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

(21) **PI 0712543-7 A2**

BRPI0712543A2

(22) Data de Depósito: 24/03/2007
(43) Data da Publicação: 26/12/2012
(RPI 2190)

(51) Int.Cl.:
H04K 1/00

(54) Título: MÉTODO E APARELHO PARA EFETUAR O RETORNO DE UM OBJETO DE GERÊNCIA DE DIREITOS

(30) Prioridade Unionista: 07/06/2006 US 11/448.492

(73) Titular(es): Motorola, INC

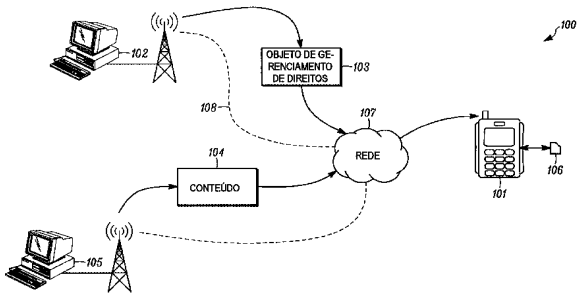
(72) Inventor(es): Douglas T. Michau, Hosane H. Abu-Amara, James Hu, Joon Young Park

(74) Procurador(es): Orlando de Souza

(86) Pedido Internacional: PCT US2007064864 de 24/03/2007

(87) Publicação Internacional: WO 2007/143252de 13/12/2007

(57) Resumo: METODO E APARELHO PARA EFETUAR A DEVOLUÇAO DE UM OBJETO DE GERENCIAMENTO DE DIREITOS. Um sistema e um método para devolução de um objeto de gerenciamento de direitos (103) para um emissor de direitos (102) são providos, o sistema e o método permitem que O emissor de direitos (102) se assegure que o objeto de gerenciamento de direitos (103) seja removido de um dispositivo eletrônico (101) antes da feitura do reembolso, enquanto se provê ao consumidor a capacidade de recuperação o objeto de gerenciamento de direitos (103) , quando a devolução for mal sucedida. Após a iniciação de uma devolução, um dispositivo eletrônico (101) transmite estruturas de dados probabilisticos (226, 228) para O emissor de direitos (102) . As estruturas de dados probabilísticos (226, 228) têm índices ali de objetos de gerenciamento de direitos dispostos dentro do dispositivo eletrônico (101). O dispositivo eletrônico (101) encripta O objeto de gerenciamento de direitos (103), envia-o para O emissor de direitos (102) , e o remove do dispositivo eletrônico (101) . Ao consultar as estruturas de dados probabilísticos (226, 228), as quais podem ser filtros de Bloom, o emissor de direitos (102) é capaz de confirmar que o objeto de gerenciamento de direitos (103) foi apagado do dispositivo eletrônico (101).



MÉTODO E APARELHO PARA EFETUAR A DEVOLUÇÃO DE UM OBJETO DE GERENCIAMENTO DE DIREITOS

CAMPO TÉCNICO

Esta invenção se refere geralmente ao gerenciamento de direitos digitais em dispositivos eletrônicos e, mais especificamente, a um método e a um aparelho para se garantir com segurança a devolução de um objeto de gerenciamento de direitos a um emissor de direitos.

TÉCNICA ANTECEDENTE

Os dispositivos eletrônicos estão se tornando cada vez mais um lugar comum na sociedade. Enquanto no passado era novidade ver alguém falando em um telefone móvel, hoje em dia muitas pessoas portam múltiplos dispositivos eletrônicos em todos os lugares a que vão. Por exemplo, um estudante pode portar um telefone móvel, um computador laptop, um assistente digital pessoal (PDA), um tocador de música portátil quando indo para a aula. De modo similar, um homem de negócios pode levar um computador portátil, um dispositivo habilitado para e-mail sem fio, um telefone móvel e um equipamento de radiochamada para e do trabalho. Da mesma forma, uma criança pode levar um tocador de música portátil, um tocador de vídeo ou um dispositivo de jogos para o parque para brincar.

Com melhoramentos na tecnologia destes dispositivos e nas redes às quais eles se conectam, cada vez mais dispositivos estão sendo projetados para a acomodação de conteúdo transferível (via download). Por exemplo, no campo de música, houve uma época em que uma pessoa tinha que ir a uma loja de discos para comprar um disco, uma fita ou um disco compacto para ouvir música em um tocador de música

portátil. Com os novos tocadores de MP3, alguns equipados com conexões sem fio com a Internet, hoje em dia alguém simplesmente transfere (via download) uma música à escolha, a qual é adequada para tocar instantaneamente. Além do conteúdo de música, um conteúdo de imagem, um conteúdo de vídeo, conteúdo de jogos, um conteúdo de software e outros aplicativos agora estão disponíveis para transferência (via download) eletrônica para dispositivos eletrônicos.

Uma tensão com este acesso fácil a um conteúdo é quanto aos direitos de propriedade intelectual. Quando uma pessoa para a um distribuidor de música por uma música transferida (via download), o artista, o editor e o distribuidor gostariam de garantir que as proteções de direito autoral associadas permanecessem com efeito. Embora o comprador da música seja livre para desfrutar a música, os detentores de direitos autorais precisam de uma forma para evitarem uma cópia não autorizada da mídia digital protegida. Com o advento de computadores e outros dispositivos eletrônicos portáteis, freqüentemente é simples copiar, modificar ou redistribuir trabalhos protegidos sem autorização.

O gerenciamento de direitos digitais é um termo que descreve amplamente as novas tecnologias pelas quais provedores de conteúdo fazem cumprir limitações quanto ao uso e à distribuição de conteúdo. Há muitos aspectos de gerenciamento de direitos digitais, incluindo autenticação de conteúdo, autorização para uso de conteúdo, contabilidade por royalties e pagamentos, verificação de direitos, cumprimento de direitos e proteção de conteúdo.

Houve várias tentativas de gerenciamento de direitos

digitais em dispositivos eletrônicos. Um método é encriptação simples. Com uma encriptação simples, um arquivo encriptado é transferido para um usuário. O arquivo pode ser transferido (via download), mas não pode ser executado ou aberto até uma senha ser provida. Uma vez que o pagamento, as condições e outros termos de uso tenham sido satisfeitos, um provedor de conteúdo provê ao usuário uma senha. O usuário emprega a senha para abrir o arquivo. O problema com a encriptação é que, embora proteja o arquivo durante a entrega, ela não provê um mecanismo de prevenção de redistribuição não autorizada, uma vez que o arquivo tenha sido aberto.

Uma outra abordagem é pelo uso de um "objeto de gerenciamento de direitos". Em gerenciamento de direitos digitais usando objetos de gerenciamento de direitos, dois arquivos são transferidos a partir do provedor de conteúdo para um usuário: um arquivo de conteúdo encriptado e um objeto de gerenciamento de direitos. O objeto de gerenciamento de direitos é requerido para uso do arquivo de conteúdo encriptado. Um objeto de gerenciamento de direitos pode incluir uma chave de encriptação capaz de desencriptar ou destravar o arquivo de conteúdo. Embora o arquivo de conteúdo encriptado possa ser livremente copiado ou redistribuído, o objeto de gerenciamento de direitos inclui limitações de uso. Por exemplo, o objeto de gerenciamento de direitos pode permitir apenas que o arquivo de conteúdo seja aberto um certo número de vezes ou em um certo número de dispositivos.

O problema com o gerenciamento de direitos digitais baseado em objeto de gerenciamento de direitos ocorre com

uma verificação de transferência. Embora seja fácil verificar que um arquivo transferido tenha sido recebido, o destinatário não tem uma forma de determinar se existem ainda cópias no dispositivo do transferidor. A título de exemplo, considere música digital. Uma pessoa pode comprar uma música para transferência (via download), e, por sua vez, pode receber um arquivo de conteúdo e um objeto de gerenciamento de direitos. O objeto de gerenciamento de direitos pode especificar que a pessoa pode ouvir a música até vinte vezes. Contudo, após uma única tocada, a pessoa pode perceber que transferiu (via download) a música errada. Alternativamente, a pessoa pode não gostar da música. Aquela pessoa gostaria de ser capaz de devolver a música por um reembolso parcial. Contudo, ao devolver o recibo do arquivo de conteúdo e o objeto de gerenciamento de direitos, o provedor de conteúdo não tem uma forma de saber se uma cópia do objeto de gerenciamento de direitos permanece de posse do comprador. O provedor de conteúdo pode ser relutante em prover um reembolso, se a pessoa ainda tiver a capacidade de ouvir a música.

Assim, há uma necessidade de um método e um aparelho para se efetuar a devolução de um objeto de gerenciamento de direitos para um emissor de direitos enquanto se verifica se os direitos digitais realmente foram removidos do dispositivo de devolução.

BREVE DESCRIÇÃO DOS DESENHOS

As figuras associadas, em que números de referência iguais se referem a elementos idênticos ou funcionalmente similares por todas as vistas separadas e as quais em conjunto com a descrição detalhada abaixo são incorporadas

em e fazem parte do relatório descritivo, servem para ilustração adicional de várias modalidades e para explicação de vários princípios e vantagens, tudo de acordo com a presente invenção.

A FIG. 1 ilustra um ambiente de exemplo adequado para uma modalidade de método e de aparelho de acordo com a invenção.

A FIG. 2 ilustra um método de devolução de objeto de gerenciamento de direitos de acordo com a invenção.

A FIG. 3 ilustra uma modalidade de um aparelho capaz de devolução de um objeto de gerenciamento de direitos de acordo com a invenção.

A FIG. 4 ilustra um fluxograma de uma modalidade de um método de devolução de um objeto de gerenciamento de direitos, conforme visto a partir da perspectiva do dispositivo de devolução de acordo com a invenção.

A FIG. 5 ilustra um método de tentativa de devolução de um objeto de gerenciamento de direitos de acordo com a invenção.

A FIG. 6 ilustra um fluxograma de uma modalidade de um método de tentativa de devolução de um objeto de gerenciamento de direitos, onde pelo menos uma tentativa de devolução de objeto de gerenciamento de direitos é mal sucedida.

A FIG. 7 ilustra um fluxograma de uma modalidade de um método de devolução de um objeto de gerenciamento de direitos, conforme visto da perspectiva do emissor de direitos de acordo com a invenção.

Técnicos versados apreciarão que elementos nas figuras são ilustrados por simplicidade e clareza e não

necessariamente foram desenhados em escala. Por exemplo, as dimensões de alguns dos elementos nas figuras podem ser exageradas em relação a outros elementos, para ajudarem a melhorar o entendimento de modalidades da presente invenção.

