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

(21) **PI0706751-8 A2**

BRPI0706751A2

(22) Data de Depósito: 25/01/2007
(43) Data da Publicação: 05/04/2011
(RPI 2100)

(51) Int.Cl.:
H04L 9/00
G06F 17/00

(54) Título: **APARELHO E MÉTODO PARA MOVER OBJETO DE DIREITOS DIGITAIS A PARTIR DE UM DISPOSITIVO PARA OUTRO DISPOSITIVO POR INTERMÉDIO DE UM SERVIDOR**

(30) Prioridade Unionista: 26/01/2006 KR 10-2006-0008575, 25/08/2006 KR 10-2006-0081343, 30/03/2006 US 60/787,232, 27/07/2006 US 60/833,493, 26/01/2006 KR 10-2006-0008575, 25/08/2006 KR 10-2006-0081343, 27/07/2006 US 60/833,493, 26/01/2006 KR 10-2006-0008575, 30/03/2006 US 60/787,232

(73) Titular(es): LG ELETRONICS INC.

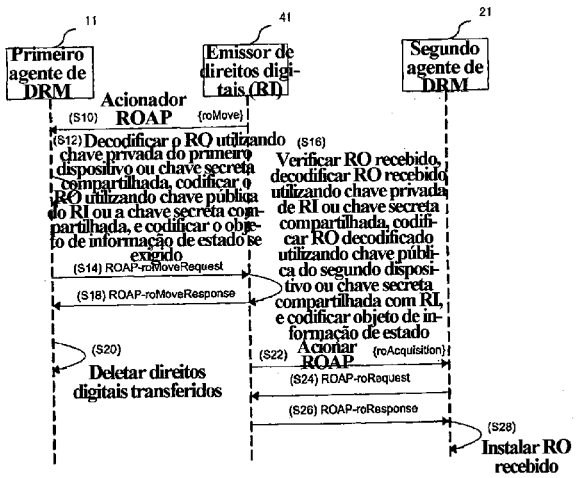
(72) Inventor(es): Kiran Kumar Keshavamurthy, Seung-Jae Lee, Sung-Mu Son, Te-Hyun Kim, Youn-Sung Chu

(74) Procurador(es): RICARDO PINHO

(86) Pedido Internacional: PCT KR2007000449 de 25/01/2007

(87) Publicação Internacional: WO 2007/086697de 02/08/2007

(57) Resumo: APARELHO E MÉTODO PARA MOVER OBJETO DE DIREITOS DIGITAIS A PARTIR DE UM DISPOSITIVO PARA OUTRO DISPOSITIVO POR INTERMÉDIO DE UMSERVIDOR Um aparelho e método para transferir um Objeto de Direitos digitais (RO) para um conteúdo entre dispositivos por intermédio de um servidor, em que um dispositivo remetente converter um primeiro RO aceito por ele próprio para codificação em um segundo RO, e envia uma mensagem de solicitação de movimento de RO incluindo o segundo RO para o servidor, visto que o servidor converte o segundo RO incluído na mensagem de solicitação de movimento de RO em um terceiro RO e transfere o terceiro RO para um dispositivo recebedor, pelo que o dispositivo recebedor recebe o terceiro RO a partir do servidor para instalação, em que o dispositivo remetente deleta ou modifica o primeiro RO em um momento apropriado.



APARELHO E MÉTODO PARA MOVER OBJETO DE DIREITOS DIGITAIS A PARTIR DE UM DISPOSITIVO PARA OUTRO DISPOSITIVO POR INTERMÉDIO DE UM SERVIDOR"

Campo Técnico

A presente invenção se refere a um aparelho e método para transferir (ou mover) um Objeto de direitos digitais (RO) entre dispositivos em um Gerenciamento de Direitos Digitais (DRM), e mais especificamente, a um aparelho e método para transferir um RO para um conteúdo digital a partir de um dispositivo para outro dispositivo por intermédio de um servidor.

Fundamentos da Técnica

Conteúdos digitais podem ser adquiridos através de todas as via disponíveis, por exemplo, mediante transferência a partir de um sítio da Rede de um Emissor de Conteúdo (CI) ou recebido por correio (por exemplo, correio eletrônico) ou quaisquer meios a partir de outro equipamento. Para utilizar os conteúdos digitais, um Objeto de Direitos digitais (RO) deve ser expedido por um emissor de Direitos Digitais (RI). Uma tecnologia relacionada a isso é referida como Gerenciamento de Direitos Digitais (DRM).

Um agente de DRM é geralmente um software ou programa instalado em um dispositivo que utiliza o conteúdo. Em vez dos CIs e provedores de RO, o agente de DRM impede o uso ilegal e a pirataria de conteúdo digital, e protege seus direitos autorais.

Dois tipos de ROs incluem um RU com informação de estado e um RO sem informação de estado. O RO com informação de estado é limitado pelas restrições tal como o número de vezes de utilização ou um tempo utilizado. Aqui, ao reproduzir um conteúdo digital correspondente, é necessário inspecionar e registrar quantos direitos digitais foram utilizados, a informação registrada sendo chamada de informação de estado. Portanto, a informação de estado é geralmente atualizada simultaneamente ao se reproduzir o conteúdo digital.

Revelação da Invenção

Problema Técnico

Tipicamente, para utilizar certo conteúdo digital no Sistema de DRM, um usuário de dispositivo deve ter diretamente um RO para o conteúdo emitido por um RI. Muitos métodos através dos quais um dispositivo acessa um RI para adquirir um RO expedido pelo RI foram introduzidos.

Contudo, ainda não foi proposto um método detalhado através do qual um dispositivo autenticado transfere (por exemplo, entrega, move, etc.) todo ou parte de seu próprio RO diretamente emitido por um RI para outro dispositivo.

Solução Técnica

Portanto, é um objetivo da presente invenção prover um aparelho e método para

mover (transferir) todo ou parte de um Objeto de Direitos digitais (RO) de um dispositivo específico para outro dispositivo por intermédio de um servidor.

Para alcançar esse objetivo da presente invenção, é provido um método para transferir um RO entre dispositivos por intermédio de um servidor compreendendo: converter, por intermédio de um dispositivo remetente, um primeiro RO para gerar um segundo RO; enviar uma mensagem de solicitação de movimento de RO a partir do dispositivo remetente para o servidor, para solicitar que o servidor transfira (ou mova) o segundo RO para um dispositivo recebedor por intermédio do servidor; receber uma mensagem de resposta a partir do servidor com relação à mensagem de solicitação de movimento de RO; e deletar o primeiro RO ou modificar a informação de estado do primeiro RO.

Em outra modalidade da presente invenção, um método para transferir um RO entre dispositivos por intermédio de um servidor compreendendo: receber uma mensagem de solicitação de movimento de RO a partir de um dispositivo de envio; enviar uma mensagem de resposta para o dispositivo remetente com relação à mensagem de solicitação de movimento de RO; converter o primeiro RO incluído na mensagem de solicitação de movimento de RO em um segundo RO; e transferir o segundo RO convertido para um dispositivo recebedor.

Para alcançar esse objetivo da presente invenção, é provido um dispositivo remetente para transferir um RO para um dispositivo recebedor por intermédio de um servidor que pode compreender: um agente de Gerenciamento de Direitos Digitais (DRM) o qual codifica um RO a ser movido para o dispositivo recebedor por intermédio do servidor e envia uma mensagem de solicitação de movimento de RO incluindo o RO codificado para o servidor; e um módulo de comunicação o qual se comunica pelo menos com o servidor.

Para alcançar esse objetivo da presente invenção, é provido um servidor para transferir um RO entre dispositivos que pode compreender: um emissor de Direitos Digitais (RI) o qual recebe a partir de um dispositivo remetente uma mensagem de solicitação de movimento de RO incluindo um RO a ser movido para um dispositivo recebedor; envia uma mensagem de resposta para o dispositivo remetente com relação à mensagem de solicitação de movimento de RO, converte o RO incluído na mensagem de solicitação de movimento de RO, e transfere o RO convertido para o dispositivo recebedor; e um módulo de comunicação o qual se comunica ao menos com o dispositivo remetente e com o dispositivo recebedor.

Para alcançar esse objetivo da presente invenção, é provido um sistema para transferir um RO entre dispositivos por intermédio de um servidor que compreende: um dispositivo remetente que envia uma mensagem de solicitação de movimento de RO incluindo um segundo RO convertido a partir de um primeiro RO; um servidor o qual converte um segundo RO incluído na mensagem de solicitação de movimento de RO em um terceiro RO e en-

via o terceiro RO convertido para um dispositivo recebedor; e o dispositivo recebedor o qual recebe o terceiro RO a partir do servidor e instala o terceiro RO.

Para alcançar esse objetivo da presente invenção, é provido um método para transferir um objeto de direitos digitais entre dispositivos por intermédio de um servidor compreendendo: enviar, por intermédio de um dispositivo remetente, uma mensagem de solicitação de movimento de objeto de direitos digitais incluindo um identificador de objeto de direitos digitais; verificando, por intermédio do servidor, um objeto de direitos digitais correspondendo ao identificador de objeto de direitos digitais; recebendo, por intermédio do dispositivo remetente, uma mensagem de resposta de movimento de objeto de direitos digitais a partir do servidor; e deletando, por intermédio do dispositivo remetente, o objeto de direitos digitais correspondendo ao identificador de objeto de direitos digitais ou modificando a informação de estado relacionada ao objeto de direitos digitais.

