR pode usar isto para efetuar uma escolha, quando confrontado com fontes múltiplas do mesmo conteúdo. Um exemplo disto é quando os dados de um certo show da BBC podem ser autenticados como sendo gerados pela BBC, isto aumenta a probabilidade de que esta informação esteja correta.

Uma realização compreende prover uma assinatura digital para pelo menos uma porção de pelo menos um dos CRID, a RAR e o localizador. Somente um CRID, RAR ou localizador adequadamente assinados, serão aceitos pelo PDR. Devido à assinatura, estes podem ser acreditados como originando de uma autoridade fidedigna.

Em uma realização adicional, a assinatura digital é provida para pelo menos uma porção do localizador, e pode ser verificada usando uma chave pública provida por um dentre um provedor CRID e um provedor RAR. Este modo de localização do conteúdo a ser recuperado pode ser acreditado, isto é, o PDR pode verificar que o localizador não foi trocado e que o localizador se origina de um certo provedor de resolução.

Uma realização adicional com prover pelo menos uma porção de pelo menos um dentre o CRID, a RAR e o localizador, de forma criptografada. Deste modo somente provedores de resolução autorizados são capazes de interpretar o CRID, a RAR ou o localizador e efetuar resolução de conteúdo.

Uma realização ainda adicional compreende prover um direito de acesso ao conteúdo, juntamente com pelo menos um dentre o CRID, a RAR e o localizador. Isto tem as seguintes vantagens:

- Nada mais é requerido para o usuário contatar também separadamente um servidor de direitos.
- Se o conteúdo é protegido, usuários são em qualquer caso requeridos a contatar uma autoridade de resolução autorizada, pois eles

somente deste modo obtém os direitos corretos para usar o conteúdo.

Uma realização adicional compreende prover informação sobre a obtenção de um direito para acessar o item de conteúdo, juntamente com pelo menos um dentre o CRID, a RAR e o localizador. Deste modo, o processo de resolução de localização e um sistema DRM são adicionalmente integrados. Após localizar o conteúdo, o PDR será capaz de resolver a localização de onde obter os direitos. Um provedor de resolução pode até oferecer tal funcionalidade como um serviço ao usuário, pois ele pode ser capaz de localizar os direitos mais baratos para aquela peça específica de conteúdo e passar a localização destes direitos para o usuário.

Uma realização adicional compreende prover um benefício com pelo menos um dentre o CRID, a RAR e o localizador. Com tais meios, usuários podem ser estimulados a contatar um provedor de resolução específico pois o usuário pode receber benefícios, tais como um desconto para adquirir um filme.

A invenção relaciona-se adicionalmente a um dispositivo arranjado para resolver um identificador de referência de conteúdo identificando um item de conteúdo usando uma gravação de autoridade de resolução para obter um localizador identificando uma localização onde o item de conteúdo pode ser obtido, condicionalmente ao verificar uma medida aplicada a pelo menos um dentre o CRID, a RAR e o localizador, para verificar integridade e autenticação de origem. Várias realizações vantajosas do dispositivo são estabelecidas nas reivindicações dependentes.

Estes e outros aspectos da invenção serão aparentes e elucidados com referência às realizações ilustrativas mostradas nos desenhos, nos quais:

Fig. 1 ilustra esquematicamente o processo de resolução de conteúdo, no qual um Gravador Digital Pessoal ou PDR é instruído para gravar um item de conteúdo identificado por um Identificador de Referência

de Conteúdo CRID;

Fig. 2 ilustra esquematicamente uma primeira realização do PDR;

Fig. 3 ilustra esquematicamente uma segunda realização do PDR; e

Fig. 4 ilustra esquematicamente uma terceira realização do PDR.

Através das figuras, os mesmos rótulos de referência indicam características similares ou correspondentes. Algumas das características indicadas nos desenhos são tipicamente implementadas por software, e como tal representam entidades de software, tais como módulos ou objetos de software.

Fig. 1 ilustra esquematicamente o processo de resolução de conteúdo. Um Gravador Digital Pessoal ou PDR é instruído para gravar um item de conteúdo identificado por um Identificador de Referência de Conteúdo CRID. A instrução do PDR para gravar um item de conteúdo, ou em outras palavras programar aquele item de conteúdo para gravação, pode ser feito de uma variedade de maneiras. Um modo comum atualmente é que o usuário indique manualmente, por exemplo, selecionando o item de conteúdo no EPG, em que o item de conteúdo deve ser gravado. Será facilmente entendido que parte ou toda a funcionalidade atribuída ao PDR abaixo poderia também ser incorporada em um ou mais outros dispositivos, tais como receptores de televisão, conversores “set-top box” ou computadores pessoais.