DESCRIÇÃO DETALHADA DA INVENÇÃO

Antes da descrição em detalhes de modalidades que estão de acordo com a presente invenção, deve ser observado que as modalidades residem primariamente em combinações de etapas de método e componentes de aparelho relacionados à devolução ou à transferência de outra forma de um objeto de gerenciamento de direitos de acordo com a invenção. Assim sendo, os componentes de aparelho e as etapas de método foram representados, quando apropriado, por símbolos convencionais nos desenhos, mostrando apenas aqueles detalhes específicos que sejam pertinentes para o entendimento das modalidades da presente invenção, de modo a não se obscurecer a exposição com detalhes que prontamente sejam evidentes para aqueles de conhecimento comum na técnica tendo o benefício da descrição aqui.

Será apreciado que modalidades da invenção descritas aqui podem ser compreendidas por um ou mais processadores convencionais e instruções de programa armazenadas únicas que controlam um ou mais processadores para implementação, em conjunto com certos circuitos não de processador, de algumas, da maioria ou de todas as funções de devolução ou transferência de objetos de gerenciamento de direitos, conforme descrito aqui. Os circuitos não de processador podem incluir, mas não estão limitados a um transceptor ou um transmissor, acionadores de sinal, circuitos de relógio,

circuitos de fonte de potência, e dispositivos de entrada de usuário. Como tal, estas funções podem ser interpretadas como etapas de um método para a realização das operações de devolução de um objeto de gerenciamento de direitos. Alternativamente, algumas ou todas as funções poderiam ser implementadas pela execução de um código de software, por uma máquina de estado que não tenha instruções de programa armazenadas, ou por um ou mais circuitos integrados específicos de aplicação, em que cada função ou algumas combinações de certas funções são implementadas como uma lógica personalizada. Ainda, é esperado que alguém de conhecimento comum na técnica, não obstante possivelmente com esforço significativo e motivado por muitas escolhas de projeto, por exemplo, tempo disponível, tecnologia atual e considerações econômicas, quando guiado pelos conceitos e princípios mostrados aqui prontamente seja capaz de gerar tais instruções de software, programas ou circuitos com uma experimentação mínima.

As modalidades da invenção são descritas, agora, em detalhes. Com referência aos desenhos, números iguais designam partes iguais por todas as vistas. Conforme usado na descrição aqui e por todas as reivindicações, os termos a seguir assumem significados explicitamente associados aqui, a menos que o contexto claramente dite de outra forma: o significado de "um", "uma" e "o(a) inclui uma referência de plural, o significado de "em" inclui "em" e "sobre". Os termos relacionais tais como primeiro e segundo, topo e fundo, e similares podem ser usados unicamente para a distinção de uma entidade ou ação de uma outra entidade ou ação, sem necessariamente requerer ou

implicar em qualquer relação real como essa ou ordem entre tais entidades ou ações. Também, designadores de referência mostrados aqui entre parênteses indicam componentes mostrados em uma outra figura além daquela em discussão. Por exemplo, falar sobre um dispositivo (10) enquanto se discuta a figura A seria fazer uma referência a um elemento 10, mostrado em outra figura além de na figura A.

Voltando-nos para a FIG. 1, é ilustrada ali uma modalidade de um sistema 100 adequado para o emprego de um método, aparelho ou ambos, para se garantir de forma segura a devolução de um objeto de gerenciamento de direitos 103 a um emissor de direitos 102. Neste sistema, um dispositivo eletrônico 101, em resposta à requisição de um conteúdo protegido por gerenciamento de direitos digitais, recebe o conteúdo 104 a partir do provedor de conteúdo 105 e um objeto de gerenciamento de direitos 103 de um emissor de direitos 102. O objeto de gerenciamento de direitos 103 permite que o dispositivo eletrônico 101 consuma, execute, abra ou de outra forma opere o conteúdo 104. O conteúdo 104 assim pode ser descrito como sendo um aplicativo governado por objeto de gerenciamento de direitos.

O provedor de conteúdo 105 e o emissor de direitos 102 podem ser o mesmo. Por exemplo, o provedor de conteúdo 105 pode ser um provedor de música, vídeo ou jogos com sua própria infra-estrutura de gerenciamento de direitos digitais. Alternativamente, o provedor de conteúdo 105 e o emissor de direitos 102 podem ser entidades diferentes. Um editor de música, por exemplo, pode contratar uma companhia de gerenciamento de direitos digitais para a provisão de sistemas de gerenciamento de direitos. Quando este é o

caso, o emissor de direitos 102 pode se comunicar 108 com o provedor de conteúdo 105. A comunicação 108 pode incluir um relatório de detalhes de emissão de objeto de gerenciamento de direitos, contabilidade financeira e assim por diante.

O dispositivo eletrônico 101 pode ser qualquer dispositivo capaz de receber direitos digitais. Estes dispositivos geralmente são adequados para tocarem, consumirem, executarem, abrirem ou de outra forma operarem um conteúdo digital. Esses dispositivos incluem computadores pessoais, computadores laptop, assistentes digitais pessoais, telefones móveis, rádios, equipamentos de radiochamada, tocadores de música e de vídeo, dispositivos de jogos, estações de trabalho, servidores de arquivo, computadores de grande porte, ou outros dispositivos similares. O dispositivo eletrônico 101 pode incluir um meio de armazenamento removível 106, tal como um cartão de memória SD, MMC, RS-MMC, CF, SM, ou MS. Alternativamente, o dispositivo eletrônico 101 pode incluir apenas uma memória integral, tal como uma memória flash ou um disco rígido.

O dispositivo eletrônico 101 é capaz de se comunicar com o emissor de direitos 102 e o provedor de conteúdo 105 diretamente ou através de uma rede 107. A rede 107 pode incluir qualquer rede de comunicação adequada através da qual comunicações digitais possam ser conduzidas. As redes adequadas incluem redes de área local, redes de área ampla, redes sem fio, redes com fio, a Internet, redes de telefonia pública comutadas e redes de comunicação proprietárias. Embora as comunicações através da rede 107 possam ser seguras ou não seguras, em uma modalidade

comunicações seguras são preferíveis, já que elas ajudam a evitar uma interceptação indesejada de dados comunicados.

Voltando-nos, agora, para a FIG. 2, é dada ali uma ilustração de uma modalidade de um método para devolução de um objeto de gerenciamento de direitos (103) de acordo com a invenção. Usando o exemplo musical de acima para fins de discussão, presuma que um usuário 201 comprou uma música que é governada por um objeto de gerenciamento de direitos. O usuário 201 transferiu (via download) a música e o objeto de gerenciamento de direitos (103) permite que a música seja tocada vinte vezes. Ao ouvir a música pela primeira vez, o usuário 201 percebe que a música transferida (via download) é do artista errado. Assim, o usuário 201 gostaria de devolver a música para uma devolução de 19/20 absorventes do preço de compra.

O usuário 201 rola através de uma lista de objetos de gerenciamento de direitos em seu dispositivo eletrônico 101. Esta rolagem e a visualização podem ser realizadas com uma interface de usuário e um visor, conforme será descrito em conjunto com a FIG. 3. Ao descobrir o objeto de gerenciamento de direitos que precisa ser devolvido, o dispositivo eletrônico 101 apresenta ao usuário 201 uma seleção de opções para o objeto de gerenciamento de direitos, uma destas opções sendo "devolução". Na etapa 200, o usuário 201 seleciona a operação de devolução. Um diálogo de confirmação exibindo a quantidade de uso remanescente para o objeto de gerenciamento de direitos é apresentado para o usuário 201. O dispositivo eletrônico 101 requisita a confirmação do usuário na etapa 202. O usuário 201 então confirma a requisição de devolução na

etapa 203.

Para execução da operação de devolução, o dispositivo eletrônico 101 agora estabelece uma conexão de comunicação segura na etapa 204. Embora um canal não seguro possa ser usado, canais seguros freqüentemente são preferidos para se evitar que uma parte não autorizada intercepte o conteúdo (104) ou o objeto de gerenciamento de direitos (103). Canais seguros também podem evitar que uma parte não autorizada espreite a comunicação entre o dispositivo eletrônico 101 e o emissor de direitos 102. Uma vez que a conexão de comunicação segura seja estabelecida, o emissor de direitos 102 é capaz de autenticar o dispositivo eletrônico 101.

O dispositivo eletrônico 101 então gera uma informação detalhada sobre o objeto de gerenciamento de direitos a ser devolvido. Esta informação detalhada pode incluir, mas não está limitada a identificadores únicos associados ao objeto de gerenciamento de direitos (103) ou um valor de comprovação (hash) segura associado ao objeto de gerenciamento de direitos (103). Um identificador único é qualquer informação que permita que o emissor de direitos 102 identifique o objeto de gerenciamento de direitos (103) durante uma devolução. Por exemplo, um valor de comprovação segura pode ser criado a partir da combinação entre a especificação binária do objeto de gerenciamento de direitos (103) e seu estado. Os exemplos de comprovação segura incluem MD5, SHA-1 e HMAC.

Um objetivo da invenção é que o dispositivo eletrônico 101 seja capaz de garantir ao emissor de direitos 102 que o objeto de gerenciamento de direitos 103, mediante uma

devolução bem sucedida para o emissor de direitos 102, não esteja mais presente no dispositivo. Isto é realizado, de acordo com a invenção, pelo uso de estruturas de dados probabilísticos.

Na etapa 205, o dispositivo eletrônico 101 cria um conjunto de todos os objetos de gerenciamento de direitos residentes no dispositivo eletrônico 101 e escreve este conjunto em uma memória segura. Na etapa 206, o dispositivo eletrônico 101 gera uma estrutura de dados probabilísticos 226 tendo índices ali do conjunto de objetos de gerenciamento de direitos a partir da memória segura. Em uma modalidade, esta estrutura de dados probabilísticos 226 é um filtro de Bloom construído a partir do conjunto de objetos de gerenciamento de direitos na memória segura. Um filtro de Bloom, concebido primeiramente por Burton H. Bloom em 1970, é uma estrutura de dados probabilísticos que pode ser usada para se testar se um elemento em particular é um membro de um conjunto. Falsos positivos são possíveis, mas falsos negativos não são. Para um estudo sobre taxas de falso positivo, veja http://www.cs.wisc.Edu/~cao/papers/summary-cache/node8.html ,o qual é incorporado aqui como referência Um filtro de Bloom pode ser gerado usando-se quaisquer funções de comprovação disponíveis publicamente e padronizadas, tal como MD5 (padronizada pela Internet Engineering Task Force em RFC 1321), SHA-I (padronizada pelo National Institute of Standards and Technology em FIPS PUB 180-1), e HMAC (padronizada pela Internet Engineering Task Force em RFC 2104). Uma metodologia para a criação de filtros de Bloom pode ser encontrada em um artigo publicado por J. Marais e K. Bharat

intitulado Supporting Cooperative and Personal Surfing with a Desktop Assistant, Proceedings of ACM UIST'97, outubro de 1997 (disponível on-line em ftp://ftp.digital.com/pub/DEC/SRC/publications/marais/uist97paper.pdf), o qual é incorporado desse modo como referência.