O método para transferir o objetivo de direitos digitais entre os dispositivos por intermédio do servidor pode compreender ainda: converter, por intermédio do servidor, o objeto de direitos digitais verificado em um objeto de direitos digitais para um dispositivo recebedor; e transferir, por intermédio do servidor, o objeto de direitos digitais convertido para o dispositivo recebedor.

A conversão do objeto de direitos digitais pode compreender: decodificar, pelo servidor, o objeto de direitos digitais verificados utilizando uma chave pública do servidor ou uma chave secreta previamente compartilhada com o dispositivo remetente; e codificar o objeto de direitos digitais decodificado utilizando uma chave pública do dispositivo recebedor ou uma chave secreta previamente compartilhada com o dispositivo recebedor.

Descrição Resumida dos Desenhos

Figura 1 ilustra uma modalidade de uma configuração de um sistema para mover um objeto de direitos digitais entre dispositivos por intermédio de um servidor de acordo com a presente invenção;

A Figura 2 ilustra uma modalidade de um método para mover um objeto de direitos digitais a partir de um dispositivo para outro dispositivo por intermédio de um servidor de acordo com a presente invenção;

A Figura 3 ilustra um texto exemplar descrevendo uma sintaxe de um acionador de movimento de RO de acordo com a presente invenção;

A Figura 4 ilustra os parâmetros de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção;

A Figura 5 ilustra uma sintaxe exemplar de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção;

A Figura 6 ilustra um fragmento de esquema de um parâmetro de extensão de identificador de redirecionamento incluído em uma mensagem de solicitação de movimento de

RO de acordo com a presente invenção;

A Figura 7 ilustra uma estrutura de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção;

A Figura 8 ilustra um texto exemplar indicando uma sintaxe de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção;

A Figura 9 ilustra um documento XML exemplar indicando permissão de movimento incluída em um RO.

Melhor Modo para Realização da Invenção

A presente invenção é implementada de tal modo que um primeiro dispositivo transfere ou move ("transfere" e "move" são usados como o mesmo significado em seguida) todo ou parte de um RO aceito pelo primeiro dispositivo para um segundo dispositivo por intermédio de um servidor.

Quando todo o RO do primeiro dispositivo é transferido para o segundo dispositivo por intermédio do servidor, o primeiro dispositivo não pode mais usar o RO e o segundo dispositivo pode usar o RO transferido para ele. Quando parte do RO do primeiro dispositivo é transferida para o segundo dispositivo por intermédio do servidor, por outro lado, o primeiro dispositivo pode usar o RO restante exceto a parte do RO transferida e o segundo dispositivo pode usar a parte do RO transferida para ele.

O RO transferido do primeiro dispositivo para o segundo dispositivo por intermédio do servidor pode ser aquele de um objeto de direitos digitais de dispositivo e um objeto de direitos digitais do domínio de usuário.

Se o servidor armazena, previamente, informação relacionada ao RO aceito pelo primeiro dispositivo (por exemplo, quando o servidor é um RI que inicialmente emitiu o RO para o primeiro dispositivo), o primeiro dispositivo e o servidor podem identificar o RO mutuamente com base em um identificador de RO. Aqui, o primeiro dispositivo transfere um identificador de RO e um objeto de informação de estado para o servidor, visto que o servidor codifica o RO correspondendo ao identificador de RO recebido e o objeto de informação de estado utilizando uma chave pública do segundo dispositivo ou uma chave secreta previamente compartilhada com o segundo dispositivo, para em seguida transferir para o segundo dispositivo.

O primeiro e o segundo dispositivos podem pertencer ao mesmo usuário ou a usuários diferentes entre si.

O servidor pode restringir a transferência de RO não permitido. O servidor é um provedor de conteúdo, o qual inclui um Emissor de Conteúdo (CI) e um Emissor de Direitos Digitais (RI).

O segundo dispositivo pode transferir o RO para outro dispositivo se o RO transferido tiver permissão de movimento.

O primeiro dispositivo envia para o servidor uma mensagem de solicitação de movimento de RO que inclui um segundo RO convertido a partir do primeiro RO aceito pelo próprio primeiro dispositivo. O servidor envia uma mensagem de resposta para o primeiro dispositivo com relação à mensagem de solicitação de movimento de RO. O servidor também converte o segundo RO incluído na mensagem de solicitação de movimento de RO em um terceiro RO e, então, transfere o terceiro RO convertido para o segundo dispositivo.

Na presente invenção, a informação de estado inclui valores cada um deles indicando um estado atual correspondendo a um RO. Aqui, quando o RO inclui qualquer uma das limitações de informação de estado (por exemplo, intervalo, contagem, contagem de tempo determinado acumulado, etc.), a informação de estado indica um valor gerenciado por um agente de DRM. O objeto de informação de estado indica uma instância de formato de informação de estado com o propósito de transferir a informação de estado de um dispositivo para outro dispositivo.

Modalidades da presente invenção serão descritas agora com referência aos desenhos anexos.

A Figura 1 ilustra uma modalidade de uma configuração de um sistema para mover um objeto de direitos digitais entre dispositivos por intermédio de um servidor de acordo com a presente invenção. Conforme ilustrado na Figura 1, um sistema de acordo com a presente invenção pode incluir um primeiro dispositivo 10 o qual envia uma mensagem de solicitação de movimento de RO que inclui um segundo RO convertido a partir de um primeiro RO, um servidor 40 que converte o segundo RO incluído na mensagem de solicitação de movimento de RO em um terceiro RO e envia o terceiro RO convertido para um segundo dispositivo 20, e o segundo dispositivo 20 o qual recebe o terceiro RO a partir do servidor 40 para instalação.

Ao receber a mensagem de solicitação de movimento de RO, o servidor 40 envia uma mensagem de resposta ao primeiro dispositivo com relação à mensagem de solicitação de movimento de RO.

O primeiro dispositivo 10 tem um primeiro agente de DRM 11 e o segundo dispositivo tem um segundo agente de DRM 21. O servidor 40 pode ser ou um provedor de conteúdo ou um RI. O provedor de conteúdo inclui um Emissor de Conteúdo (CI) e um Emissor de Direitos Digitais (RI).

O primeiro dispositivo 10 compreende ainda um módulo de comunicação o qual se comunica ao menos com o servidor e o segundo dispositivo 20 compreende ainda um módulo de comunicação o qual se comunica ao menos com o servidor. O servidor compreende ainda um módulo de comunicação o qual se comunica ao menos com o primeiro e segundo dispositivos 10 e 20.

O primeiro RO denota um RO expedido para o primeiro dispositivo 10 por intermé-

dio do servidor 40.

O segundo RO denota todo ou parte do primeiro RO ao mover (transferir) o primeiro RO para o segundo dispositivo 20 por intermédio do servidor 40.

O segundo RO denota um RO obtido por intermédio de decodificação, pelo primeiro dispositivo 10, o primeiro RO utilizando uma chave privada do primeiro dispositivo 10 ou uma chave secreta compartilhada com o servidor 40 (aqui, uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC do primeiro RO são decodificadas) e, então, codificando o primeiro RO decodificado utilizando uma chave pública do servidor 40 ou uma chave secreta compartilhada com o servidor 40.

O segundo RO inclui ao menos uma chave de criptografia de direitos digitais (REK) codificada (ou criptografada) mediante uso da chave pública do servidor 40 ou uma chave secreta compartilhada com o servidor 40. A chave MAC decodificada dentro do primeiro RO pode ser incluída no segundo RO.

O segundo RO pode ter permissões, restrições, um valor de assinatura digital, uma CEK, e uma REK, todos os quais são idênticos àqueles do primeiro RO.

Quando o primeiro RO é de informação de estado, o primeiro dispositivo 10 envia o segundo RO para o servidor 40 junto com o objeto de informação de estado.

O segundo RO inclui uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC as quais são envoltas e codificadas utilizando-se uma chave pública do servidor 40 de modo que o servidor 40 pode decodificar (ou decifrar) a chave REK e a chave MAC, e também inclui um valor MAC calculado utilizando a chave MAC decodificada no primeiro RO ou uma chave MAC recentemente gerada, de modo a permitir que o servidor 40 verifique o segundo RO.

O terceiro RO denota um RO obtido mediante decodificação, por intermédio do servidor 40, do segundo RO utilizando a chave privada do servidor 40 ou a chave secreta compartilhada com o primeiro dispositivo 10 e, então, codificando o segundo RO decodificado utilizando a chave pública do segundo dispositivo 20 ou uma chave secreta compartilhada com o segundo dispositivo 20.

O servidor 40 decodifica uma chave REK e uma chave MAC do segundo RO utilizando uma chave pública do servidor 40 ou a chave secreta compartilhada com o primeiro dispositivo 10.

O servidor 40 codifica a REK do segundo RO decodificada pelo servidor 40 utilizando uma chave pública do segundo dispositivo 20 ou a chave secreta compartilhada com o segundo dispositivo 20. O servidor 40 então modifica um valor de limitação de contagem de movimento (ou transferência) entre as restrições incluídas no segundo RO e gera um valor MAC utilizando a chave MAC decodificada no segundo RO ou uma chave MAC recentemente gerada, de modo a contestar o terceiro RO.

Se o primeiro dispositivo 10 transfere ambos, o segundo RO e o objeto de informação de estado, o servidor 40 converte o segundo RO no terceiro RO o qual é o estado incorporado do segundo RO a partir do objeto de informação de estado transferido.

Após o primeiro objeto 10 converter todo o primeiro RO no segundo RO e, então, transferir o segundo RO para o servidor 40, ao receber uma mensagem de resposta a partir do servidor 40 com relação à mensagem de solicitação de movimento de RO, o primeiro dispositivo 10 deleta o primeiro RO.