O PDR, ou um outro dispositivo ao qual o PDR é conectado, pode ser equipado para determinar espécies de item de conteúdo em que o consumidor pode estar interessado. Isto é conhecido como perfil de usuário ou sistemas recomendados. Não perdendo de vista itens de conteúdo que o consumidor visualiza, e empregando um sistema de classificação implícito ou explícito para tais itens de conteúdo, torna-se possível prever com graus

variáveis de precisão em quais outros itens de conteúdo o consumidor pode estar interessado. Tais itens de conteúdo poderiam então ser gravados pelo PDR. Muitas técnicas para perfil de usuário são conhecidas na técnica. Quando o PDR determina, usando perfil de usuário, que um item de conteúdo particular pode ser de interesse, este programa o item de conteúdo para gravação.

O CRID para o item de conteúdo é usado para facilitar a gravação automática do item de conteúdo. O CRID poderia ser inserido manualmente pelo usuário, ou ser o resultado de selecionar um item de conteúdo através de um Guia de Programa Eletrônico. Esta segunda opção assume que o CRID é de algum modo provido pelo PDR juntamente com outros metadados usados no EPG. Alternativamente, se o CRID não é conhecido pelo usuário ou pelo PDR, o usuário poderia efetuar uma busca usando por exemplo o título do item de conteúdo em uma base de dados de metadados, e selecionar o item de conteúdo desejado a partir dos resultados de busca. O CRID é então fornecido ao PDR pela máquina de busca.

Há muitos outros modos de prover o CRID ao PDR. Por exemplo, um trailer ou visão prévia de um filme poderia ser radiofundido com o CRID embutido no conteúdo do comercial, de algum modo (por exemplo, uma marca d'água). O usuário poderia então pressionar um botão em seu controle remoto, televisão ou PDR. O PDR ou televisão extrai então o CRID do conteúdo.

Uma vez que o CRID para o item de conteúdo é conhecido, o PDR tenta obter informação de localizador para o item de conteúdo, usando o CRID como entrada. Esta informação de localizador não está necessariamente sempre disponível. Por exemplo, o CRID pode se referir a um filme que somente recentemente foi liberado nos cinemas. Este filme não é provável de ser radiofundido em televisão em futuro próximo, e então não pode ser programado usando informação do EPG. Em tal caso, o PDR poderia

regularmente tentar obter o localizador, pois o localizador pode-se tornar disponível mais tarde (por exemplo, um ano mais tarde, quando o filme estiver indo para ser transmitido na TV). O CRID poderia também se referir a uma série de TV, o qual é então resolvido em um número de vários CRID para episódios individuais daquela série. É possível que nenhuma informação de localizador esteja disponível para alguns episódios. Aqui o PDR poderia também tentar novamente, regularmente, obter o localizador(es) para aqueles episódios.

O processo de traduzir um CRID em outros CRID ou localizadores é conhecido no TV a Qualquer Tempo como resolução de localização. A resolução de localização envolve mapear uma referência de conteúdo independente de localização (o CRID) para sua localização no tempo (por exemplo, horário de transmissão programado em um sistema de radiodifusão) e espaço (canal de TV, endereço IP). Conforme explicado acima, estas localizações no tempo e espaço são referidas como “localizadores”. O processo de resolução de localização pode acontecer dentro do PDR, ou usando um servidor fisicamente remoto, tal como um servidor na Internet.

Para o PDR, o CRID contém essencialmente informação opaca, a qual não pode resolver para uma localização, sem assistência externa. Um Provedor de Resolução (RP) que provê informação de localizador para os CRID, é provido para resolver este problema. Usualmente, RP múltiplas estão disponíveis, e o PDR precisa saber quais RP usar para um CRID particular. Frequentemente, este é o mesmo corpo que criou o CRID. O nome da autoridade está presente no CRID no campo <authority> conforme explicado acima. O nome está presente na forma de um nome de domínio Internet registrado. É possível para um provedor de resolução (RP) ser encontrado na Internet usando o processo de resolução de nome de domínio especificado na especificação TV a Qualquer Tempo SP004.

Cada resolução requererá uma ou mais Gravações de Autoridade de Resolução (RAR) para existir no PDR para a resolução de localização ter lugar. Cada gravação de autoridade de resolução precisa ser colocada dentro de alguma espécie de recipiente específico de transporte que permita que o PDR saiba que esta é uma RAR. No caso de gravações múltiplas para a mesma autoridade, o PDR pode escolher usar exatamente uma delas, ou tentá-las todas por sua vez. A Gravação de Autoridade de Resolução (RAR) contém a informação que identifica os provedores de resolução onde a informação de resolução de referência de conteúdo pode ser encontrada.

Usando a RAR o PDR determina qual RP usar para resolver um CRID particular. O PDR então submete então uma requisição para uma localização acompanhada por um CRID, ao Provedor de Resolução em questão. Em resposta a esta requisição, o provedor de resolução retorna a informação do localizador (supondo que esta informação está disponível naquele RP, naturalmente). O PDR pode então acessar a fonte de conteúdo e obter o item de conteúdo. Um item de conteúdo pode ter mais de um localizador, por exemplo, se é radiofundido múltiplas vezes ou disponível de provedores múltiplos. O PDR pode então escolher qual localizador usar, ou orientar o usuário para fazer uma seleção.