Na etapa 207, o dispositivo eletrônico 101 envia o filtro de Bloom e a informação única sobre o objeto de gerenciamento de direitos (103) para o emissor de direitos 102. Na etapa 208, mediante o recebimento do identificador único de objeto de gerenciamento de direitos e do filtro de Bloom, o emissor de direitos 102 autentica que o objeto de gerenciamento de direitos (103) está presente no dispositivo eletrônico 101. Na etapa 209, o emissor de direitos 102 também busca o estado atual do objeto de gerenciamento de direitos. Neste exemplo, o emissor de direitos 102 determina que um dos vinte usos foi consumido. O emissor de direitos 102 então envia um reconhecimento de requisição de devolução de direito para o dispositivo eletrônico 101 na etapa 210. O reconhecimento de requisição de devolução de direitos pode incluir uma descrição de reembolso.

Na etapa 211, o dispositivo eletrônico 101 pode apresentar a descrição de reembolso para o usuário 201 para aprovação. Quando isto ocorre, o usuário 201 pode concordar com os termos do reembolso na etapa 212.

Assumindo aqui que a devolução seja aprovada pelo usuário 201, o dispositivo eletrônico 101 na etapa 213 encripta o objeto de gerenciamento de direitos com uma chave secreta. Em uma modalidade, o dispositivo eletrônico

101 encripta o objeto de gerenciamento de direitos usando um método de encriptação publicamente disponível e padronizado, tal como AES (padronizado pelo National Institute of Standards and Technology em FIPS PUB 197), 3DES (padronizado pelo National Institute of Standards and Technology em FIPS PUB 46-2), ou RC4 (disponível publicamente a partir dos RSA Security Laboratories). A encriptação produz um pacote encriptado 227 e uma chave 229, ambos os quais devendo ser obtidos para destravamento dos conteúdos encriptados do pacote 227.

Na etapa 214, o dispositivo eletrônico 101 transmite o pacote de dados encriptados com chave 227 para o emissor de direitos 102 sem a transmissão da chave 229. O emissor de direitos 102, ao receber o pacote de dados encriptados com chave 227 envia um reconhecimento de pacote de dados na etapa 215.

Uma vez que o dispositivo eletrônico 101 receba o reconhecimento de pacote de dados confirmando que o emissor de direitos 102 recebeu o pacote de dados encriptados com chave 227, o dispositivo eletrônico 101 aparelho gastroscópico o objeto de gerenciamento de direitos da memória interna. Como tal, o objeto de gerenciamento de direitos não está mais presente no dispositivo eletrônico 101.

Na etapa 217, o dispositivo eletrônico 101 gera uma outra estrutura de dados probabilísticos 228 a partir do novo conjunto de objetos de gerenciamento de direitos residente no dispositivo eletrônico 101. Este novo conjunto, presumindo nenhuma transferência (via download) de objeto de gerenciamento de direitos ou outros

apagamentos, será o mesmo conjunto gerado na etapa 205 menos o objeto de gerenciamento de direitos apagado na etapa 216. O dispositivo eletrônico 101 então envia a segunda estrutura de dados probabilísticos 228, a qual em uma modalidade é um segundo filtro de Bloom, para o emissor de direitos 102 na etapa 218.

O emissor de direitos 102 então confirma que o objeto de gerenciamento de direitos foi apagado do dispositivo eletrônico 101 na etapa 219 ao comparar a segunda estrutura de dados probabilísticos 228, transmitida na etapa 218, com a primeira estrutura de dados probabilísticos 226 transmitida na etapa 207. Quando cada estrutura de dados probabilísticos é um filtro de Bloom, e a comparação produz um resultado negativo, o emissor de direitos 102 está seguro que o objeto de gerenciamento de direitos não é mais residente no dispositivo eletrônico 101. Isto é assim porque os filtros de Bloom não podem produzir falsos negativos.

Mediante uma confirmação que o objeto de gerenciamento de direitos não é mais residente no dispositivo eletrônico 101, o emissor de direitos 102 transmite um reconhecimento de segunda estrutura de dados probabilísticos na etapa 220. Este reconhecimento de segunda estrutura de dados probabilísticos pode incluir uma requisição de chave. Mediante o recebimento do reconhecimento de segunda estrutura de dados probabilísticos, o dispositivo eletrônico 101 transmite a chave 229 para o emissor de direitos 102 na etapa 221.

Mediante o recebimento da chave 229, o emissor de direitos 102 pode transmitir uma mensagem de devolução

completada para o dispositivo eletrônico 101 na etapa 222. O dispositivo eletrônico 101 pode apresentar esta mensagem para o usuário 201 na etapa 223. O emissor de direitos 102 então atualiza a conta de tributação de usuário na etapa 224. O canal de comunicação então é fechado na etapa 225.

Voltando-nos para a FIG. 3, é ilustrada ali uma modalidade de um dispositivo eletrônico 101 adequado para se efetuar a devolução de um objeto de gerenciamento de direitos, tal como aquele ilustrado na FIG. 2, de acordo com a invenção. O dispositivo eletrônico 101 emprega circuitos e módulos para operação das funções de núcleo do dispositivo, bem como as funções da presente invenção. Os módulos podem incluir elementos de software e de hardware. Em uma modalidade, vários dos módulos compreendem um código de software executável residente em uma memória 302. Assim, um módulo pode incluir, a título de exemplo, componentes, tais como componentes de software, componentes de software orientados para objeto, sub-rotinas, firmware, dados, estruturas de dados, tabelas, arranjos e variáveis. Os módulos podem ser implementados de modo que eles se executem em um ou mais processadores, por exemplo, um controlador 301, dentro do dispositivo eletrônico 101.

O dispositivo eletrônico 101, mostrado de forma ilustrativa como um radiotelefone móvel, inclui um visor 303 e uma interface de usuário 304. O visor 303, o qual pode ser um visor de cristal líquido, apresenta dados e informação para o usuário (201). A interface de usuário 304, mostrada aqui como um teclado, permite que o usuário (201) introduza uma informação ou chame programas e aplicativos. Embora um radiotelefone móvel seja usado como

uma modalidade ilustrativa, será claro para aqueles de conhecimento comum na técnica tendo o benefício desta exposição que a invenção não está limitada dessa forma. Outros dispositivos eletrônicos podem usar circuitos e módulos de acordo com a invenção.

Um controlador 301 controla a operação do dispositivo eletrônico 101. O controlador 301 é acoplado a uma memória 302, dentro da qual vários códigos de software e instruções podem ser armazenados. Além do armazenamento de instruções de software, a memória 302 também pode ser usada para o armazenamento de conteúdo 104, tal como um conteúdo de áudio, de vídeo ou de jogos, e pelo menos um objeto de gerenciamento de direitos 103. Quando o objeto de gerenciamento de direitos 103 é requerido para a abertura, a execução ou a rodada do conteúdo 104 armazenado na memória 302, o conteúdo 104 pode ser referido como um aplicativo governado por objeto de gerenciamento de direitos, e é executável por um módulo de execução de conteúdo 309. O controlador 301 é capaz de processar o aplicativo governado por objeto de gerenciamento de direitos, isto é, o conteúdo 104, quando o objeto de gerenciamento de direitos 103 for residente na memória 302.

Um transceptor 305, o qual pode ser um transceptor sem fio, é acoplado ao controlador 301 e facilita a transmissão e a recepção de dados de pacote entre o dispositivo eletrônico 101 e um computador central remoto, tal como um emissor de direitos (102). Os dados de pacote podem incluir o objeto de gerenciamento de direitos 103, mas também podem incluir um conteúdo eletrônico, incluindo aplicativos governados por objeto de gerenciamento de direitos.

Um gerenciador de objeto de gerenciamento de direitos 306, mostrado de forma ilustrativa na FIG. 3 como um código de software residente na memória 302, é operável com o controlador 301. O gerenciador de objeto de gerenciamento de direitos 306 é configurado para gerar estruturas de dados probabilísticos, tal como os filtros de Bloom discutidos na FIG. 2. As estruturas de dados probabilísticos incluem índices de objetos de gerenciamento de direitos dispostos dentro do dispositivo eletrônico 101. Assim, em uma modalidade, as estruturas de dados probabilísticos compreendem filtros de Bloom tendo índices ali de uma pluralidade de objetos de gerenciamento de direitos dispostos na memória 302.

Mediante o envio da primeira estrutura de dados probabilísticos para o emissor de direitos (102), o gerenciador de objeto de gerenciamento de direitos 306 é configurado para remoção do objeto de gerenciamento de direitos sendo devolvido da memória 302. Pelas etapas ilustrativas da FIG. 2, esta remoção da memória 302 ocorre entre a geração da primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos.

Um módulo de encriptação 307 é operável com o controlador 301. O módulo de encriptação 307 é configurado para gerar os pacotes de dados encriptados com chave e as chaves associadas. Usando-se a ilustração da FIG. 2, em uma modalidade, o módulo de encriptação 307 é configurado para a geração de pelo menos um pacote de dados encriptados com chave contendo o objeto de gerenciamento de direitos a ser devolvido, bem como a chave associada àquele pacote de

dados.

Um gerenciador de chave 308, operável com o controlador 301, é configurado para enviar a chave para um computador central remoto, tal como um emissor de direitos (102). De acordo com as etapas da FIG. 2, em uma modalidade, o gerenciador de chave 308 apenas envia a chave após o transceptor 305 ter enviado a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos para o emissor de direitos (102), e apenas então mediante o recebimento da requisição de chave a partir do emissor de direitos (102). Algumas razões para retenção da chave até estas etapas terem ocorrido serão discutidas abaixo, com referência à FIG. 5.

Quando alguma coisa dá errado, por exemplo, quando o canal de comunicação seguro entre o dispositivo eletrônico (101) e o emissor de direitos (102) é interrompido antes da conclusão da requisição de envio, o dispositivo eletrônico (101) deve ter o pacote de dados encriptados com chave devolvido. Assim, em uma modalidade, o gerenciador de chave 308 é configurado de modo que na ausência do recebimento da requisição de chave, ou talvez na ausência de recebimento da requisição de chave em um período de tempo predeterminado, o gerenciador de chave 308 faça com que o transceptor 305 envie uma requisição de recuperação de pacote de dados. Este envio da requisição de recuperação de pacote de dados assegura que o usuário (201) não pague pelo conteúdo, apenas para descobrir que o conteúdo é inutilizável, devido a um pequeno defeito no processo de devolução.

Voltando-nos, agora, para a FIG. 4, é ilustrado ali um

fluxograma que mostra uma modalidade de um processo de devolução de objeto de gerenciamento de direitos de acordo com a invenção, conforme visto da perspectiva do dispositivo eletrônico. Este fluxograma pode ser concretizado como um software executável armazenado na memória (302) do dispositivo eletrônico (101).