Após o primeiro dispositivo 10 converter parte do primeiro RO no segundo RO e, então, enviar o segundo RO convertido para o servidor 40, ao receber uma mensagem de resposta a partir do servidor 40 com relação à mensagem de solicitação de movimento de RO, o primeiro dispositivo 10 modifica (atualiza) a informação de estado no primeiro RO.

Na presente invenção, a primeira e a segunda modalidades descrevem a transferência (ou movimento, etc.) de todo o RO por intermédio do servidor e a transferência (ou movimento, etc.) de parte do RO por intermédio do servidor, respectivamente.

Em primeiro lugar, um método para transferir um RO a partir de um dispositivo para outro dispositivo por intermédio de um servidor é descrito esquematicamente de acordo com a primeira modalidade abaixo. A primeira modalidade ilustra uma transferência de todo o RO.

Um primeiro usuário do primeiro dispositivo 10 pesquisa um conteúdo específico (por exemplo, arquivo de música MP3, um arquivo de vídeo, etc.) a partir do servidor 40 (isto é, um provedor de conteúdo, particularmente um Emissor de Direitos Digitais (RI) 41) por intermédio do uso do primeiro dispositivo 10 (por exemplo, um entre telefones móveis e terminais de comunicação móvel) ou outro meio como um PC. Aqui, um RO gerado para o conteúdo específico pelo RI 41 pode incluir permissão de movimento.

Se o conteúdo específico é um arquivo de MP3, o primeiro usuário pretende dar o arquivo de MP3 para um segundo usuário como um presente.

Quando o RO gerado pelo RI 41 para o arquivo de MP3 contém a permissão de movimento, o primeiro usuário transfere ambos, o arquivo de MP3 e o RO para o mesmo.

Posteriormente, para transferir (mover) todo o RO o qual ainda não foi usado ou foi parcialmente usado, o primeiro usuário acessa o servidor 40 e transfere o RO para o arquivo de MP3 para o servidor 40.

O segundo dispositivo 20 (por exemplo, um aparelho de MP3 portátil) do segundo usuário se conecta ao servidor 40 do primeiro dispositivo 10 para transferir ambos, o arquivo de MP3 e o RO transferido para o servidor 40 por intermédio do primeiro usuário.

O segundo usuário pode conseqüentemente reproduzir o arquivo de MP3 utilizando seu segundo dispositivo 20, e o primeiro usuário não pode mais reproduzir o arquivo de MP3 utilizando o primeiro dispositivo 10.

Como tal, o primeiro dispositivo 10 pode transferir (mover) todos os RO aceitos por ele próprio para o segundo dispositivo 20 por intermédio do servidor 40.

Em seguida, um método para transmitir parte do RO a partir de um dispositivo para outro dispositivo por intermédio do servidor será descrito esquematicamente de acordo com a segunda modalidade da presente invenção. A segunda modalidade ilustra uma transferência de parte do RO.

O primeiro usuário pesquisa conteúdo utilizável (isto é, vídeos) a partir do servidor 40 utilizando o primeiro dispositivo 10.

O primeiro usuário seleciona um vídeo específico com instrução de que ele deseja reproduzir, dez vezes, o vídeo específico e compartilhar o mesmo.

O servidor 40 gera um RO para o vídeo selecionado, o RO tendo uma restrição de reprodução em 10 vezes e permissão para movimento.

O primeiro usuário então transfere ambos, o vídeo e o RO utilizando o primeiro dispositivo 10.

O primeiro usuário reproduz o vídeo uma vez utilizando o primeiro dispositivo 10.

Se o segundo dispositivo 20 desejar reproduzir o vídeo certo número de vezes, o primeiro usuário acessa o servidor 40 utilizando o primeiro dispositivo 10 e transfere parte do RO para o vídeo para o servidor 40.

Isto é, se o segundo dispositivo 20 pretende reproduzir o vídeo uma vez, o primeiro dispositivo transfere para o servidor 40 um RO para uma reprodução em uma vez a partir de todo o RO aceito por ele próprio.

O segundo usuário acessa o servidor 40 por intermédio do segundo dispositivo 20 e, então, transfere o vídeo e o RO transferido a partir do primeiro dispositivo 10 para o servidor 40 (aqui, o segundo usuário pode ser o mesmo usuário como o primeiro usuário ou um usuário diferente).

O segundo usuário pode conseqüentemente reproduzir o vídeo com base no RO para a reprodução de uma vez obtida por intermédio do segundo dispositivo 20.

Entretanto, o primeiro dispositivo 10 então tem o RO para reproduzir o vídeo oito vezes.

Em seguida, a primeira e a segunda modalidades serão descritas em mais detalhe com referência à Figura 2.

A Figura 2 ilustra um método exemplar para mover o objeto de direitos digitais a partir de um dispositivo para outro dispositivo por intermédio de um servidor de acordo com a primeira modalidade da presente invenção. A primeira modalidade será descrita com base em um fluxo de sinal mostrado na Figura 2. A segunda modalidade será descrita apenas mediante focalização na diferença a partir da primeira modalidade.

Um primeiro agente de DRM é provido no primeiro dispositivo 10, e um segundo

agente de DRM 21 é provido no segundo dispositivo 20. O RI 41 é provido no servidor 40. O primeiro usuário do primeiro dispositivo 10 pode ser o mesmo que o segundo usuário do segundo dispositivo 20 ou ser diferente dele. Além disso, um RO a ser transformado pode ser um RO de dispositivo ou um RO de domínio de usuário.

Com o propósito de explanação, um RO aceito pelo primeiro dispositivo 10 é referido como um primeiro RO, um RO a ser transferido a partir do primeiro dispositivo 10 para o servidor 40 é referido como um segundo RO, e um RO a ser transferido do servidor 40 para o segundo dispositivo 20 é referido como um terceiro RO.

O primeiro RO foi emitido para o primeiro agente de DRM 11 pelo RI 41. O primeiro RO pode ser um RO não utilizado ou RO restante após ser parcialmente usado.

Em seguida, é feita uma explanação para um caso onde o primeiro agente de DRM 11 transfere (move) todo ou parte do primeiro RO para o segundo agente de DRM 21.

Quando com a intenção de transferir um RO a partir de um agente de DRM para outro agente de DRM, isto é, ao transferir um RO por intermédio do RI, o RO deve ter uma assinatura digital gerada pelo RI. Portanto, enquanto solicitando um movimento (transferência) do segundo RO convertido a partir do primeiro RO, a assinatura digital pode prover o RI 41 com uma funcionalidade de integridade e uma funcionalidade de não-rejeição de modo a permitir que o RI 41 verifique se o RO foi emitido por ele próprio.

Em primeiro lugar, o primeiro usuário do primeiro agente de DRM 11 pesquisa um portal de RI e seleciona um serviço de movimento para mover (transferir) o RO para outro agente de DRM. O primeiro usuário então solicita um serviço a partir do RI 41, o serviço sendo para transferir o primeiro RO aceito por ele próprio para o segundo agente de DRM.

O RI 41 envia um acionador de ROAP (acionador de movimento de RO) para o primeiro agente de DRM para instruir o início de uma transferência de RO para o RI 41 (S10).

Se o primeiro agente de DRM 11 tiver conhecimento de um identificador de um agente de DRM alvo (por exemplo, o segundo agente de DRM 21), a etapa S10 pode não ser realizada. O identificador do segundo agente de DRM denota um ID do segundo dispositivo.

A partir do recebimento do acionador de ROAP ou de uma iniciação de usuário, o primeiro agente de DRM 11 gera um RO protegido (isto é, o segundo RO) para transferir para o RI 41.

Isto é, o primeiro agente de DRM 11 decodifica o RO expedido pelo RI 41 (isto é, o RO aceito pelo primeiro agente de DRM 11, a saber, o primeiro RO) utilizando uma chave privada do primeiro dispositivo ou uma chave secreta previamente compartilhada com o RI 41. Aqui, a Chave de Criptografia de Direitos Digitais (REK) e a chave MAC do primeiro RO são decodificadas.

O primeiro agente de DRM 11 gera outro RO protegido (isto é, o segundo RO). O outro RO protegido também pode incluir chave de criptografia de conteúdo (CEK), permis-

sões, restrições, e uma assinatura digital todas as quais são idênticas àquelas incluídas no RO aceito pelo primeiro dispositivo 10 (isto é, o primeiro RO).

Enquanto o RO protegido (isto é, o segundo RO) está sendo gerado, o primeiro agente de DRM 11 codifica o REK e a chave MAC utilizando uma chave pública ou o RI 41 ou uma chave secreta previamente compartilhada com o RI 41, de modo a permitir que o RI 41 leia a REK e a chave MAC. O primeiro agente de DRM 11 também gera um valor MAC a ser usado para verificação de integridade do segundo RO de modo a permitir que o RI 41 verifique a integridade do segundo RO.

Supondo que o primeiro RO é um RO com informação de estado, se o primeiro RO for completamente ou parcialmente transferido, o primeiro agente de DRM 11 gera um objeto de informação de estado a partir da informação de estado gerenciada (S12).

Após gerar o RO protegido (isto é, o segundo RO), o primeiro agente de DRM 11 gera uma mensagem de solicitação de movimento de RO (por exemplo, ROAP-roMoveRequest) e envia a mesma para o RI 41, a mensagem de solicitação de movimento de RO incluindo o RO gerado, o objeto de informação de estado (se o RO é o RO com informação de estado) e um identificador do segundo dispositivo (S14) e assinatura digital da mensagem. O identificador do segundo dispositivo pode não ser incluído. O primeiro usuário pode designar o identificador do segundo dispositivo posteriormente em um portal de RI. A mensagem de solicitação de movimento de RO denota uma mensagem para solicitar uma transferência (movimento) de um RO para outro agente de DRM, o qual será explicado em detalhe posteriormente.