Uma vez que a informação do localizador tenha sido obtida, o PDR aguarda a data e horário especificado e então grava o episódio conforme este é radiofundido no canal especificado. Naturalmente, se o localizador indica uma localização na Internet ou similar, o PDR pode simplesmente recuperar o conteúdo a partir da localização indicada, tão logo este se torne disponível.

Itens de conteúdo para os quais a informação de localizador está disponível, podem ser gravados pelo PDR no momento apropriado. Para esta finalidade, o PDR pode compreender armazenagem local tal como um

disco rígido suficientemente grande, e/ou um dispositivo tal como um gravador de DVD + RW. O meio de armazenagem no qual os itens de conteúdo são armazenados, não precisa ser local para o PDR, mas pode também ser um dispositivo externo tal como um disco rígido em um servidor de arquivo conectado ao PDR através de uma rede doméstica. Uma vez que os
5 itens de conteúdo tenham sido gravados, eles podem ser reproduzidos a qualquer instante, até que sejam apagados.

Se o PDR opera de acordo com um sistema de Gerenciamento de Direitos Digital, então um item de conteúdo pode ser apagado quando os
10 direitos associados ao item de conteúdo requerem tal apagamento. Também, alguns itens de conteúdo podem não vir com um direito a gravação do item como um todo, ou com um direito que permita visualizar somente por uma quantidade de tempo limitada, ou um número de vezes limitado. O PDR deveria então apagar o item de conteúdo quando o limite é excedido, ou
15 recusar acesso adicional ao conteúdo, até que direitos adicionais sejam obtidos, os quais permitam acesso adicional.

Fig. 2 ilustra esquematicamente uma primeira realização do PDR. Nesta realização, o PDR compreende um módulo de verificação de assinatura SIG VERIFIER, um módulo de resolução de CRID, RESOLVER,
20 e um módulo de recuperação de conteúdo RETRIEVER. Também está presente um meio de armazenagem local HD e um módulo opcional DRM para gerenciar direitos digitais associados a conteúdo recuperado pelo módulo RETRIEVER e armazenado no HD.

O módulo RESOLVER é responsável pelo processo de
25 resolução de localização conforme descrito acima. Dados um CRID e uma RAR o RESOLVER é arranjado para obter um localizador para o conteúdo identificado pelo CRID. O localizador é então fornecido ao módulo RETRIEVER que transfere ou caso contrário obtém um espécime do conteúdo. Este conteúdo pode ser armazenado no meio de armazenagem local HD.

Em uma primeira realização da invenção, assinaturas digitais são usadas para assinar o conteúdo do CRID. Somente os CRID adequadamente assinados serão aceitos pelo módulo SIG VERIFIER no PDR. Tais CRID podem ser acreditados para originar de uma autoridade fidedigna.

- 5 Isto não protege contra resolução incorreta do CRID. Se o módulo SIG VERIFIER verificou corretamente a assinatura, o PDR pode supor que o CRID é autêntico. Se a assinatura não é verificada como correta, o RESOLVER deveria recusar a obter um localizador para o conteúdo, usando o CRID. Isto poderia, por exemplo, ser implementado tendo o módulo SIG
- 10 VERIFIER recebido os CRID e passado para o RESOLVER, somente se a assinatura é verificada corretamente. Então, provedores de conteúdo e serviço podem estar certos de que os PDR obterão somente conteúdo usando CRID autênticos. Uma vantagem adicional deste aspecto é que isto permite que um PDR detecte um CRID mal formado ou corrompido, uma vez que tal CRID
- 15 teria também uma assinatura digital inválida.

- A assinatura de CRID individuais é feita preferivelmente sem mudar o formato do CRID. Ainda mais, a quantidade de informação é pequena, fazendo a proteção mais fraca. Um modo de adicionar assinaturas a CRID individuais é adicionando-os ao término do CRID. Deste modo,
- 20 assinatura seria parte da parte de dados do CRID e não prejudicará o comportamento normal.

- Como a quantidade de informação que pode ser adicionada a um CRID é limitada, somente o núcleo pode ser especificado. Ainda mais, devido ao tamanho do CRID, não é necessário fracionamento e a assinatura
- 25 pode ser calculada diretamente usando um algoritmo PKI.

De acordo com a presente invenção, o CRID é redefinido conforme segue. A sintaxe de um CRID assinado é:

CRID://<authority>/<data>&signatureAuthority>:<signature>

O significado dos elementos acima é conforme segue.

<authority> Usa as regras de nome de autoridade TV a Qualquer Tempo dadas na seção 7 do documento de especificação TV a Qualquer Tempo SP002, para assegurar unicidade.

5 <data> é uma cadeia de formato livre que é conforme o Identificador de Recurso Uniforme (URI) e é significativo para a autoridade dada pelo campo <authority>. A porção <data> do CRID é insensível ao caso.