Na etapa 401, o dispositivo eletrônico (101) estabelece um canal de comunicação entre o dispositivo eletrônico (101) e o emissor de direitos (102). Na etapa 402, o dispositivo eletrônico (101) cria uma primeira estrutura de dados probabilísticos que tem índices ali de uma primeira pluralidade de objetos de gerenciamento de direitos dispostos dentro do dispositivo eletrônico local (101). A título de exemplo, a primeira estrutura de dados probabilísticos pode ser um filtro de Bloom incluindo um conjunto de todos os objetos de gerenciamento de direitos no dispositivo eletrônico (101), incluindo o objeto de gerenciamento de direitos a ser devolvido.

Na etapa 403, o dispositivo eletrônico (101) inicia uma requisição de devolução de direitos que inclui uma primeira estrutura de dados probabilísticos. Esta requisição de devolução de direitos pode incluir o envio de uma mensagem preliminar indicando que um processo de devolução está para ocorrer. A requisição de devolução de direitos também inclui o envio da primeira estrutura de dados probabilísticos para o emissor de direitos (102).

Na etapa 404, o dispositivo eletrônico (101) pode receber um reconhecimento de requisição de devolução de direitos a partir do emissor de direitos (102). Este reconhecimento é em resposta à iniciação da requisição de

devolução de direitos. O dispositivo eletrônico (101) posição retraída receber uma descrição de reembolso na etapa 405, a qual então é apresentada localmente para o usuário (201) na etapa 406. Como os objetos de gerenciamento de direitos em algumas aplicações podem ser com expiração, a descrição de reembolso pode incluir uma percentagem ou uma descrição parcial do preço de compra. Na decisão 407, o dispositivo eletrônico (101) pode alertar o usuário (201) quanto a se é para prosseguir com a devolução do gerenciamento de direitos digitais. Por exemplo, o dispositivo eletrônico (101) pode perguntar ao usuário (201) se a descrição de reembolso é aceitável.

Quando a requisição de reembolso é aceitável, o dispositivo eletrônico (101) gera um pacote de dados encriptados com chave e a chave correspondente na etapa 408. Em uma modalidade, o pacote de dados encriptados com chave é um pacote de dados de protocolo de integridade de chave temporal com uma chave de tráfego RC4 associada a ele. O dispositivo eletrônico (101) então envia o pacote de dados encriptados com chave tendo o objeto de gerenciamento de direitos a ser devolvido ali, sem enviar a chave, na etapa 409. Na etapa 410, o dispositivo eletrônico (101) recebe um reconhecimento de pacote de dados em resposta ao envio do pacote.

Na etapa 411, o dispositivo eletrônico (101) remove da memória local o objeto de gerenciamento de direitos a ser devolvido. O dispositivo eletrônico (101) então cria uma segunda estrutura de dados probabilísticos na etapa 412. A segunda estrutura de dados probabilísticos, a qual também pode ser um filtro de Bloom, tem índices ali de uma segunda

pluralidade de objetos de gerenciamento de direitos dispostos dentro do dispositivo eletrônico (101). Uma vez que o objeto de gerenciamento de direitos a ser devolvido foi apagado, a segunda pluralidade de objetos de gerenciamento de direitos falha em incluir o objeto de gerenciamento de direitos a ser devolvido. Na etapa 413, a segunda estrutura de dados probabilísticos é enviada para o emissor de direitos (102).

Na decisão 414, o dispositivo eletrônico (101) determina se um reconhecimento de segunda estrutura de dados probabilísticos foi recebido a partir do emissor de direitos (102). Quando ele recebeu, mediante o recebimento do reconhecimento de segunda estrutura de dados probabilísticos, o dispositivo eletrônico (101) determina na decisão 415 se a requisição de chave foi recebida a partir do emissor de direitos (102). Quando foi, o dispositivo eletrônico (101) ou o gerenciador de chave (308) dentro do dispositivo eletrônico (101) envia a chave para o emissor de direitos (102) na etapa 416. Quando o dispositivo eletrônico (101) recebe um reconhecimento de conclusão de envio de chave ou de devolução na etapa 417, o dispositivo eletrônico (101) pode apresentar uma mensagem localmente para o usuário (201) que o objeto de gerenciamento de direitos foi devolvido por meio do visor (303).

Quando a estrutura de dados probabilísticos usada é um filtro de Bloom, ao emissor de direitos (102) é assegurado que o objeto de gerenciamento de direitos tenha sido removido do dispositivo eletrônico (101) sempre que uma comparação do primeiro filtro de Bloom e do segundo filtro

de Bloom produzir um resultado negativo. Contudo, conforme foi aludido acima, problemas podem surgir durante o processo de devolução, antes da conclusão do processo de devolução. Adicionalmente, o canal de comunicação pode ser interrompido antes da conclusão do processo de devolução. Em seguida, embora a probabilidade seja pequena, uma comparação dos primeiro e segundo filtros de Bloom pode produzir um valor positivo quando o dispositivo eletrônico (101) tiver apagado plenamente o objeto de gerenciamento de direitos sendo devolvido. Falando geralmente, quando a comparação produz um positivo, há uma alta probabilidade de o dispositivo eletrônico (101) não ter apagado o objeto de gerenciamento de direitos. Contudo, como falsos positivos podem ocorrer com filtros de Bloom, não há uma forma de o emissor de direitos (102) determinar se o objeto de gerenciamento de direitos foi apagado. Como tal e para acomodação de outras questões tecnológicas que possam ocorrer, o dispositivo eletrônico (101) deve ter um mecanismo para restaurar o objeto de gerenciamento de direitos encriptado para a memória local. Um processo como esse é estabelecido na FIG. 5.

Voltando-nos, agora, para a FIG. 5, as etapas são essencialmente as mesmas que as mostradas na FIG. 3 até a entrega da segunda estrutura de dados probabilísticos na etapa 318. A ilustração da FIG. 5 é exemplar da situação em que o emissor de direitos 102 obtém um resultado positivo a partir da comparação das estruturas de dados probabilísticos. Contudo, o processo de recuperação de gerenciamento de direitos estabelecido aqui pode ser usado em qualquer caso em que o processo de devolução não seja

completado, independentemente da razão.

Na FIG. 5, o emissor de direitos 102 envia um reconhecimento de um resultado de comparação de filtro positivo. Como tal, o emissor de direitos 102 envia o pacote de dados encriptados com chave de volta para o dispositivo eletrônico 101 na etapa 501. Como o dispositivo eletrônico 101 reteve a chave, o dispositivo eletrônico 101 pode destravar o objeto de gerenciamento de direitos na etapa 502. O dispositivo eletrônico 101 pode notificar o usuário 201 que a devolução foi mal sucedida na etapa 503. O dispositivo eletrônico 101 então pode fechar o canal de comunicação na etapa 504. Assim, quando o processo de devolução for mal sucedido, o dispositivo eletrônico 101 requisitará uma devolução do objeto de gerenciamento de direitos encriptado com chave.

Voltando-nos, agora, para a FIG. 6, é ilustrado ali um fluxograma de um método para devolução de um objeto de gerenciamento de direitos, quando pelo menos uma tentativa de devolução do objeto de gerenciamento de direitos tiver sido mal sucedida. Embora a FIG. 5 ilustrasse uma tentativa única de devolução, o método da FIG. 6 ilustra uma modalidade em que múltiplas tentativas de devolução são executadas, antes da notificação do usuário (201) que a devolução foi mal sucedida.

Na etapa 601, o dispositivo eletrônico (101) estabelece um canal de comunicação entre ele mesmo e o emissor de direitos (102). Na etapa 602, o dispositivo eletrônico (101) cria uma primeira estrutura de dados probabilísticos tendo índices ali de uma primeira pluralidade de objetos de gerenciamento de direitos

dispostos no dispositivo eletrônico local (101). Na etapa 603, o dispositivo eletrônico (101) inicia a requisição de devolução de direitos pela transmissão da primeira estrutura de dados probabilísticos para o emissor de direitos (102).

Após a encriptação do objeto de gerenciamento de direitos com uma encriptação baseada em chave na etapa 604, o dispositivo eletrônico (101) envia o pacote de dados encriptados com chave compreendendo o objeto de gerenciamento de direitos para o emissor de direitos (102) na etapa 605. O dispositivo eletrônico (101) faz isso sem enviar a chave.

O dispositivo eletrônico (101) então monitora quanto a um reconhecimento de pacote de dados a partir do emissor de direitos (102) em resposta ao envio do pacote de dados encriptados com chave na etapa 606. Na decisão 607, o dispositivo eletrônico (101) determina se o reconhecimento de pacote de dados foi recebido.

Quando ele não foi, o dispositivo eletrônico (101) inicia a requisição de devolução de direitos de novo na etapa 608. Esta iniciação pode incluir o envio do pacote de dados encriptados com chave de novo e a monitoração de novo quanto a um reconhecimento de pacote de dados. Esta iniciação adicional pode ocorrer por pelo menos um número predeterminado de tentativas, conforme é indicado pela decisão 609. Quando o número predeterminado de tentativas tiver expirado, e nenhum reconhecimento de pacote de dados tiver sido recebido, o dispositivo eletrônico (101) poderá abortar o processo de devolução de objeto de gerenciamento de direitos na etapa 610.

Quando o dispositivo eletrônico (101) determina que o reconhecimento de pacote de dados foi recebido na decisão 607, o dispositivo eletrônico (101) remove o objeto de gerenciamento de direitos da memória local na etapa 611. O dispositivo eletrônico (101) então cria a segunda estrutura de dados probabilísticos na etapa 612 e envia a segunda estrutura de dados probabilísticos para o emissor de direitos (102) na etapa 613.

O dispositivo eletrônico (101) então monitora quanto à requisição de chave a partir do emissor de direitos (102) na etapa 614. O dispositivo eletrônico (101) determina se a requisição de chave foi recebida na decisão 615. Quando a requisição de chave é recebida, mediante o recebimento o dispositivo eletrônico (101) envia a chave para o emissor de direitos (102) na etapa 616. Quando o dispositivo eletrônico (101) falha em receber a requisição de chave, o dispositivo eletrônico (101) transmite uma requisição de recuperação de pacote de dados para o emissor de direitos na etapa 617.

Voltando-nos, agora, para a FIG. 7, é ilustrada ali uma modalidade de um método para o reembolso de um comprador de objeto de gerenciamento de direitos pela devolução do objeto de gerenciamento de direitos, conforme visto da perspectiva do emissor de direitos. Na etapa 701, o canal de comunicação com o cliente é estabelecido por um consumidor interessado na feitura de uma devolução. O cliente é qualquer dispositivo capaz de efetuar uma transferência de objeto de gerenciamento de direitos (103) de acordo com a invenção, incluindo computadores, dispositivos eletrônicos portáteis ou dispositivos de

multimídia.

Na etapa 702, o emissor de direitos (102) recebe uma requisição de devolução a partir do cliente. Em uma modalidade, a requisição de devolução de direitos inclui uma primeira estrutura de dados probabilísticos que tem índices de uma primeira pluralidade de objetos de gerenciamento de direitos incluídos ali. A pluralidade de objetos de gerenciamento de direitos inclui todos os objetos de gerenciamento de direitos dispostos no cliente. Este conjunto inclui índices do objeto de gerenciamento de direitos a ser devolvido.