Após completar de forma bem-sucedida uma autenticação incluindo uma verificação de status de revocação utilizando uma assinatura digital na solicitação de ROAP (por exemplo, ROAP-roMoveRequest) a mensagem enviada a partir do primeiro agente de DRM 11, o RI 41 gera um RO protegido destinado ao segundo agente de DRM (isto é, o terceiro RO) (S16).

Isto é, o RI 41 verifica o RO recebido (isto é, o segundo RO), e decodifica o RO recebido utilizando uma chave privada do RI 41 (ou uma chave secreta previamente compartilhada), de modo a gerar um RO (isto é, o terceiro RO) destinado ao segundo dispositivo 20.

Ao gerar o terceiro RO (isto é, o RO destinado ao segundo agente DRM), se recebendo o objeto de informação de estado, o RI 41 deve combinar o objeto de informação de estado recebido e informação de restrição e deve também modificar os valores de restrição incluídos no RO recebido a partir do primeiro dispositivo (dispositivo remetente) 10.

Além disso, se um elemento <move> incluído no segundo RO recebido tem uma restrição de contagem, o RI 41 deve diminuir o valor do elemento <count> tendo o elemento <move> por 1.

Após modificar os valores de restrição incluídos em um elemento <rights> no se-

gundo RO recebido, o RI 41 gera um valor de assinatura digital com relação ao elemento <rights>.

O RI 41 codifica uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC utilizando a chave pública de um dispositivo alvo (isto é, o segundo dispositivo 20) ou a chave secreta previamente compartilhada com o segundo dispositivo 20 e, então, anexa a REK codificada integrada e a chave MAC a um elemento <encKey> posicionado abaixo de um elemento <ro>.

O RI 41 gera um valor MAC para o elemento <ro> e anexa o valor MAC gerado a um elemento <mac> posicionado abaixo de um elemento <protected RO>. Desse modo, o RI 41 gera o RO para o segundo agente de DRM 21 (isto é, o terceiro RO ou o RO destinado ao segundo agente de DRM 21).

O RI 41 então envia uma mensagem de resposta de movimento de RO (por exemplo, ROAP-roMoveResponse) para o primeiro agente de DRM 11 em resposta à mensagem de solicitação de movimento de RO (por exemplo, ROAP-roMoveResponse) (S18). A mensagem de resposta de movimento de RO manifesta se o RI 41 garante que o segundo RO transferido será entregue de forma bem-sucedida. A mensagem de resposta de movimento de RO será explicada em detalhe posteriormente.

Após reconhecer que o RO foi transferido de forma bem-sucedida para o RI 41, o primeiro agente de DRM 11, o qual recebeu a mensagem de resposta de movimento de RO, deleta o RO correspondente (isto é, o primeiro RO) na primeira modalidade (isto é, para transferir o RO integralmente) (S20), enquanto modificando a informação de estado relacionada ao RO correspondente (isto é, o primeiro RO) na segunda modalidade (isto é, para transferir o RO parcialmente).

O RI 41, por outro lado, conduz um protocolo de aquisição de RO de 1-passagem ou 2-passagem (S22, S24 e S26). No caso do RO de 2-passagem, o RI 41 envia um acionador de ROAP para o segundo agente DRM 21 para instruir o segundo agente DRM 21 a transferir o RO transferido a partir do primeiro agente de DRM 11.

O segundo agente de DRM 21 transfere o RO enviado para o RI 41 pelo primeiro usuário do primeiro agente de DRM 11 após a conclusão bem-sucedida do procedimento de protocolo de aquisição com o RI 41. O segundo agente de DRM 21 conseqüentemente instala o RO transferido (S28).

Explanação detalhada será feita agora para o acionador de movimento de RO, mensagem de solicitação de movimento de RO e a mensagem de resposta de movimento de RO propostas na presente invenção.

O acionador de movimento de RO é descrito primeiro, abaixo.

O acionador de movimento de RO denota um acionador de ROAP enviado a partir do RI para o dispositivo remetente quando o dispositivo remetente deseja transferir (mover)

um RO para um dispositivo recebedor por intermédio do RI. O acionador de movimento de RO pode ser aquele das extensões de um acionador DRM ROAP.

O acionador de movimento de RO, conforme mostrado na etapa S10 da Figura 12, é enviado a partir do RI 41 para o primeiro agente de DRM 11 de modo a indicar o primeiro agente de DRM 11 para começar a transferir o RO para o RI 41.

A Figura 3 ilustra um texto exemplar descrevendo uma sintaxe de um acionador de movimento de RO de acordo com a presente invenção. As partes sublinhadas na Figura 3 indicam particularmente partes de texto estendido.

Quando o primeiro agente de DRM 11 recebe um acionador de ROAP o qual compreende um elemento <roapTrigger> tendo um elemento <roMove>, o primeiro agente de DRM 11 deve adquirir a permissão do primeiro usuário e iniciar um protocolo de solicitação de movimento ROAP-RO. Se o primeiro agente de DRM não tem um Contexto de RI para o <riID> especificado no acionador de movimento de RO recebido, o primeiro agente de DRM 11 deve iniciar um protocolo de registro alô do dispositivo ROAP utilizando um elemento <roapURL> no acionador de movimento de RO.

Quando o primeiro usuário seleciona um ou mais RO a serem transferidos, o RI 41 pode designar um elemento(s) <roID> no acionador de movimento de RO.

Após receber o elemento <roID> designado pelo RI 41 através do acionador de movimento de RO, o primeiro agente de DRM 11 deve incluir (adicionar) os ROs ou roIDs (identificadores de ROs) a serem transferidos na mensagem de solicitação de movimento ROAP-RO (isto é, ROAP-roMoveRequest).

Se o primeiro usuário que pretende transferir seu RO para outro dispositivo designa um dispositivo alvo, o RI 41 deve aplicar o elemento <targetDevice ID> no elemento <roap Trigger>. Portanto, o elemento <roap Trigger> incluído no acionador de movimento de RO pode ter o elemento <targetDevice ID>. O elemento <targetDevice ID> pode incluir um valor de ID do dispositivo (isto é, o valor alvo) para o qual o RO deve ser transferido.

A mensagem de solicitação de movimento de RO é descrita em seguida.

A mensagem de solicitação de movimento de RO (isto é, a mensagem de solicitação de movimento de ROAP-RO) é enviada a partir do dispositivo remetente para o RI 41 para iniciar um protocolo de movimento pelo RI. A mensagem indica que um RO deve ser transferido para um agente de DRM alvo por intermédio do RI. Com referência à Figura 2, a mensagem de solicitação de movimento de RO é enviada a partir do primeiro agente de DRM 11 para o RI 41 na etapa S14.

A Figura 4 ilustra os parâmetros de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção. Na Figura 4, M denota o componente obrigatório, e o é um componente opcional.

Um ID de dispositivo denota um dispositivo solicitante, isto é, um dispositivo reme-

tente. O ID de RI denota um ID de um servidor, isto é, o RI.

O número utilizável uma vez do acionador é o mesmo que um valor utilizável uma vez incluído no acionador de movimento de RO recebido a partir do RI 41. Ao especificar (definir) o parâmetro utilizável uma vez de acionador, o RI 41 pode armazenar um ID de um dispositivo alvo (isto é, o ID do segundo dispositivo) o qual o primeiro usuário designou durante pesquisa. Nesse caso, pode não ser exigido que o parâmetro ID do dispositivo alvo seja especificado (definido) na mensagem de solicitação de movimento de RO.

O número utilizável uma vez do dispositivo denota um número utilizável uma vez selecionado pelo dispositivo remetente (isto é, primeiro dispositivo).

O tempo de solicitação denota um tempo de DRM atual reconhecido pelo dispositivo remetente.

O ID de dispositivo alvo deve ser especificado se o acionador de movimento de RO recebido a partir do RI tem o <targetDevice ID>. O valor de ID de dispositivo alvo deve ser idêntico ao elemento <targetDevice ID> no acionador de movimento de RO. Se o parâmetro ID de dispositivo alvo não for especificado, o primeiro usuário deve designar o dispositivo alvo no portal de RI.

Os parâmetros ROInfo(s) denotam um ou mais ROs a serem movidos (transferidos). O mesmo deve conter um ou mais pares de ROID e objeto de informação de estado, ou um ou mais RO protegido e objeto de informação de estado.

Os conteúdos do RO protegido devem ser idênticos àqueles do RO que foi inicialmente recebido a partir do RI exceto pelo elemento <encKey> incluído no elemento <ro> do elemento <protected RO> e o elemento <mac> incluído no elemento <protected RO>.

O elemento <encKey> tem uma Chave de Criptografia de Direitos Digitais envolta (REK) e uma chave MAC. As duas chaves devem ser codificadas pelo primeiro dispositivo utilizando uma chave pública do RI ou a chave secreta previamente compartilhada com o RI, a chave pública tendo sido previamente compartilhada no processo de inter-certificação.

O elemento <mac> inclui um valor mac para o elemento <protected RO>. O valor mac deve ser calculado utilizando-se a chave MAC no elemento <encKey> ou calculado utilizando uma chave MAC recentemente gerada, e anexada no elemento <mac>.

Um parâmetro de objeto(s) de informação de estado deve ser incluído na mensagem de solicitação de movimento de RO quando o RO é um RO com informação de estado. O parâmetro de objeto(s) de informação de estado indica a informação de estado gerenciada pelo primeiro agente de DRM do primeiro dispositivo.