10 <signatureAuthority> Usa as regras de nome de autoridade TV a Qualquer Tempo dadas na seção 7 do documento de especificação TV a Qualquer Tempo SP002, para assegurar unicidade. signatureAuthority indica a parte que definiu o algoritmo e maneira de calcular a assinatura.

 <signature> O valor de assinatura deste CRID calculado conforme definido pela signatureAuthority.

15 Mais de uma assinatura pode ser aplicada, reassinando o CRID assinado. Algumas ou todas as assinaturas prévias podem ser incluídas na competição de uma nova assinatura. Isto poderia ser indicado usando um outro campo adicional, por exemplo, separado por uma das outras cadeias (reservada). Alguns exemplos de CRID assinados são:

CRID://comp;com/3874y32&com.com:32843829174

CRID://broadcast.com/1.4.5&sign.com:7asd76ad7

20 Como uma variação deste método, é possível usar um tipo de URL diferente para representar um CRID assinado. Um exemplo desta variação é:

SCRID://comp.com/3874y32&comp.com:32843829174

25 Ordens diferentes e cadeias diferentes poderiam ser usadas para constituir o novo CRID assinado. Também, uma restrição poderia ser adicionada, a qual indicasse que marcadores não podem ser usados na parte de dados (“&” e “:”).

 Em uma outra realização da invenção, o provedor de resolução assina o localizador que é passado ao PDR. Este modo de localização do

conteúdo a ser recuperado pode ser acreditado, isto é, o PDR pode verificar que o localizador não foi mudado e que o localizador se origina de um certo provedor de resolução. Se a assinatura pode ser verificada em relação a algum certificado assinado pela autoridade CRID, o PDR pode também se assegurar

5 que a autoridade CRID confia no provedor de resolução. O localizador poderia também ser criptografado para habilitar um serviço pago similar aos dos CRID criptografados, conforme discutido abaixo.

Em uma outra realização da invenção, a RAR é assinada pelo provedor de resolução ou pelo provedor CRID. Isto protege o PDR, e daí o

10 usuário, contra RAR maliciosas. Se a RAR é assinada pela autoridade CRID, ou a assinatura do provedor de resolução pode ser autenticada pela autoridade CRID, então o PDR seria interrompido de encontrar provedores de resolução que não fossem acreditados pela autoridade CRID. A RAR poderia também ser criptografada para habilitar um serviço pago similar àquele dos CRID

15 criptografados, conforme discutido abaixo.

Como uma extensão opcional, o provedor do CRID ou RAR pode efetuar uma chave pública para um provedor de resolução particular disponível, preferivelmente provendo a chave pública com o CRID ou a RAR. Usando esta chave pública, o PDR pode verificar a resposta assinada por um

20 provedor de resolução. Deste modo, o PDR pode determinar que esta resposta (e o provedor de resolução) é aceitável para o provedor do CRID ou RAR. Preferivelmente, a chave pública é provido na forma de um certificado digital assinado pelo provedor do CRID ou RAR.

Fig. 3 ilustra esquematicamente uma segunda realização do

25 PDR. Nesta realização, o módulo SIG VERIFIER foi substituído por um módulo DECRYPTOR. Este módulo é arranjado para descriptografar um CRID, RAR ou localizador pelo menos parcialmente criptografados e passar o CRID, a RAR e o localizador descriptografados no RETRIEVER.

Em uma variante da realização, a parte <data> do CRID é pelo

menos parcialmente criptografada, como uma chave somente conhecido do provedor de resolução. Se há provedores de resolução múltiplos, chaves de criptografia múltiplos deveriam ser usados. Preferivelmente, a criptografia é efetuada usando criptografia assimétrica, embora criptografia simétrica seja também possível. Deste modo, somente provedores de resolução autorizados serão capazes de interpretar o <data> e efetuar resolução de conteúdo. Notar, entretanto, que a porção <data> de um CRID é essencialmente uma cadeia sem significado para o PDR. Criptografar uma cadeia sem significado apenas gera uma outra cadeia sem significado. Para resolução de localização de radiodifusão o PDR está simplesmente coincidindo a configuração do CRID com uma tabela de resolução que está sendo radiofundida. Para solução IP, uma parte <data> criptografada poderia ser usada, porém isto não impediria um resolvidor malicioso de mapear o CRID criptografado no conteúdo errado.

Para superar este problema, este é alertado para criptografar a parte de <data> de um criptografia diferentemente para instâncias diferentes no tempo e para usuários diferentes. Por exemplo, a parte cleartext<data> poderia ser estendida com preenchimento randômico que o receptor pode simplesmente filtrar. Isto torna difícil adivinhar os dados às claras com base no valor dos dados cifrados.