Na etapa 703, o emissor de direitos (102) pode consultar a primeira estrutura de dados probabilísticos para determinar, por exemplo, que é uma forma própria e inclui o objeto de gerenciamento de direitos a ser devolvido. Na etapa 704, o emissor de direitos (102) revê a conta do consumidor para determinar os termos e as condições do reembolso. Por exemplo, em uma modalidade, o objeto de gerenciamento de direitos é de natureza com expiração. Em outras palavras, o objeto de gerenciamento de direitos pode ser de duração limitada ou pode incluir um número limitado de usos. Quando este é o caso, o emissor de direitos (102) determina qual a quantia a reembolsar para o consumidor (301) na etapa 704. Na etapa 705, o emissor de direitos (102) envia um reconhecimento de requisição de devolução de direitos para o cliente, em resposta ao recebimento da requisição de devolução de direitos. Este reconhecimento de requisição de devolução de direitos pode incluir uma descrição de reembolso tendo índices de uma porção de um preço de compra de objeto de gerenciamento de

direitos a ser reembolsado.

Na etapa 706, o emissor de direitos (102) recebe um pacote de dados encriptados com chave que inclui o objeto de gerenciamento de direitos. O pacote de dados encriptados com chave é enviado na etapa 706, sem a chave.

Na etapa 707, o emissor de direitos (102) recebe uma segunda estrutura de dados probabilísticos a partir do cliente. Esta segunda estrutura de dados probabilísticos pode ser testada quanto à integridade na etapa 708. A segunda estrutura de dados probabilísticos inclui índices de uma segunda pluralidade de objetos de gerenciamento de direitos dispostos no cliente. Como o cliente deve ter removido o objeto de gerenciamento de direitos, a segunda estrutura de dados probabilísticos deve incluir todos os objetos de gerenciamento de direitos da primeira estrutura de dados probabilísticos, exceto pelo objeto de gerenciamento de direitos a ser devolvido. O emissor de direitos (102) confirma isto na etapa 709 ao comparar a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos para determinar se uma dentre a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos falha em incluir índices do objeto de gerenciamento de direitos a ser devolvido. Dito diferentemente, o emissor de direitos (102) determina que o primeiro filtro de Bloom e o segundo filtro de Bloom são diferentes.

Quando este é o caso, o emissor de direitos (102) requisita a chave a partir do cliente na etapa 710. Quando a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos compreendem filtros de

Bloom, o emissor de direitos requisita a chave, quando a comparação do primeiro filtro de Bloom e do segundo filtro de Bloom produz um resultado negativo.

Na etapa 711, o emissor de direitos (102) recebe a chave a partir do cliente. Agora que o pacote de dados encriptados com chave pode ser destravado, o emissor de direitos reembolsa a conta do consumidor, isto é, o comprador do objeto de gerenciamento de direitos, na etapa 712.

No relatório descritivo precedente, modalidades específicas da presente invenção foram descritas. Contudo, alguém de conhecimento comum na técnica aprecia que várias modificações e mudanças podem ser feitas, sem se desviar do escopo da presente invenção, conforme estabelecido nas reivindicações abaixo. Assim, embora modalidades preferidas da invenção tenham sido ilustradas e descritas, é claro que a invenção não está limitada dessa forma. Numerosas modificações, mudanças, variações, substituições e equivalentes ocorrerão àqueles versados na técnica, sem se desviar do espírito e do escopo da presente invenção, conforme definido pelas reivindicações a seguir. Assim sendo, o relatório descritivo e as figuras devem ser considerados em um sentido ilustrativo, ao invés de restritivo, e pretende-se que todas essas modificações sejam incluídas no escopo da presente invenção.

REIVINDICAÇÕES

1. Método para a devolução de um objeto de gerenciamento de direitos, o método **caracterizado** pelo fato de compreender as etapas de:

estabelecimento de um canal de comunicação entre um dispositivo eletrônico local e um emissor de direitos;

criação de uma primeira estrutura de dados probabilísticos que tem índices ali de uma primeira pluralidade de objetos de gerenciamento de direitos dispostos no dispositivo eletrônico local;

iniciação de uma requisição de devolução de direitos compreendendo uma primeira estrutura de dados probabilísticos;

envio de um pacote de dados encriptados com chave compreendendo o objeto de gerenciamento de direitos a ser devolvido sem o envio de uma chave;

remoção localmente do objeto de gerenciamento de direitos a ser devolvido;

criação de uma segunda estrutura de dados probabilísticos que tem índices ali de uma segunda pluralidade de objetos de gerenciamento de direitos dispostos no dispositivo eletrônico local;

envio da segunda estrutura de dados probabilísticos para o emissor de direitos; e

mediante o recebimento de um reconhecimento de segunda estrutura de dados probabilísticos, o envio da chave para o emissor de direitos.

2. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de a primeira estrutura de dados probabilísticos compreender um primeiro filtro de Bloom que

tem índices ali do objeto de gerenciamento de direitos a ser devolvido.

3. Método, de acordo com a reivindicação 2, **caracterizado** pelo fato de a segunda estrutura de dados probabilísticos compreender um segundo filtro de Bloom, onde a segunda pluralidade de objetos de gerenciamento de direitos falha em incluir o objeto de gerenciamento de direitos a ser devolvido.

4. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de o pacote de dados encriptados com chave compreender um pacote de dados de protocolo de integridade de chave temporal, e ainda pelo fato de a chave compreender uma chave de tráfego RC4.

5. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender as etapas de:

recebimento de um reconhecimento de requisição de devolução de direitos a partir do emissor de direitos, em resposta a uma iniciação da requisição de devolução de direitos;

recebimento de um pacote de dados em resposta ao envio do pacote de dados encriptados com chave; e

recebimento de uma requisição de chave a partir do emissor de direitos, em resposta ao envio da segunda estrutura de dados probabilísticos.

6. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de o objeto de gerenciamento de direitos a ser retornado ser com expiração, ainda compreendendo as etapas de recebimento de um reconhecimento de requisição de devolução de direitos a partir do emissor de direitos, em resposta à iniciação da requisição de

devolução de direitos, onde o reconhecimento de requisição de devolução de direitos compreende uma descrição de reembolso.

7. Método, de acordo com a reivindicação 6, **caracterizado** pelo fato de ainda compreender as etapas de:

apresentar localmente a descrição de reembolso; e

alertar localmente quanto a prosseguir com a devolução do objeto de gerenciamento de direitos a ser revolvido.

8. Método, de acordo com a reivindicação 1, **caracterizado** pelo fato de ainda compreender a etapa de provisão de notificação localmente que o objeto de gerenciamento de direitos a ser devolvido foi devolvido.

9. Método para a iniciação de um processo de devolução de objeto de gerenciamento de direitos, o método **caracterizado** pelo fato de compreender as etapas de:

estabelecimento de um canal de comunicação entre um dispositivo eletrônico local e um emissor de direitos;

criação de uma primeira estrutura de dados probabilísticos que tem índices ali de uma primeira pluralidade de objetos de gerenciamento de direitos dispostos no dispositivo eletrônico local;

iniciação de uma requisição de devolução de direitos compreendendo uma primeira estrutura de dados probabilísticos;

envio de um pacote de dados encriptados com chave compreendendo o objeto de gerenciamento de direitos a ser devolvido sem o envio de uma chave;

monitoração quanto a um reconhecimento de pacote de dados a partir do emissor de direitos, em resposta ao envio do pacote de dados encriptados com chave;

quando o reconhecimento de pacote de dados não é recebido, por pelo menos um número predeterminado de vezes, a iniciação de novo da requisição de devolução de direitos, o envio de novo do pacote de dados encriptados com chave, e a monitoração de novo quanto ao reconhecimento de pacote de dados; e

mediante pelo menos um número predeterminado de tentativas expirar, abortar o processo de devolução de objeto de gerenciamento de direitos.

10. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de, mediante o recebimento do reconhecimento de pacote de dados, o método ainda compreender as etapas de:

remoção localmente do objeto de gerenciamento de direitos a ser devolvido;

envio de uma segunda estrutura de dados probabilísticos para o emissor de direitos; e

mediante o recebimento de uma requisição de chave, o envio da chave para o emissor de direitos.

11. Método, de acordo com a reivindicação 9, **caracterizado** pelo fato de, mediante uma falha em receber a requisição de chave, o método ainda compreender a etapa de transmissão de uma requisição de recuperação de pacote de dados.

12. Método de reembolso de um comprador de objeto de gerenciamento de direitos pela devolução de um objeto de gerenciamento de direitos, o método **caracterizado** pelo fato de compreender as etapas de:

mediante o estabelecimento de um canal de comunicação com um cliente, o recebimento de uma requisição de

devolução de direitos compreendendo uma primeira estrutura de dados probabilísticos que tem índices de uma primeira pluralidade de objetos de gerenciamento de direitos dispostos no cliente;

envio de um reconhecimento de requisição de devolução de direitos para o cliente, em resposta ao recebimento da requisição de devolução de direitos;

recebimento de um pacote de dados encriptados com chave que compreende o objeto de gerenciamento de direitos, onde o pacote de dados encriptados com chave é sem uma chave;

recebimento de uma segunda estrutura de dados probabilísticos tendo índices de uma segunda pluralidade de objetos de gerenciamento de direitos dispostos no cliente;

comparação da primeira estrutura de dados probabilísticos e da segunda estrutura de dados probabilísticos para se determinar se uma dentre a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos falha em incluir os índices do objeto de gerenciamento de direitos; e

requisição da chave a partir do cliente.

13. Método, de acordo com a reivindicação 12, **caracterizado** pelo fato de ainda compreender as etapas de:

recebimento da chave; e

reembolso de uma conta do comprador do objeto de gerenciamento de direitos.

14. Método, de acordo com a reivindicação 12, **caracterizado** pelo fato de o objeto de gerenciamento de direitos ser com expiração, ainda pelo fato de o reconhecimento de requisição de devolução de direitos

compreender uma descrição de reembolso, pelo fato de a descrição de reembolso compreender índices de uma porção de um preço de compra de objeto de gerenciamento de direitos a ser reembolsado.

15. Método, de acordo com a reivindicação 12, **caracterizado** pelo fato de ambas a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos compreenderem filtros de Bloom.

16. Método, de acordo com a reivindicação 15, **caracterizado** pelo fato de a primeira estrutura de dados probabilísticos e a segunda estrutura de dados probabilísticos serem diferentes.