Ao transferir (mover) completamente um RO específico, o objeto de informação de estado é gerado a partir da informação de estado correspondendo a todo o RO específico. Inversamente, ao transferir parcialmente um RO específico, o objeto de informação de estado é gerado a partir da informação de estado correspondendo à parte do RO específico.

Um parâmetro de cadeia de certificado é incluído na mensagem de solicitação de movimento de RO se o contexto de RI não indicar que o RI armazenou sua informação de certificado de dispositivo exigida.

Um parâmetro de extensões pode incluir uma extensão de identificador de redirecionar. Quando a extensão de identificador de redirecionar existe em um campo de parâmetro de extensões, o parâmetro de extensões indica um ID de um dispositivo recebedor (por exemplo, segundo dispositivo) para receber um RO protegido. O ID pode ser um número telefônico definido pelos operadores celulares para cada dispositivo. Se a extensão de identificador de redirecionar não existe, isso indica implicitamente para o RI que o primeiro dispositivo está submetendo o RO não utilizado para um novo RO tendo o valor igual ou valor menor (aqui, o RO não utilizado corresponde ao parâmetro de RO protegido). Isto é, se a extensão de identificador de redirecionar não existe no campo de parâmetro de extensões da mensagem de solicitação de movimento de RO, o RI o qual recebeu a mensagem de solicitação de movimento de RO reconhece que o RO incluído na mensagem de solicitação de movimento de RO (isto é, o RO correspondendo ao campo de RO protegido) deve ser expedido mediante conversão em outro RO.

Um parâmetro de assinatura denota uma assinatura digital para a mensagem de solicitação de movimento de RO.

A Figura 5 ilustra uma sintaxe exemplar de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção. Na Figura 5, o elemento <roMoveRequest> define uma mensagem de solicitação de movimento de ROAP-RO e tem o tipo complexo "roap:ROMove Request". O tipo "roap:ROMove Request" estende a função básica "roap:Request type".

A Figura 6 ilustra um fragmento de esquema de um parâmetro de extensão de identificador de redirecionar incluído em uma mensagem de solicitação de movimento de RO de acordo com a presente invenção.

Uma mensagem de resposta de movimento de RO é descrita a seguir.

A mensagem de resposta de movimento de RO (isto é, ROAP-ROMove response) é enviada a partir do RI para o dispositivo remetente em resposta à mensagem de solicitação de movimento de RO (isto é, ROAP-ROMove request), a saber, uma mensagem enviada a partir do RI 41 para o primeiro agente de DRM 11 na etapa S18 da Figura 2. A mensagem de resposta de movimento de RO indica se o RI garante que o RI deve ser entregue de forma bem-sucedida (transferida).

A Figura 7 ilustra uma sintaxe exemplar de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção.

Um parâmetro de status denota um estado processado da mensagem de solicitação de movimento de RO pelo RI. O parâmetro de status tem um valor "sucesso", se o pro-

cessamento é bem-sucedido. Caso contrário, o RI seleciona uma das mensagens de status indicando erros.

O parâmetro ID de dispositivo denota um ID de um dispositivo recebendo a mensagem de resposta de movimento de RO. Esse parâmetro tem o mesmo valor que o valor do parâmetro ID de dispositivo incluído na mensagem de solicitação de movimento de RO (isto é, o valor do parâmetro ID de dispositivo da Figura 4).

Um parâmetro ID de RI denota um ID de um RI o qual envia a mensagem de resposta de movimento de RO. Um parâmetro de número utilizável uma vez de RI tem um número utilizável uma vez selecionado pelo RI.

O parâmetro ROURI denota um endereço (por exemplo, HTTP URL) para obter um RO destinado a um dispositivo alvo. Um dispositivo pode entregar o ROURI ao dispositivo alvo para permitir que o dispositivo alvo transfira o RO.

Um parâmetro de extensões é definido para a mensagem de resposta de movimento RO, porém, ele não é aqui usado.

Um parâmetro de assinatura denota uma assinatura digital para a mensagem de resposta de movimento de RO.

A Figura 8 ilustra um texto exemplar indicando uma sintaxe de uma mensagem de solicitação de movimento de RO de acordo com a presente invenção.

O elemento <roMoveResponse> define uma mensagem ROAP-ROMoveResponse

O elemento <roMoveResponse> tem um tipo complexo “roap:ROMoveResponse”. Esse tipo complexo estende o tipo básico “roap:Response”.

Em seguida, uma assinatura digital incluída em um RO emitido pelo RI é descrita.

Quando um RO deve ser transferido a partir de um agente de DRM para outro agente de DRM, o RI emite o RO tendo a assinatura digital independente do RO sendo transferido por intermédio do RI ou sendo transferido diretamente. Embora a solicitação de movimento de RO seja processada, a assinatura digital pode prover o RI com funcionalidade de não-rejeição para que o RI verifique se o RI foi emitido pelo próprio RI.

Com referência à Figura 2, embora o primeiro dispositivo 10 receba o RO emitido pelo RI 41 e instale o mesmo, se permissão de “mover” é definida no elemento <rights>, o primeiro agente de DRM 11 do primeiro dispositivo 10 deve armazenar o valor do elemento <signature> (aqui, o valor do elemento <signature> é gerado pelo RI se o RO incluir a permissão de movimento). O primeiro agente de DRM 11 deve ser capaz de criar o mesmo elemento <rights> como o elemento <rights> incluído no RO inicialmente emitido pelo RI 41.

Além disso, o primeiro agente de DRM 11 deve armazenar a REK e a chave MAC incluídas no RO inicialmente emitido.

A Figura 9 ilustra um documento XML exemplar indicando a permissão de “mover” incluída em um RO.

Um elemento <type> posicionado abaixo de um elemento <move> pode ter um valor(es) de "via RI" e/ou "diretamente". Se o valor do elemento <type> é "via RI", o primeiro agente de DRM 11 pode mover o RO por intermédio do RI 41. Se o valor do elemento <type> é "diretamente", o primeiro agente de DRM 11 pode mover o RO diretamente para outro agente de DRM (aqui, descrição detalhada da transferência direta de RO pode não ser considerada na presente invenção).

Um elemento <count> sob o elemento <constraint> indica o número de vezes para transferir o RO.

Se o valor do elemento <count> é "0", o primeiro agente de DRM 11 não deve enviar a mensagem de solicitação de movimento de RO com relação ao RO para o RI 41.

Processando as operações realizadas quando o primeiro agente de DRM 11 instala o RO a ser transferido, o RO inicialmente emitido pelo RI 41, pode ser igualmente aplicado quando o segundo agente de DRM 21 do segundo dispositivo 20 instala o RO recebido.

Em outra modalidade da presente invenção, será descrito um método para transferir um objeto de direitos digitais entre dispositivos por intermédio de um servidor. Em outra modalidade, um dispositivo remetente envia um identificador de RO diferente do próprio RO para o servidor para solicitar um movimento de RO. Isto é, a outra modalidade é diferente da primeira e da segunda modalidades descritas acima em que o dispositivo remetente envia para o servidor não o RO, mas sim o identificador de RO.

Com referência às Figuras 1 e 2, serão feitas descrições de um caso para transferir um RO do primeiro dispositivo 10 para o segundo dispositivo 20 por intermédio do servidor 40, isto é, o RI 41.

Se o RI 41 armazenou o RO do primeiro dispositivo 10, ambos, o primeiro dispositivo 10 e o RI 41 podem identificar o RO com base em um identificador de RO.

O primeiro dispositivo 10 envia uma mensagem de solicitação de movimento de RO incluindo um identificador de RO para identificar o RO para o RI 41 para solicitar que o RI 41 transfira seu RO para o segundo dispositivo 20. Aqui, a mensagem de solicitação de movimento de RO pode não incluir o parâmetro de RO(s) protegido mostrado na Figura 4 como componentes obrigatórios, porém, mais propriamente incluir o identificador de RO como o componente obrigatório.

O RI 41 então verifica o RO correspondendo ao identificador de RO incluído na mensagem de solicitação de movimento de RO, recebida. O RI 41 decodifica o RO verificado utilizando sua chave privada ou uma chave secreta previamente compartilhada com o primeiro dispositivo 10. Posteriormente, o RI 41 codifica o RO decodificado utilizando uma chave pública do segundo dispositivo 20 ou uma chave secreta previamente compartilhada com o segundo dispositivo 20.

Ao codificar o RO, o RI 41 diminui o número de vezes de transferência em 1 vez se

o RO decodificado tiver uma restrição de contagem de movimento. O RI 41 também codifica uma REK e uma chave MAC incluída no RO decodificado utilizando a chave pública do segundo dispositivo 20 ou a chave secreta previamente compartilhada com o segundo dispositivo 20. O RI 41 gera um valor MAC mediante cálculo da chave MAC ou de uma chave MAC recentemente gerada.

Se o RO é um RO com informação de estado, o RI 41 pode codificar um objeto de informação de estado.

Como tal, após gerar o RO a ser movido para o segundo dispositivo 20 ou durante a geração do RO, o RI 41 envia uma mensagem de resposta (por exemplo, uma mensagem de resposta de movimento de RO) para o primeiro dispositivo 10 em resposta à mensagem de solicitação de movimento de RO. Se a mensagem de resposta indica uma garantia de uma transferência bem-sucedida do RO, o primeiro dispositivo 10 deleta o RO para a transferência de um RO inteiro, e modifica a informação de estado relacionada ao RO para a transferência de um RO parcial.

O RI 41 transfere ambos, o RO codificado e o objeto de informação de estado (no caso do RO com informação de estado) para o segundo dispositivo 20. O segundo dispositivo 20 conseqüentemente recebe o RO para instalação.