É também possível criptografar o CRID inteiro. Neste caso, a resolução de localização pode ser subsequente oferecida a usuários como um serviço pago. Neste caso, somente usuários que tenham subscrito o serviço de resolução de localização serão capazes de mapear o CRID na RAR e enviá-lo, (possivelmente às claras) a uma autoridade de resolução. Similarmente a RAR poderia ser criptografada ou mesmo o localizador da autoridade de resolução. Caso pague pelo serviço, os usuários utilizarão preferivelmente o provedor de resolução autorizado/pretendido.

Fig. 4 ilustra esquematicamente uma terceira realização do

PDR. Nesta realização, o módulo SIG VERIFIER foi substituído por um módulo RIGHTS EXTRACTOR.

5 O conteúdo recuperado por um usuário pode ser protegido. Proteção de conteúdo é usada tipicamente para guardar contra cópia não autorizada ou outro uso não autorizado do conteúdo. Se o conteúdo protegido é obtido, são requeridos chave criptográfica e/ou direitos para uso (visualização) do conteúdo, isto é, o usuário necessita acessar uma outra entidade, que é um servidor de autorização.

10 Nesta realização, o processo de resolução de localização e as etapas necessárias para prover os direitos e chaves para acesso, são combinados provendo um direito de acesso ao conteúdo juntamente com o CRID, a RAR e o localizador. Este direito é extraído pelo módulo RIGHTS EXTRACTOR e fornecido ao módulo DRM. Isto apresenta as seguintes vantagens:

15 - Nada mais é requerido para o usuário contatar também separadamente um servidor de direitos.

- Se o conteúdo é protegido, usuários são em qualquer caso requeridos a contatar uma autoridade de resolução autorizada, pois eles somente deste modo obtém os direitos corretos para usar o conteúdo.

20 O sistema de controle de acesso pode ser sofisticado, isto é, um sistema de Gerenciamento de Dados Digitais (DRM), mas poderia também ser muito simples, por exemplo, comparável a um sistema conforme descrito no Pedido de Patente Internacional WO 01/86387 (registro de procurador PHNL000264).

25 Esta realização é especialmente vantajosa quando o provedor de resolução é a mesma entidade que está provendo o conteúdo. Um exemplo de onde isto não funcionaria é quando, por exemplo, um radiodifusor de TV cria o CRID, um serviço de listagem de programa de TV de 3ª parte resolve o CRID, e um provedor de TV satélite provê o conteúdo através de seu serviço

satélite.

Em uma realização adicional, o processo de resolução de localização e um sistema DRM são integrados adicionalmente. O CRID nesta realização é também usado para obter informação para obter direitos usando o
5 processo de resolução de localização. Em seguida a localizar o conteúdo, o provedor de resolução será também capaz de resolver a localização de onde obter os direitos. Um RP pode até oferecer tal funcionalidade como um serviço ao usuário pois pode ser capaz de localizar os direitos mais baratos para aquela peça específica de conteúdo e passar a localização destes direitos
10 ao usuário. O usuário pode então contatar esta localização e adquirir os direitos.

Em uma outra realização, benefícios são englobados na parte de <data> de um CRID ou enviados juntamente com, ou nos RAR e localizadores. Com tais meios, os usuários podem ser estimulados a contatar
15 um provedor de resolução específico, pois o usuário pode receber benefícios, tais como um desconto para adquirir um filme. O benefício poderia também compreender créditos de alguma espécie, por exemplo, um número de Milhas Aéreas ou outros pontos para uso em um sistema de bônus. Os créditos poderiam também ser trocados por acesso a material de conteúdo adicional
20 relacionado ao conteúdo referenciado pelo CRID. Uma realização possível desta última opção é descrita no pedido de patente internacional PCT/IB02/03023 (registro de procurador PHNL010573) pelo mesmo requerente do presente pedido.

Outros tipos de modelos de negócios podem também ser
25 realizados usando esta solução. Oferecer um CRID específico com dados de benefício nele a um provedor de resolução, pode automaticamente resultar em um direito de usar o item de conteúdo conforme indicado pelo localizador, ou para obter o localizador. O mecanismo pode ser usado para estimular a visualização de um programa para ser capaz de assistir a um próximo

programa.

As medidas usadas nas realizações acima podem ser usadas individualmente, porém estas medidas poderiam também ser combinadas para prover melhor proteção ou para proteção contra ameaças múltiplas.

- 5 Deveria ser notado que as realizações acima mencionadas ilustram ao invés de limitar a invenção, e aqueles especialistas na técnica serão capazes de projetar muitas realizações alternativas sem se afastar do escopo das reivindicações anexas.

- 10 Nas reivindicações, quaisquer sinais de referência colocados entre parênteses não serão considerados como limitando a reivindicação. A palavra “compreendendo” não exclui a presença de elementos ou etapas diferentes daqueles listados em uma reivindicação. A palavra “um” precedendo um elemento não exclui a presença de diversos de tais elementos. A invenção pode ser implementada por meio de hardware compreendendo
15 diversos elementos distintos, e por meio de um computador adequadamente programado.