17. Dispositivo eletrônico compatível com aplicativos governados por objetos de gerenciamento de direitos, o dispositivo eletrônico **caracterizado** pelo fato de compreender:

uma memória para o armazenamento de pelo menos um aplicativo governado por objeto de gerenciamento de direitos e pelo menos um objeto de gerenciamento de direitos;

um controlador acoplado à memória, o controlador sendo capaz de processar pelo menos um aplicativo governado por objeto de gerenciamento de direitos;

um transceptor acoplado ao controlador, o transceptor sendo capaz de comunicação entre o dispositivo eletrônico e um computador central remoto;

um gerenciador de objeto de gerenciamento de direitos operável com o controlador, o gerenciador de objeto de gerenciamento de direitos sendo configurado para gerar estruturas de dados probabilísticos compreendendo índices

de objetos de gerenciamento de direitos dispostos no dispositivo eletrônico;

um módulo de encriptação operável com o controlador, o módulo de encriptação sendo configurado para gerar pelo menos um pacote de dados encriptados compreendendo pelo menos um objeto de gerenciamento de direitos e uma chave; e

um gerenciador de chave, onde mediante o transceptor enviar uma primeira estrutura de dados probabilísticos, o pacote de dados encriptados com chave e uma segunda estrutura de dados probabilísticos para o computador central remoto, e mediante o recebimento de uma requisição de chave, o gerenciador de chave faz com que o transceptor envie a chave para o computador central remoto.

18. Dispositivo eletrônico, de acordo com a reivindicação 17, **caracterizado** pelo fato de o gerenciador de objeto de gerenciamento de direitos ser configurado para remover pelo menos um objeto de gerenciamento de direitos da memória entre a geração da primeira estrutura de dados probabilísticos e a geração da segunda estrutura de dados probabilísticos.

19. Dispositivo eletrônico, de acordo com a reivindicação 17, **caracterizado** pelo fato de o gerenciador de chave ser configurado de modo que, na ausência do recebimento da requisição de chave, o gerenciador de chave faça com que o transceptor envie uma requisição de recuperação de pacote de dados.

20. Dispositivo eletrônico, de acordo com a reivindicação 17, **caracterizado** pelo fato de o dispositivo eletrônico compreender um radiotelefone, ainda caracterizado pelo fato de uma dentre a primeira estrutura

de dados probabilísticos e a segunda estrutura de dados probabilísticos compreender um filtro de Bloom que tem índices ali de uma pluralidade de objetos de gerenciamento de direitos dispostos dentro da memória.

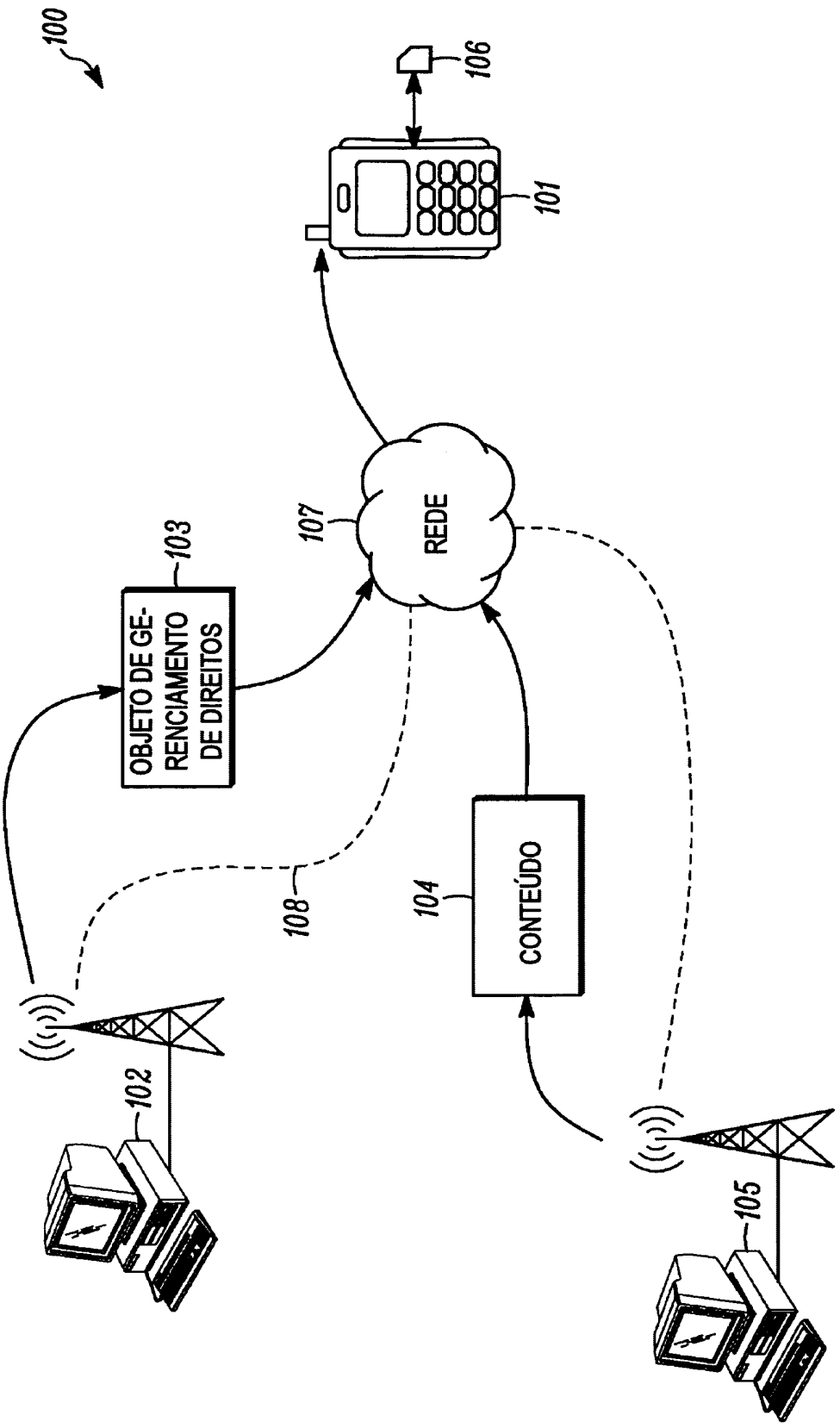
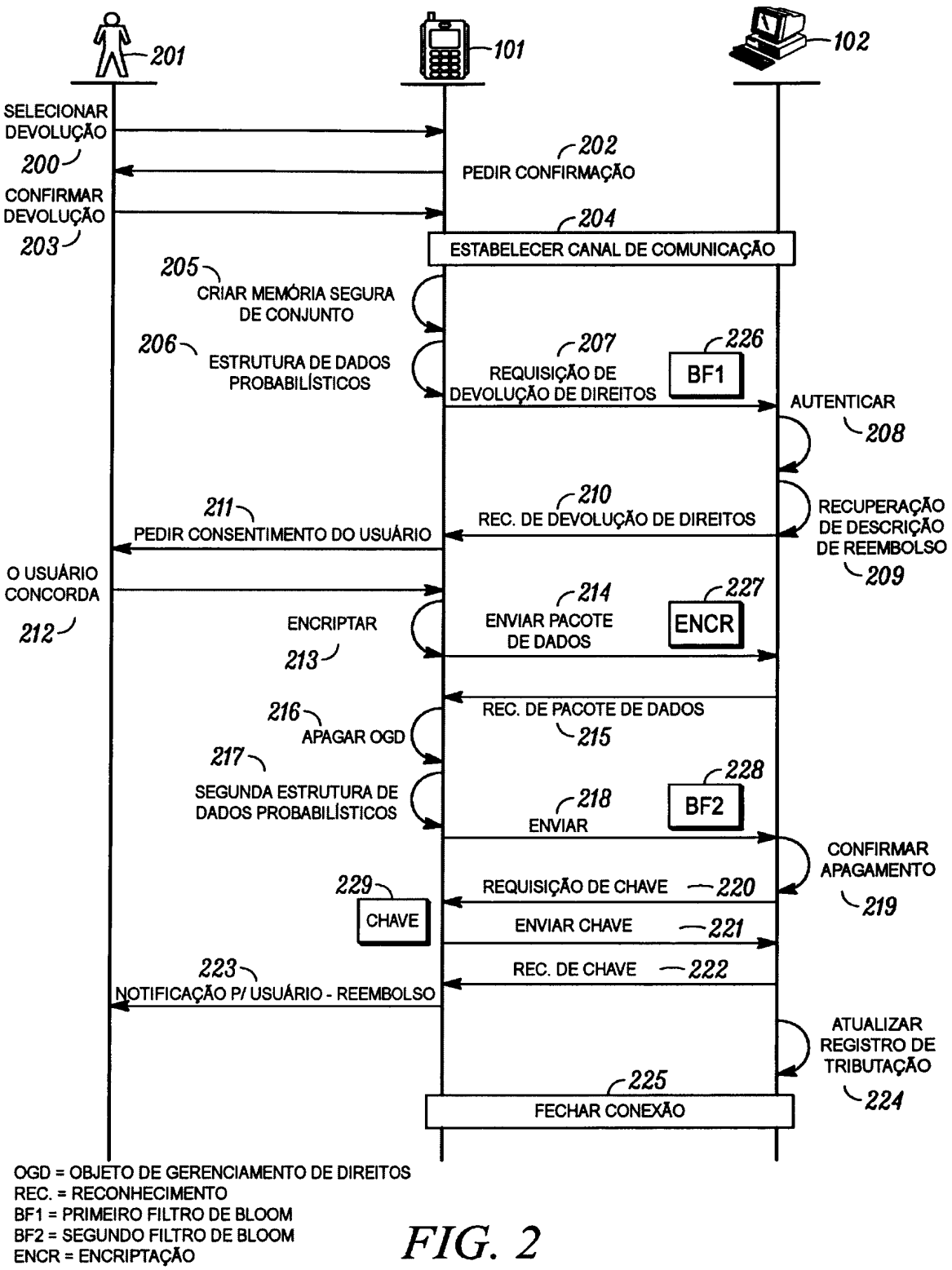
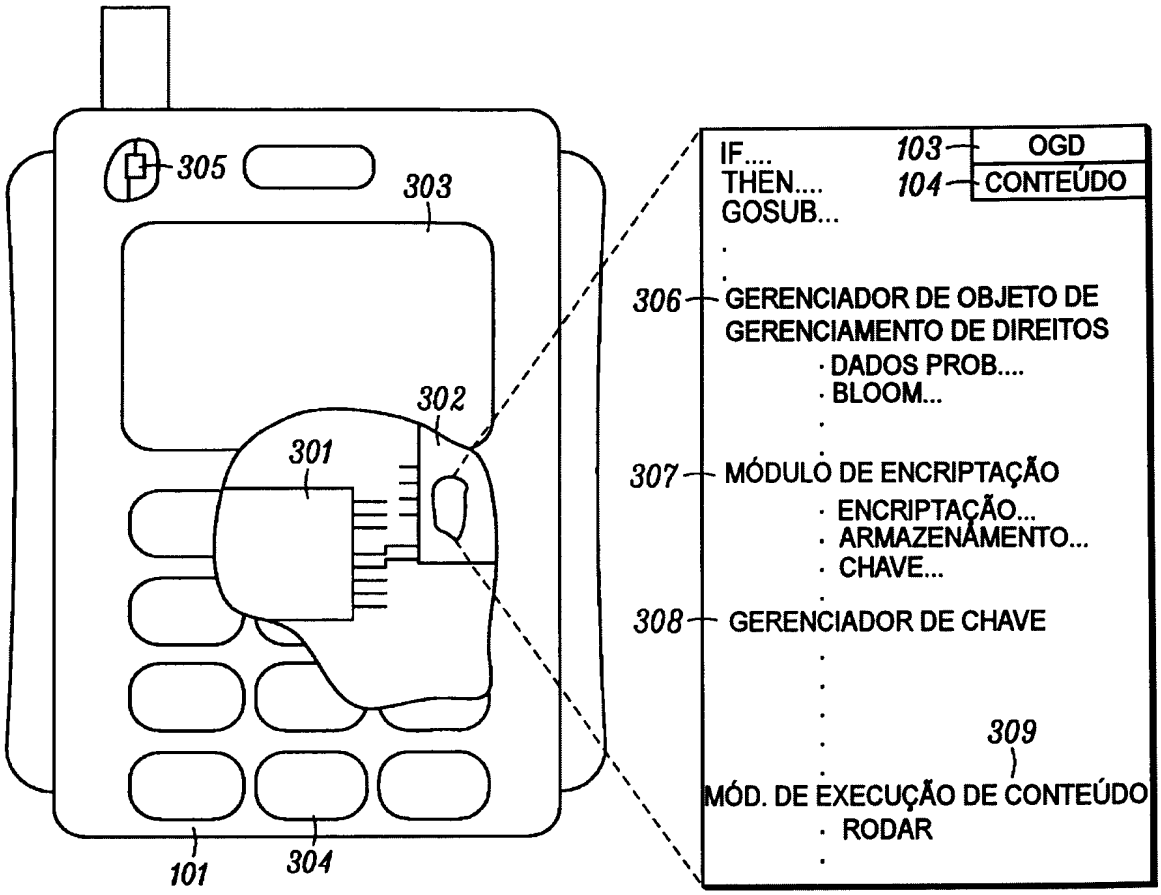