Como descrito até aqui, como a presente invenção provê o método para transferir (mover) todo ou parte de um RO aceito por um dispositivo específico para outro dispositivo por intermédio de um servidor, o RO para um conteúdo específico emitido pelo servidor pode ser transferido para outro dispositivo por intermédio do servidor.

A presente invenção foi explicada com referência às modalidades que são apenas exemplares. Será evidente para aqueles versados na técnica que várias modificações e variações podem ser feitas na presente invenção sem se afastar do espírito ou escopo da invenção. Desse modo, pretende-se que a presente invenção cubra as modificações e variações dessa invenção desde que elas estejam abrangidas pelo escopo das reivindicações anexas e seus equivalentes.

REIVINDICAÇÕES

1. Método para transferir um objeto de direitos digitais entre dispositivos por intermédio de um servidor **CARACTERIZADO** por compreender:

converter, por intermédio de um dispositivo remetente, um primeiro objeto de direitos digitais para gerar um segundo objeto de direitos digitais;

enviar a partir do dispositivo remetente para o servidor uma mensagem de solicitação de movimento de objeto de direitos digitais para solicitar uma transferência do segundo objeto de direitos digitais para um dispositivo recebedor por intermédio do servidor;

receber uma mensagem de resposta a partir do servidor com relação à mensagem de solicitação de movimento de objeto de direitos digitais; e

deletar o objeto de direitos digitais ou modificar a informação de estado relacionada ao primeiro objeto de direitos digitais.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que gerar o segundo objeto de direitos digitais compreende:

decodificar o primeiro objeto de direitos digitais utilizando uma chave privada do dispositivo remetente; e

codificar o primeiro objeto de direitos digitais, decodificado, utilizando uma chave pública do servidor ou uma chave secreta compartilhada com o servidor.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que gerar o segundo objeto de direitos digitais compreende:

codificar, por intermédio do dispositivo remetente, uma Chave de Criptografia de Conteúdo (CEK) incluída no primeiro objeto de direitos digitais utilizando a chave pública do servidor ou a chave secreta compartilhada com o servidor;

incluir, como parâmetros, permissões, restrições e uma assinatura digital cada um dos quais é idêntico àquele do primeiro objeto de direitos digitais;

codificar uma Chave de Criptografia de Objeto de direitos digitais (REK) e uma chave MAC utilizando a chave pública do servidor ou a chave secreta compartilhada com o servidor; e

gerar um valor MAC mediante cálculo da chave MAC ou uma nova chave MAC.

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento de objeto de direitos digitais inclui, como parâmetros obrigatórios, um ID do dispositivo remetente, um ID de servidor, um número utilizável uma vez de dispositivo, um tempo de solicitação, o segundo objeto de direitos digitais a ser transformado e uma assinatura digital, e inclui, como parâmetros opcionais, um número utilizável uma vez de acionador, um ID do dispositivo recebedor, um objeto de informação de estado, uma cadeia de certificado, e um parâmetro de extensões.

5. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a

mensagem de resposta inclui, como parâmetros obrigatórios, um status de processamento da mensagem de solicitação de movimento do objeto de direitos digitais, um ID de um dispositivo para receber a mensagem de resposta, o ID de servidor, um número utilizável uma vez de servidor e uma assinatura digital para a mensagem de resposta, e inclui, como parâmetros opcionais, um parâmetro URI para adquirir um objeto de direitos digitais destinado ao dispositivo recebedor, e um parâmetro de extensões.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que se todo o primeiro objeto de direitos digitais é transferido para o dispositivo recebedor por intermédio do servidor, o dispositivo remetente deleta o primeiro objeto de direitos digitais.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que se parte do primeiro objeto de direitos digitais é transferida para o dispositivo recebedor por intermédio do servidor, o dispositivo remetente modifica a informação de estado relacionada ao primeiro objeto de direitos digitais.

8. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o primeiro e o segundo objetos de direitos digitais incluem um entre um objeto de direitos digitais de dispositivo e um objeto de direitos digitais de domínio de usuário.

9. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o primeiro e o segundo objetos de direitos digitais têm pelo menos restrição de movimento.

10. Método para transferir objeto de direitos digitais entre dispositivos por intermédio de um servidor **CARACTERIZADO** por compreender:

receber a partir de um dispositivo remetente uma mensagem de solicitação de movimento de objeto de direitos digitais;

enviar uma mensagem de resposta para o dispositivo remetente com relação à mensagem de solicitação de movimento de objeto de direitos digitais;

converter um primeiro objeto de direitos digitais incluído na mensagem de solicitação de movimento de objeto de direitos digitais para um segundo objeto de direitos digitais; e

transferir o segundo objeto de direitos digitais para um dispositivo recebedor.

11. Método, de acordo com a reivindicação 10, em que a conversão do primeiro objeto de direitos digitais em segundo objeto de direitos digitais compreende:

decodificar o primeiro objeto de direitos digitais utilizando uma chave privada do servidor ou uma chave secreta compartilhada com o dispositivo remetente; e

codificar o primeiro objeto de direitos digitais, decodificado utilizado uma chave pública do dispositivo recebedor ou uma chave secreta previamente compartilhada com o dispositivo recebedor.

12. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que a conversão do primeiro objeto de direitos digitais no segundo objeto de direitos digitais

compreende:

codificar, por intermédio do servidor, uma Chave de Criptografia de Conteúdo (CEK) incluída no primeiro objeto de direitos digitais utilizando uma chave pública do dispositivo recebedor ou uma chave secreta previamente compartilhada com o dispositivo recebedor;

modificar um valor de restrição de contagem de movimento incluído no primeiro objeto de direitos digitais;

gerar um valor de assinatura digital;

codificar uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC utilizando a chave pública do dispositivo recebedor ou a chave secreta previamente compartilhada com o dispositivo recebedor; e

gerar um valor MAC.

13. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento com objeto de direitos digitais inclui, como parâmetros obrigatórios, um ID do dispositivo remetente, um ID de servidor, um número utilizável uma vez de dispositivo, um tempo de solicitação, o primeiro objeto de direitos digitais a ser transferido e uma assinatura digital, e inclui, como parâmetros opcionais, um número utilizável uma vez de acionador, um ID do dispositivo recebedor, um objeto de informação de estado, uma cadeia de certificado, e um parâmetro de extensões.

14. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que a mensagem de resposta inclui, como parâmetros obrigatórios, um estado processado da mensagem de solicitação de movimento do objeto de direitos digitais, um ID de um dispositivo para receber a mensagem de resposta, o ID de servidor, um número utilizável uma vez de servidor e uma assinatura digital para a mensagem de resposta, e inclui, como parâmetros opcionais, um parâmetro URI para adquirir o terceiro objeto com assinatura digital, e um parâmetro de extensão.

15. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento de objeto de direitos digitais compreende pelo menos o primeiro objeto de direitos digitais, e em que o primeiro objeto de direitos digitais é convertido a partir de um objeto de direitos digitais emitido para o dispositivo remetente.

16. Método, de acordo com a reivindicação 15, **CARACTERIZADO** pelo fato de que o primeiro objeto de direitos digitais é convertido a partir do objeto de direitos digitais pelo dispositivo remetente ou pelo servidor.

17. Método, de acordo com a reivindicação 10, **CARACTERIZADO** por compreender ainda:

enviar um acionador ROAP para indicar ao dispositivo remetente para iniciar a transferência do objeto de direitos digitais para o servidor, para o dispositivo remetente.

18. Método, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o segundo objeto de direitos digitais é transferido a partir do servidor para o dispositivo recebedor e instalado no dispositivo recebedor.

19. Dispositivo remetente em um aparelho para transferir o objeto de direitos digitais entre dispositivos, **CARACTERIZADO** por compreender:

um agente de Gerenciamento de Direitos Digitais (DRM) o qual codifica um objeto de direitos digitais a ser transferido para um dispositivo recebedor por intermédio de um servidor e envia uma mensagem de solicitação de movimento de objeto de direitos digitais incluindo o objeto de direitos digitais, codificado para o servidor; e

um módulo de comunicação o qual se comunica com o servidor.

20. Dispositivo remetente, de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que o objeto de direitos digitais, codificado compreende uma Chave de Criptografia de Conteúdo (CEK) codificado utilizando uma chave pública do servidor ou uma chave secreta compartilhada com o servidor.

21. Dispositivo remetente, de acordo com a reivindicação 20, **CARACTERIZADO** pelo fato de que o objeto de direitos digitais codificado compreende permissões, restrições e uma assinatura digital cada uma das quais é idêntica àquela do objeto de direitos digitais possuído pelo agente de DRM.

22. Dispositivo remetente, de acordo com a reivindicação 21, **CARACTERIZADO** pelo fato de que o objeto de direitos digitais, codificado, compreende uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC cada uma delas codificada utilizando uma chave pública no servidor ou uma chave secreta previamente compartilhada com o servidor.

23. Dispositivo remetente, de acordo com a reivindicação 22, **CARACTERIZADO** pelo fato de que o objeto de direitos digitais, codificado compreende um valor MAC gerado mediante cálculo da chave MAC ou de uma nova chave MAC.

24. Dispositivo remetente, de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento de objeto de direitos digitais é uma mensagem para solicitar ao servidor que transfira o objeto de direitos digitais para o dispositivo recebedor por intermédio do servidor.