- 20 Na reivindicação de dispositivo enumerando diversos meios, diversos destes meios podem ser realizados por um e mesmo item de hardware. O mero fato de que certas medidas são descritas em reivindicações dependentes mutuamente diferentes, não indica que uma combinação destas medidas não possa ser usada com vantagem.

REIVINDICAÇÕES

1. Método para prover confiança verificável automaticamente em um processo de resolução de conteúdo, no qual um identificador de referência de conteúdo (CRID) identificando um item de conteúdo é resolvido usando uma gravação de autoridade de resolução (RAR) para obter um localizador identificando uma localização onde o item de conteúdo pode ser obtido, caracterizado pelo fato de compreender aplicar uma medida a pelo menos um dentre o CRID, a RAR e o localizador, para prover integridade e autenticação de origem.
2. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender prover uma assinatura digital para pelo menos uma porção de pelo menos um dentre o CRID, a RAR e o localizador.
3. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a assinatura digital é provida para pelo menos uma porção do localizador e pode ser verificada usando uma chave pública provida por um dentre um provedor CRID e um provedor RAR.
4. Método de acordo com a reivindicação 3, caracterizado pelo fato de compreender prover a chave pública com pelo menos um dentre o CRID e a RAR.
5. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender prover pelo menos uma porção de pelo menos um dentre o CRID, a RAR e o localizador de forma criptografada.
6. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender prover um direito de acesso ao conteúdo, juntamente com pelo menos um dentre o CRID, a RAR e o localizador.
7. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender prover informação sobre obtenção de um direito de acesso ao item de conteúdo, juntamente com pelo menos um dentre o CRID, a RAR e o localizador.