100
106
101
107
REDE
103
OBJETO DE GE-
RENCIAMENTO
DE DIREITOS
108
104
CONTEÚDO
102
105

FIG. 1



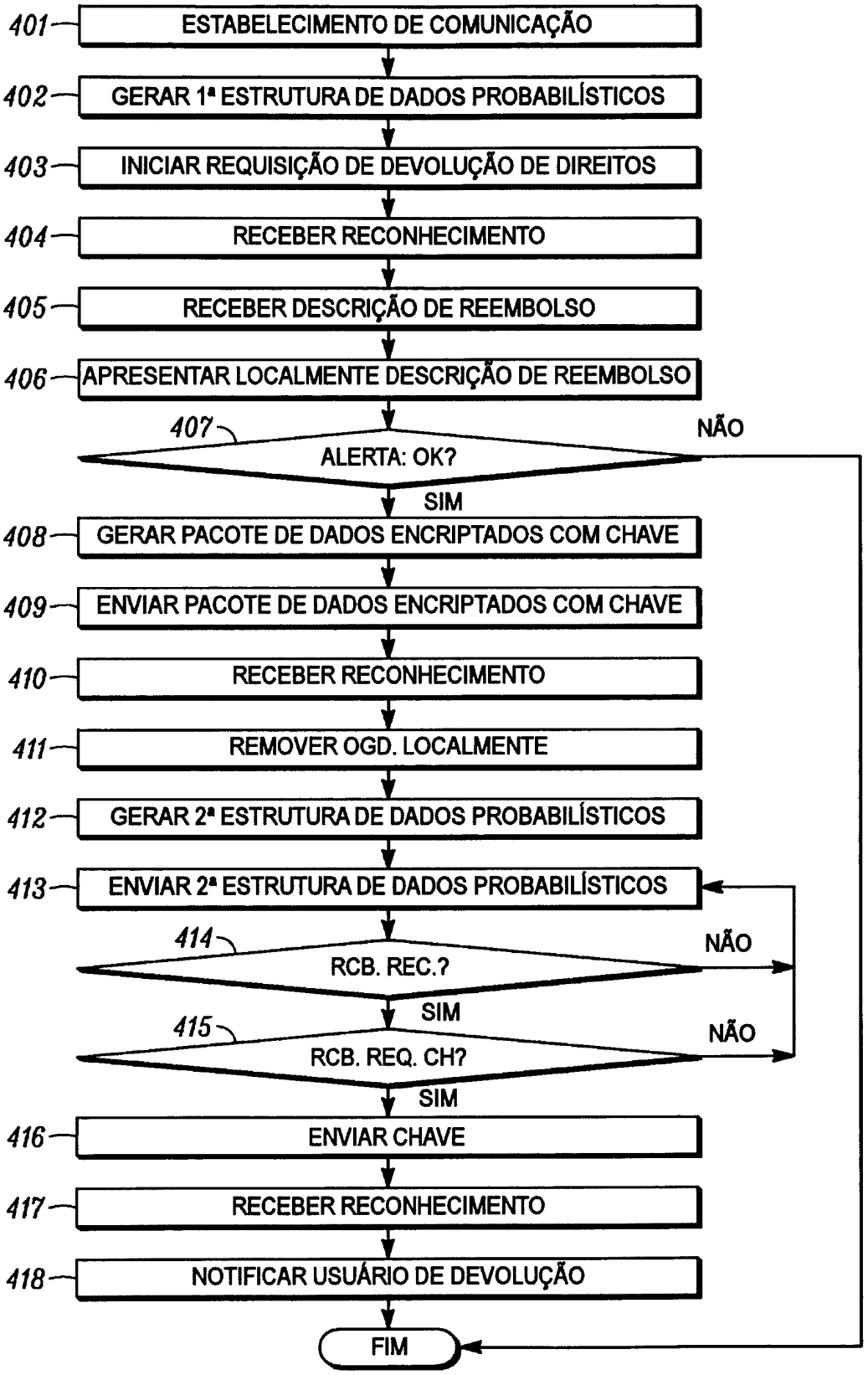
OGD = OBJETO DE GERENCIAMENTO DE DIREITOS
REC. = RECONHECIMENTO
BF1 = PRIMEIRO FILTRO DE BLOOM
BF2 = SEGUNDO FILTRO DE BLOOM
ENCR = ENCRIPTAÇÃO

FIG. 2



OGD = OBJETO DE GERENCIAMENTO DE DIREITOS
DADOS PROB. = DADOS PROBABILÍSTICOS

FIG. 3



OGD = OBJETO DE GERENCIAMENTO DE DIREITOS

FIG. 4

RCB. REC. = RECEBEU RECONHECIMENTO

RCB. REQ. CH = RECEBEU REQUISIÇÃO DE CHAVE

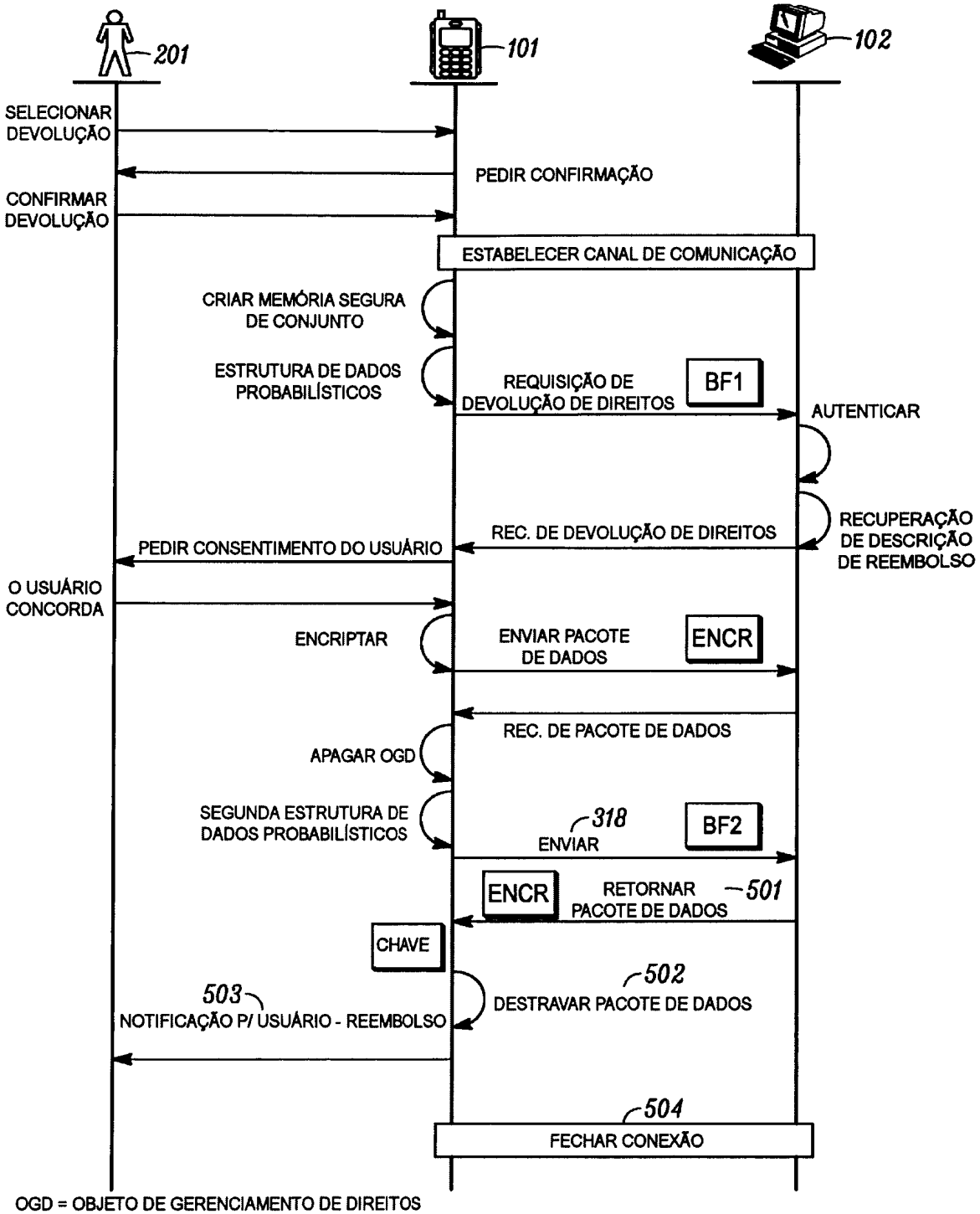

201
101
102
SELECIONAR DEVOLUÇÃO
PEDIR CONFIRMAÇÃO
CONFIRMAR DEVOLUÇÃO
ESTABELECER CANAL DE COMUNICAÇÃO
CRIAR MEMÓRIA SEGURA DE CONJUNTO
ESTRUTURA DE DADOS PROBABILÍSTICOS
REQUISIÇÃO DE DEVOLUÇÃO DE DIREITOS
BF1
AUTENTICAR
RECUPERAÇÃO DE DESCRIÇÃO DE REEMBOLSO
REC. DE DEVOLUÇÃO DE DIREITOS
PEDIR CONSENTIMENTO DO USUÁRIO
O USUÁRIO CONCORDA
ENCRIPTAR
ENVIAR PACOTE DE DADOS
ENCR
REC. DE PACOTE DE DADOS
APAGAR OGD
SEGUNDA ESTRUTURA DE DADOS PROBABILÍSTICOS
318
ENVIAR
BF2
ENCR
RETORNAR PACOTE DE DADOS
501
CHAVE
502
DESTRAVAR PACOTE DE DADOS
503
NOTIFICAÇÃO P/ USUÁRIO - REEMBOLSO
504
FECHAR CONEXÃO
OGD = OBJETO DE GERENCIAMENTO DE DIREITOS
REC. = RECONHECIMENTO
BF1 = PRIMEIRO FILTRO DE BLOOM
BF2 = SEGUNDO FILTRO DE BLOOM
ENCR = ENCRIPTAÇÃO