25. Dispositivo remetente, de acordo com a reivindicação 19, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento de objeto de direitos digitais inclui, como parâmetros obrigatórios, um ID do dispositivo remetente, um ID de servidor, um número utilizável uma vez de dispositivo, um tempo de solicitação, o segundo objeto de direitos digitais a ser transferido e uma assinatura digital, e inclui, como parâmetros opcionais, um número utilizável uma vez de acionador, um ID do dispositivo recebedor, um objeto de informação de estado, uma cadeia de certificado, e um parâmetro de extensões.

26. Servidor em um aparelho para transferir um objeto de direitos digitais entre dispositivos **CARACTERIZADO** por compreender:

um emissor de direitos digitais (RI) o qual recebe a partir de um dispositivo remetente uma mensagem de solicitação de movimento de objetos de direitos digitais incluindo um objeto de direitos digitais a ser transferido para um dispositivo recebedor, envia uma mensagem de resposta para o dispositivo remetente com relação à mensagem de solicitação de movimento de objeto de direitos digitais, converte o objeto de direitos digitais incluído na mensagem de solicitação de movimento de objeto de direitos digitais, e transfere o objeto de direitos digitais, convertido para o dispositivo recebedor; e

um módulo de comunicação o qual se comunica com o dispositivo remetente e o dispositivo recebedor.

27. Servidor, de acordo com a reivindicação 26, **CARACTERIZADO** pelo fato de que o emissor de direitos digitais decodifica o objeto de direitos digitais incluído na mensagem de solicitação de movimento de objetos de direitos digitais utilizando uma chave privada que o emissor de direitos digitais possui ou uma chave secreta previamente compartilhada com o dispositivo remetente ou uma chave secreta compartilhada, e codifica o objeto de direitos digitais, decodificado utilizando a chave pública do dispositivo recebedor ou uma chave secreta previamente compartilhada com o dispositivo recebedor.

28. Servidor, de acordo com a reivindicação 26, **CARACTERIZADO** pelo fato de que o emissor de direitos digitais modifica um valor de restrição de contagem de movimento quando o objeto de direitos digitais incluído na mensagem de solicitação de movimento de objeto de direitos digitais tem a limitação de contagem de movimento.

29. Servidor, de acordo com a reivindicação 26, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento de objeto de direitos digitais inclui, como parâmetros obrigatórios, um ID do dispositivo remetente, um ID do emissor de direitos digitais, um número utilizável uma vez de dispositivo, um tempo de solicitação, o objeto de direitos digitais a ser transferido e uma assinatura digital, e inclui, como parâmetros opcionais, um número a ser utilizado uma vez de acionador, um ID do dispositivo recebedor, um objeto de informação de estado, uma cadeia de certificado, e um parâmetro de extensões.

30. Servidor, de acordo com a reivindicação 26, **CARACTERIZADO** pelo fato de que a mensagem de resposta inclui, como parâmetros obrigatórios, um estado processado da mensagem de solicitação de movimento de objeto de direitos digitais, um ID de um dispositivo para receber a mensagem de resposta, o ID de servidor, um número utilizável uma vez de servidor e uma assinatura digital para a mensagem de resposta, e inclui, como parâmetros opcionais, um parâmetro URI de objeto de direitos digitais para adquirir o objeto de direitos digitais, e um parâmetro de extensões.

31. Sistema para transferir um objeto de direitos digitais entre dispositivos por in-

termédio de servidor **CARACTERIZADO** por compreender:

um dispositivo remetente que envia uma mensagem de solicitação de movimento de objeto de direitos digitais incluindo um segundo objeto de direitos digitais convertido a partir de um primeiro objeto de direitos digitais;

um servidor que converte o segundo objeto de direitos digitais incluído na mensagem de solicitação de movimento de objeto de direitos digitais em um terceiro objeto de direitos digitais e transfere o terceiro objeto de direitos digitais para um dispositivo recebedor; e

um dispositivo recebedor que recebe o terceiro objeto de direitos digitais a partir do servidor e instala o terceiro objeto de direitos digitais.

32. Sistema, de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que o segundo objeto de direitos digitais inclui uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC cada uma delas codificada utilizando uma chave pública do servidor ou uma chave secreta previamente compartilhada entre o servidor e o dispositivo remetente.

33. Sistema, de acordo com a reivindicação 31, **CARACTERIZADO** pelo fato de que o terceiro objeto de direitos digitais inclui uma Chave de Criptografia de Direitos Digitais (REK) e uma chave MAC cada uma delas codificada utilizando uma chave pública do dispositivo recebedor ou uma chave secreta previamente compartilhada entre o servidor e o dispositivo recebedor.

34. Método para transferir um objeto de direitos digitais entre dispositivos por intermédio de um servidor **CARACTERIZADO** por compreender:

enviar, por intermédio de um dispositivo remetente, uma mensagem de solicitação de movimento de objeto de direitos digitais incluindo um identificador de objeto de direitos digitais;

verificar, por intermédio do servidor, um objeto de direitos digitais correspondendo ao identificador de objeto de direitos digitais;

receber, por intermédio do dispositivo remetente, uma mensagem de resposta de movimento de objeto de direitos digitais a partir do servidor; e

deletar, por intermédio do dispositivo remetente, o objeto de direitos digitais correspondendo ao identificador de objeto de direitos digitais ou modificar a informação de estado relacionada ao objeto de direitos digitais.

35. Método, de acordo com a reivindicação 34, **CARACTERIZADO** por compreender ainda:

converter, por intermédio do servidor, o objeto de direitos digitais, verificado em um objeto de direitos digitais para um dispositivo recebedor; e

transferir, por intermédio do servidor, o objeto de direitos digitais convertido para o

dispositivo recebedor.

36. Método, de acordo com a reivindicação 35, **CARACTERIZADO** pelo fato de que a conversão do objeto de direitos digitais compreende:

decodificar, por intermédio do servidor, o objeto de direitos digitais, verificado utilizando uma chave pública do servidor ou uma chave secreta previamente compartilhada com o dispositivo remetente; e

codificar o objeto de direitos digitais decodificado utilizando uma chave pública do dispositivo recebedor ou uma chave secreta previamente compartilhada com o dispositivo recebedor.

37. Método, de acordo com a reivindicação 34, **CARACTERIZADO** pelo fato de que a mensagem de solicitação de movimento de objeto de direitos digitais inclui, como parâmetros obrigatórios, um ID do dispositivo remetente, um ID de servidor, um número utilizável uma vez de dispositivos, um tempo de solicitação, um identificador de objeto de direitos digitais e uma assinatura digital, e inclui, como parâmetros opcionais, um número utilizável uma vez de acionador, um ID do dispositivo recebedor, um objeto de informação de estado, uma cadeia de certificado, e um parâmetro de extensões.

38. Método, de acordo com a reivindicação 34, **CARACTERIZADO** pelo fato de que a mensagem de resposta de objeto de direitos digitais inclui, como parâmetros obrigatórios, um estado processado da mensagem de solicitação de movimento de objeto de direitos digitais, um ID de um dispositivo para receber a mensagem de resposta, o ID de servidor, um número utilizável uma vez de servidor e uma assinatura digital para a mensagem de resposta, e inclui, como parâmetros opcionais, um parâmetro URI para adquirir um objeto de direitos digitais destinado ao dispositivo recebedor, e um parâmetro de extensão.

39. Método, de acordo com a reivindicação 34, **CARACTERIZADO** pelo fato de que quando todo o objeto de direitos digitais é transferido para o dispositivo recebedor por intermédio do servidor, o dispositivo remetente deleta o objeto de direitos digitais.

40. Método, de acordo com a reivindicação 34, **CARACTERIZADO** pelo fato de que quando uma parte do objeto co direitos digitais é transferida para o dispositivo recebedor por intermédio do servidor, o dispositivo remetente modifica a informação de estado relacionada ao objeto de direitos digitais.

41. Método, de acordo com a reivindicação 34, **CARACTERIZADO** pelo fato de que o objeto de direitos digitais inclui um de um objeto de direitos digitais de dispositivo e um objeto de direitos digitais de domínio.

42. Método, de acordo com a reivindicação 34, **CARACTERIZADO** pelo fato de que o objeto de direitos digitais tem pelo menos restrição de movimento.

Fig. 1

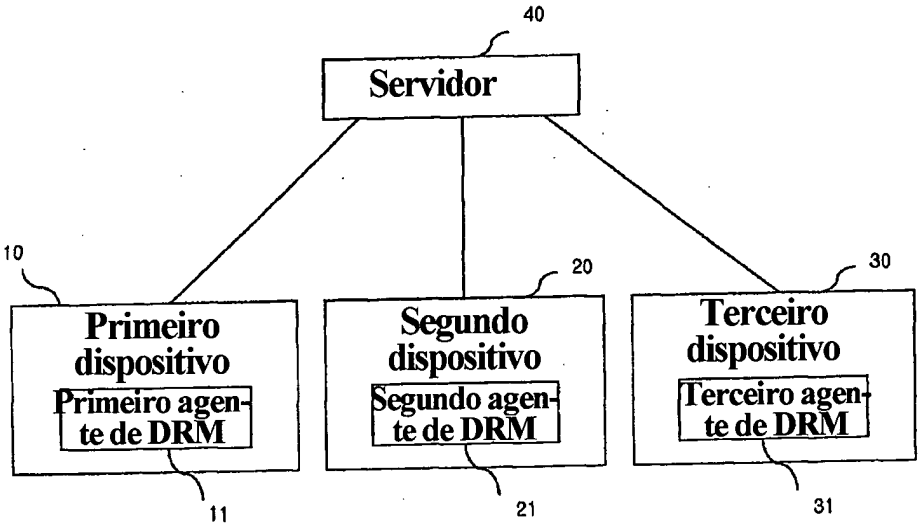

40
Servidor
10
20
30
Primeiro dispositivo
Primeiro agente de DRM
Segundo dispositivo
Segundo agente de DRM
Terceiro dispositivo
Terceiro agente de DRM
11
21
31