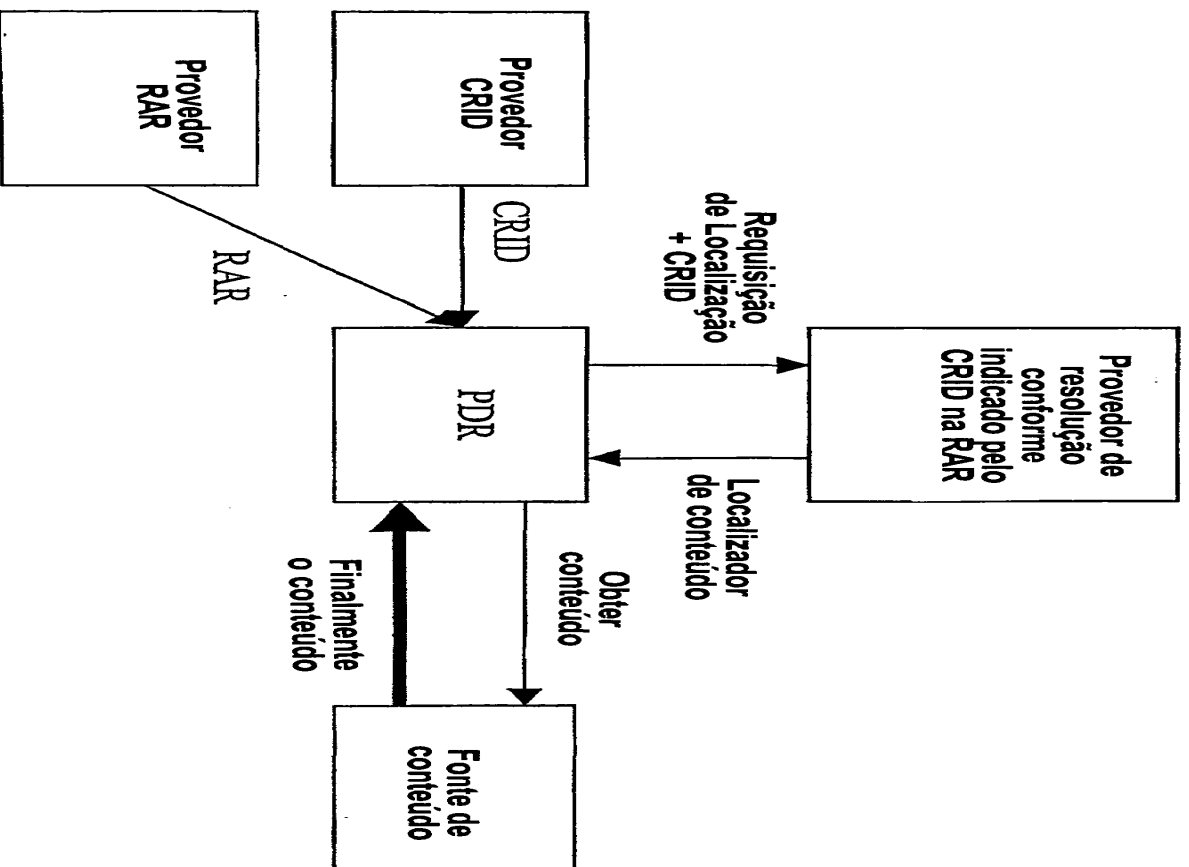


FIG.1

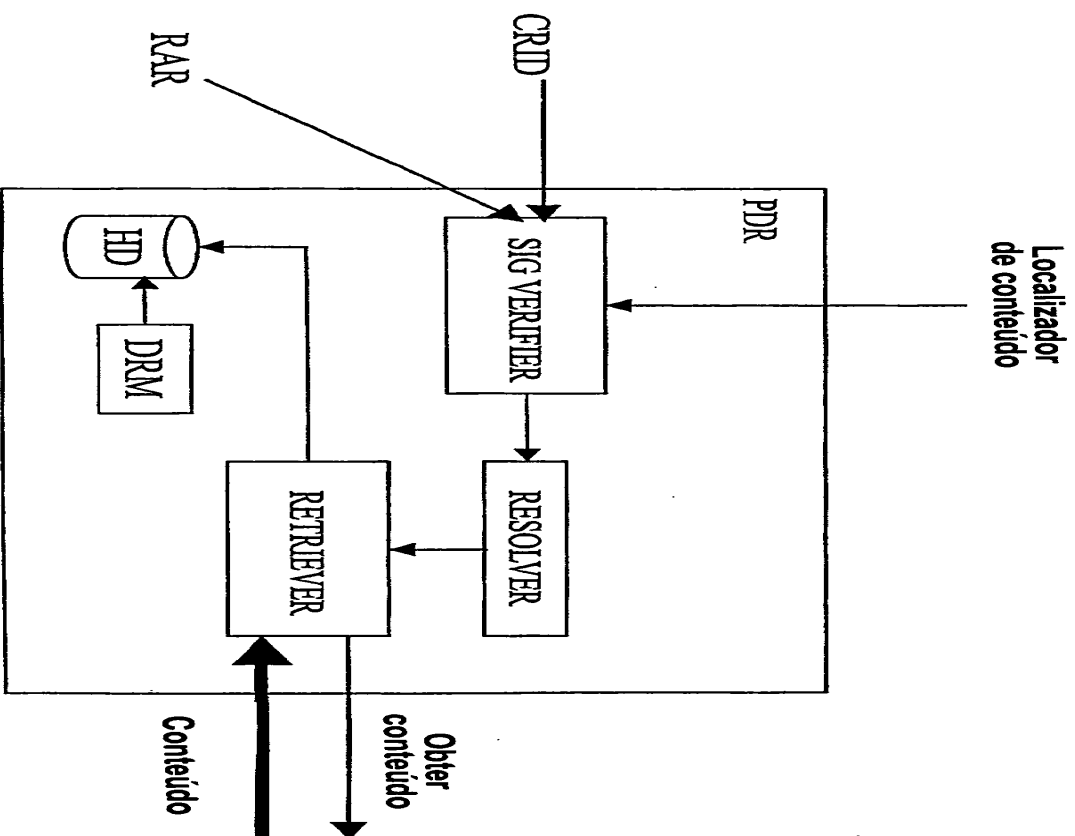


FIG.2

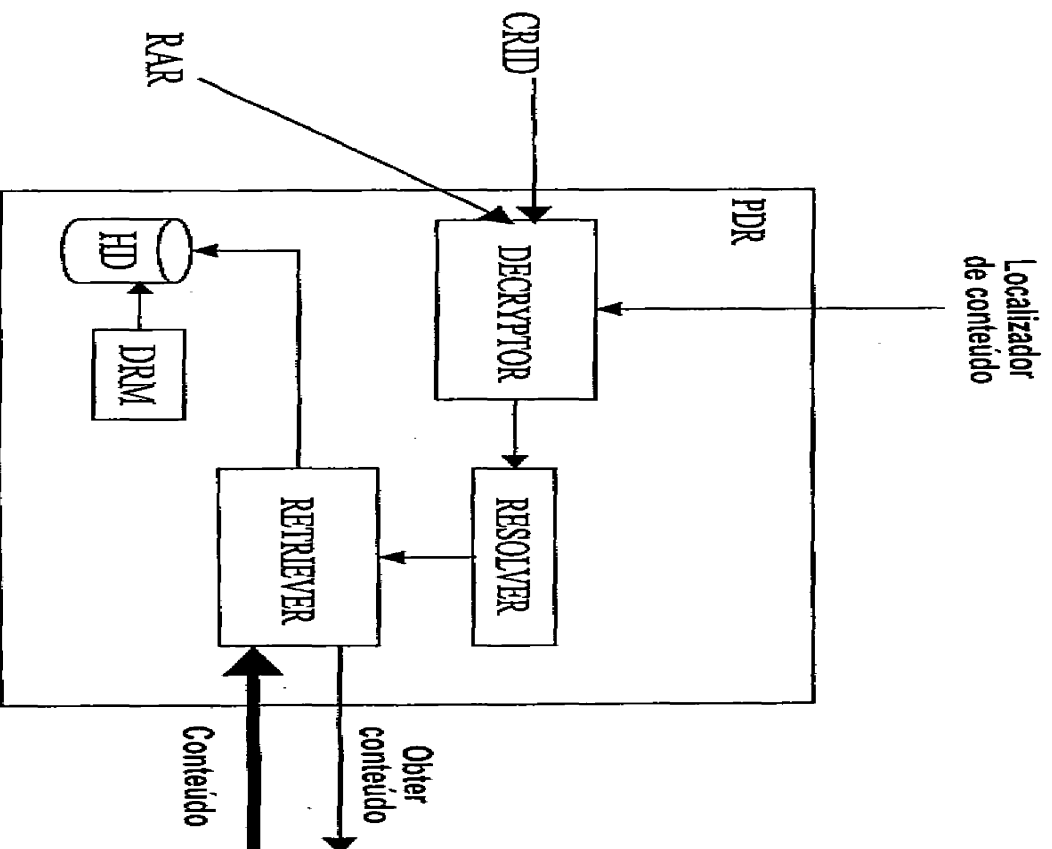


FIG.3

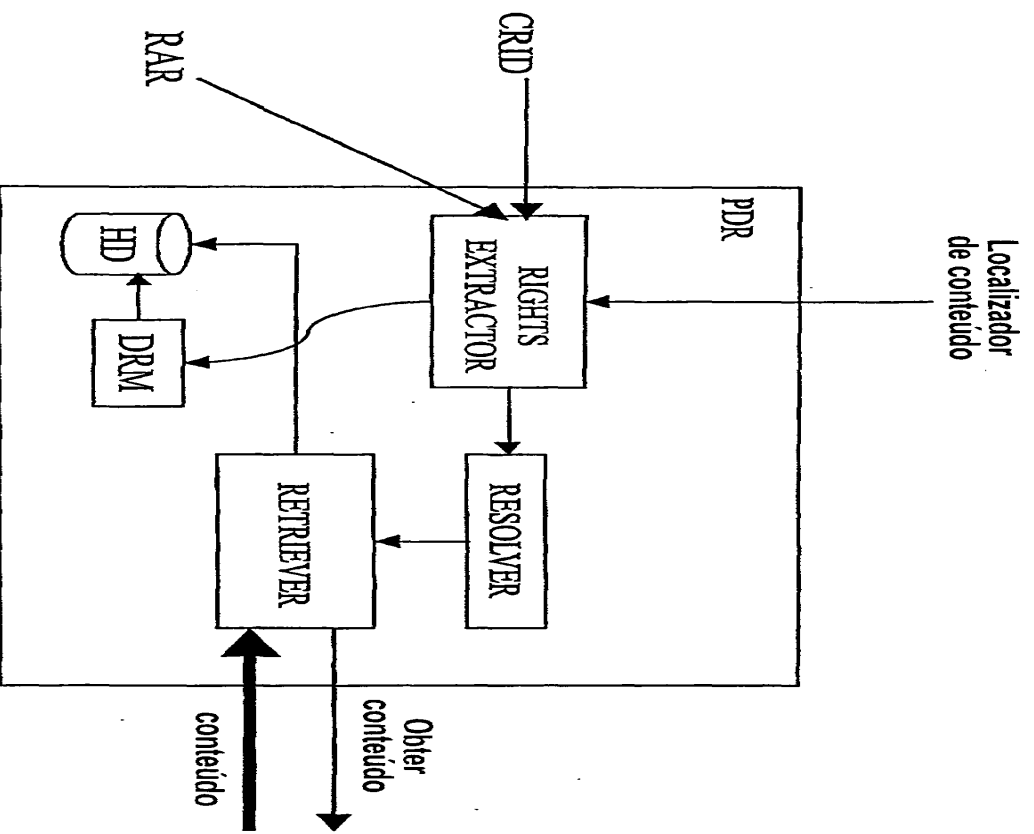


FIG. 4

RESUMO

“MÉTODO PARA PROVER CONFIANÇA VERIFICÁVEL AUTOMATICAMENTE EM UM PROCESSO DE RESOLUÇÃO DE CONTEÚDO, E, DISPOSITIVO (PDR)”

5 Um método de prover confiança verificável automaticamente em um processo de resolução de conteúdo, no qual um PDR resolve um identificador de referência de conteúdo (CRID) identificando um item de conteúdo usando uma gravação de autoridade de resolução (RAR) para obter um localizador identificando uma localização onde o PDR pode obter o item
10 de conteúdo. Preferivelmente, a medida compreende computar uma assinatura digital ao longo de pelo menos uma parte dos conteúdos do CRID, do localizador e/ou da RAR. O método pode também compreender criptografar pelo menos uma porção de dados do CRID, da RAR ou localizador. Direitos digitais necessários para acessar o item de conteúdo podem ser providos com
15 o CRID, a RAR e o localizador.