Fig. 2

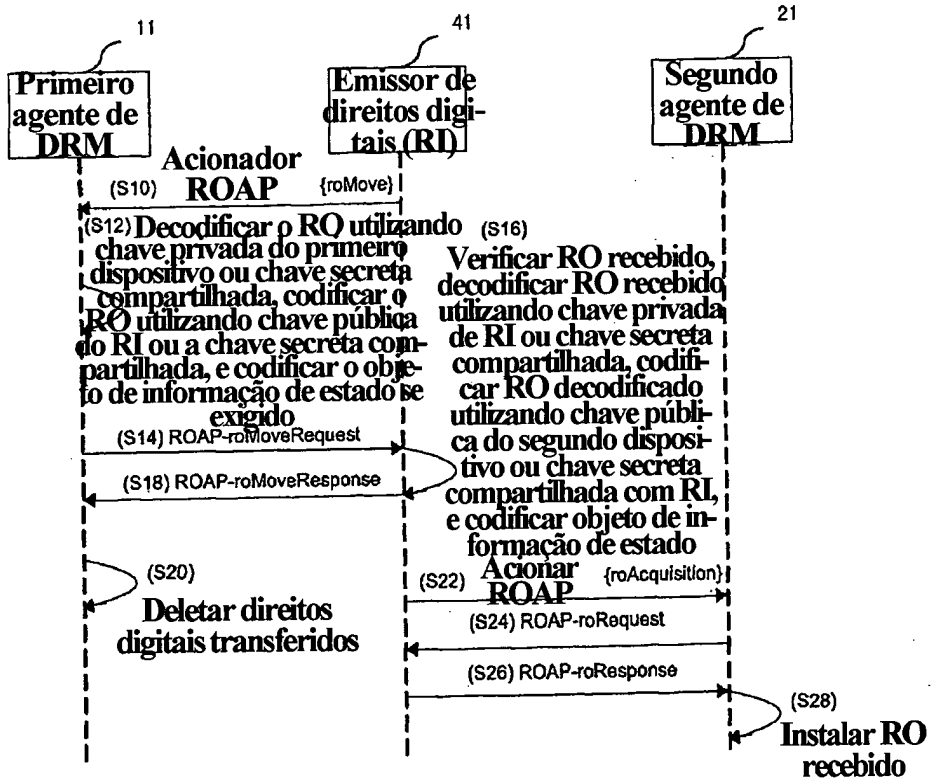

11
41
21
Primeiro agente de DRM
Emissor de direitos digitais (RI)
Segundo agente de DRM
Acionador ROAP
(S10)
{roMove}
(S12) Decodificar o RO utilizando chave privada do primeiro dispositivo ou chave secreta compartilhada, codificar o RO utilizando chave pública do RI ou a chave secreta compartilhada, e codificar o objeto de informação de estado se exigido
(S16) Verificar RO recebido, decodificar RO recebido utilizando chave privada de RI ou chave secreta compartilhada, codificar RO decodificado utilizando chave pública do segundo dispositivo ou chave secreta compartilhada com RI, e codificar objeto de informação de estado
(S14) ROAP-roMoveRequest
(S18) ROAP-roMoveResponse
(S20)
Deletar direitos digitais transferidos
(S22) Acionar ROAP
{roAcquisition}
(S24) ROAP-roRequest
(S26) ROAP-roResponse
(S28)
Instalar RO recebido

Fig. 3

```
<complexType name="ROMoveTrigger">
 <sequence>
  <element name="riID" type="roap:Identifier"/>
 <element name="riAlias" type="string" minOccurs="0"/>
  <element name="nonce" type="roap:Nonce" minOccurs="0"/>
  <element name="roID" type="roap:Identifier" minOccurs="0" maxOccurs="unbounded"/>
  <element name="roapURL" type="anyURI"/>
<element name="targetDeviceID" type="roap:Identifier" minOccurs="0"/>
<attribute name="id" type="ID"/>
<attribute name="ROrequested" type="boolean" default="true" />
</complexType>
<!— ROAP trigger —>
<element name="roapTrigger" type="roap:RoapTrigger"/>
<complexType name="RoapTrigger">
 <annotation>
  <documentation xml:lang="en">
  Mensagem utilizada para acionar o dispositivo para iniciar um protocolo de
  </documentation>    aquisição de objeto de direitos digitais
 </annotation>
 <sequence>
  <choice>
   <element name="registrationRequest" type="roap:RegistrationRequestTrigger"/>
   <element name="roAcquisition" type="roap:ROAcquisitionTrigger"/>
   <element name="joinDomain" type="roap:DomainTrigger"/>
   <element name="leaveDomain" type="roap:DomainTrigger"/>
   <element name="roMove" type="roap:ROMoveTrigger"/>
  </choice>
  <element name="signature" type="ds:SignatureType" minOccurs="0"/>
  <element name="encKey" type="xenc:EncryptedKeyType" minOccurs="0"/>
 </sequence>
 <attribute name="version" type="roap:Version"/>
 <attribute name="proxy" type="boolean"/>
 </complexType>
```

Fig. 4

Parâmetro	Solicitação de movimento de ROAP-RO
ID de dispositivo	M
ID de RI	M
Número utilizável uma vez de acionador	O
Número utilizável uma vez de dispositivo	M
Tempo de solicitação	M
ID de dispositivo alvo	O
ROinfo	M
Cadeia de certificado	O
Extensões	O
Assinatura	M

Fig. 5

```
<!--ROMoveRequest -->
<element name="roMoveRequest" type="roap:ROMoveRequest" />
<complexType name="ROMoveRequest">
 <annotation>
  <documentation xml:lang="en">
   Message sent from Device to RI to request submit RO.
  </documentation>
 </annotation>
 <complexContent>
  <extension base="roap:Request">
   <sequence>
    <element name="deviceID" type="roap:Identifier" />
    <element name="riID" type="roap:Identifier" />
    <element name="nonce" type="roap:Nonce" />
    <element name="targetDeviceID" type="roap:Identifier" />
    <element name="ROInfo" maxOccurs="unbounded">
     <complexType>
      <sequence>
       <choice>
        <sequence>
         <element name="protectedRO" type="roap:ProtectedRO" form="qualified" />
         <element name="StateInformationObject" type="o-ex:constraintType"
          minOccurs="0" maxOccurs="unbounded" />
        </sequence>
        <sequence>
         <element name="roID" type="ID" />
         <element name="signature" type="ds:SignatureType" />
         <element name="StateInformationObject" type="o-ex:constraintType"
          minOccurs="0" maxOccurs="unbounded" />
        </sequence>
       </choice>
      </sequence>
     </complexType>
    </element>
    <element name="certificateChain" type="roap:CertificateChain" minOccurs="0" />
    <element name="extensions" type="roap:Extensions" minOccurs="0" />
    <element name="signature" type="base64Binary" />
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

Fig. 6

```
<!— Used In ROAP-ROMoveRequest message —>
<complexType name="RedirectIdentifier">
 <complexContent>
  <extension base="roap:Extension"/>
    <sequence minOccurs="0">
     <element name="id" type="string"/>
          <minLength value="12"/>
    </sequence>
  </extension>
 </complexContent>
</complexType>
```

Fig. 7

Parâmetro	Resposta de movimento de ROAP-ROM	
	Status = Sucesso	Status ≠ Sucesso
	M	M
ID de dispositivo	M	-
ID de RI	M	-
Número utilizável uma vez de RI	M	-
ROURI	O	-
Extensões	O	-
Assinatura	M	-

Fig. 8

```
<!--ROMoveResponse -->
<element name="roMoveResponse" type="roap:ROMoveResponse"/>
<complexType name="ROMoveResponse">
<annotation>
  <documentation xml:lang="en">
Mensagem enviada a partir do RI para dispositivo
  </documentation>      em resposta a um ROSubmit.
 </annotation>
 <complexContent>
  <extension base="roap:Response">
   <sequence minOccurs="0">
    <element name="deviceID" type="roap:Identifier"/>
    <element name="riID" type="roap:Identifier"/>
    <element name="nonce" type="roap:Nonce" minOccurs="0"/>
    <element name="signature" type="base64Binary"/>
    <element name="extensions" type="roap:Extensions"/>
   </sequence>
  </extension>
 </complexContent>
</complexType>
```

Fig. 9

```
<permission>
...
<move partial="true">
 <type>viaRI</type>
 <type>directly</type>
<constraint>
<count>5</count>
</constraint>
</move>
</permission>
```

RESUMO

"APARELHO E MÉTODO PARA MOVER OBJETO DE DIREITOS DIGITAIS A PARTIR DE UM DISPOSITIVO PARA OUTRO DISPOSITIVO POR INTERMÉDIO DE UM SERVIDOR"

Um aparelho e método para transferir um Objeto de Direitos digitais (RO) para um conteúdo entre dispositivos por intermédio de um servidor, em que um dispositivo remetente converter um primeiro RO aceito por ele próprio para codificação em um segundo RO, e envia uma mensagem de solicitação de movimento de RO incluindo o segundo RO para o servidor, visto que o servidor converte o segundo RO incluído na mensagem de solicitação de movimento de RO em um terceiro RO e transfere o terceiro RO para um dispositivo recebedor, pelo que o dispositivo recebedor recebe o terceiro RO a partir do servidor para instalação, em que o dispositivo remetente deleta ou modifica o primeiro RO em um momento apropriado.