FIG. 5

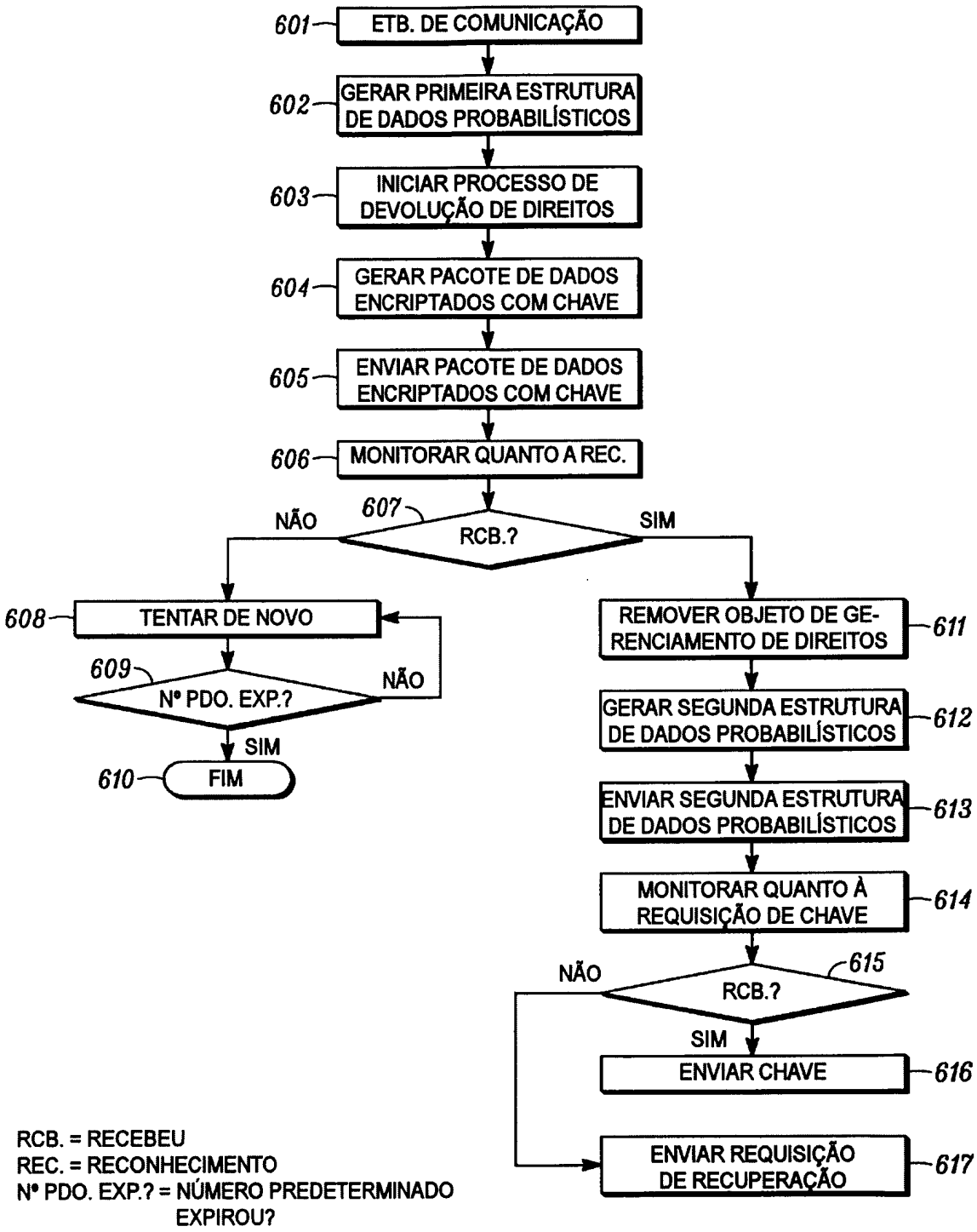
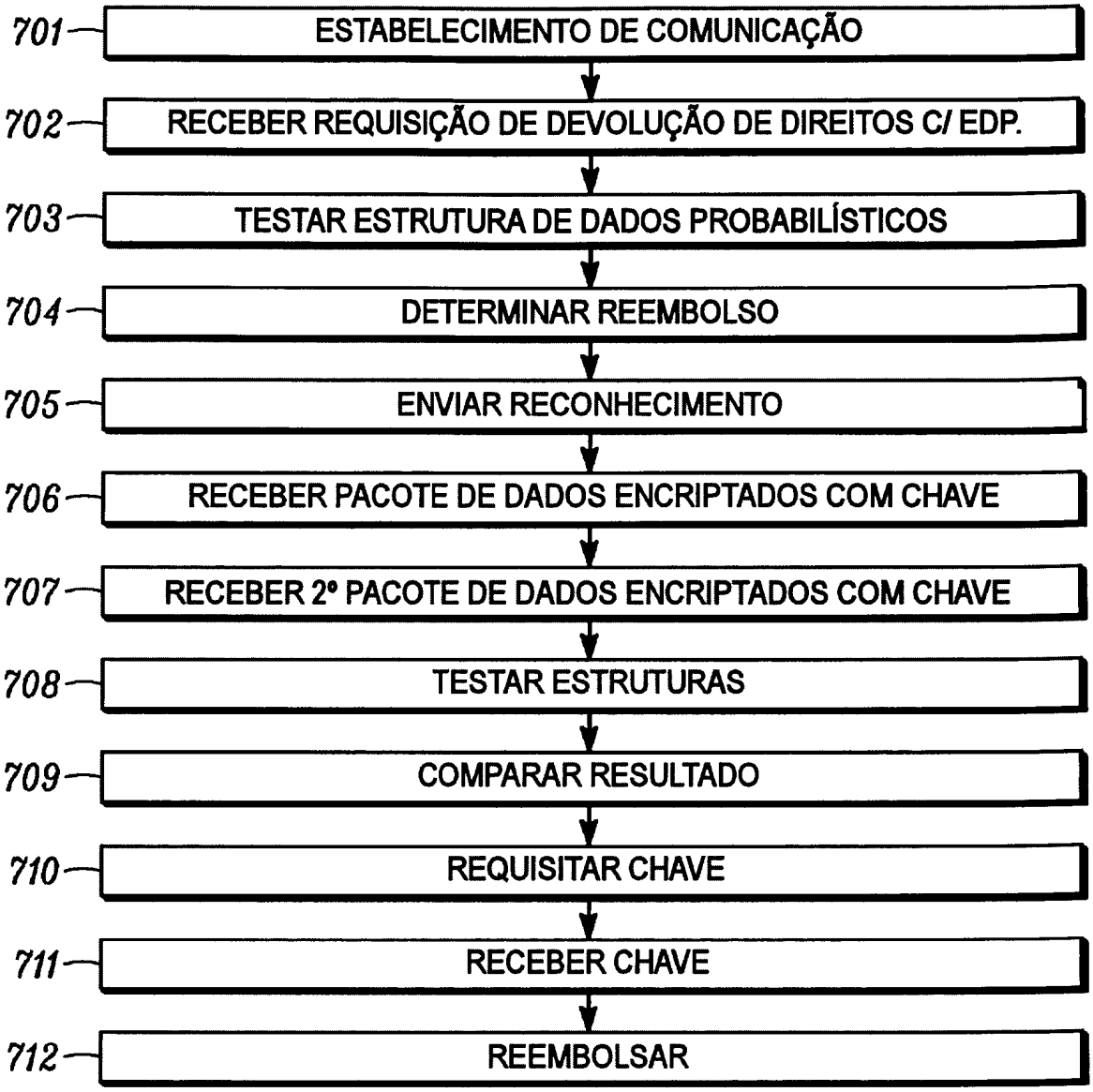

601
ETB. DE COMUNICAÇÃO
602
GERAR PRIMEIRA ESTRUTURA DE DADOS PROBABILÍSTICOS
603
INICIAR PROCESSO DE DEVOLUÇÃO DE DIREITOS
604
GERAR PACOTE DE DADOS ENCRIPTADOS COM CHAVE
605
ENVIAR PACOTE DE DADOS ENCRIPTADOS COM CHAVE
606
MONITORAR QUANTO A REC.
607
RCB.?
NÃO
SIM
608
TENTAR DE NOVO
609
Nº PDO. EXP.?
NÃO
SIM
610
FIM
REMOVER OBJETO DE GERENCIAMENTO DE DIREITOS
611
GERAR SEGUNDA ESTRUTURA DE DADOS PROBABILÍSTICOS
612
ENVIAR SEGUNDA ESTRUTURA DE DADOS PROBABILÍSTICOS
613
MONITORAR QUANTO À REQUISIÇÃO DE CHAVE
614
615
RCB.?
NÃO
SIM
ENVIAR CHAVE
616
ENVIAR REQUISIÇÃO DE RECUPERAÇÃO
617
RCB. = RECEBEU
REC. = RECONHECIMENTO
Nº PDO. EXP.? = NÚMERO PREDETERMINADO EXPIROU?

FIG. 6



EDP. = ESTRUTURA DE DADOS PROBABILÍSTICOS

FIG. 7

RESUMO

MÉTODO E APARELHO PARA EFETUAR A DEVOLUÇÃO DE UM OBJETO DE GERENCIAMENTO DE DIREITOS

Um sistema e um método para devolução de um objeto de gerenciamento de direitos (103) para um emissor de direitos (102) são providos. O sistema e o método permitem que o emissor de direitos (102) se assegure que o objeto de gerenciamento de direitos (103) seja removido de um dispositivo eletrônico (101) antes da feitura do reembolso, enquanto se provê ao consumidor a capacidade de recuperação o objeto de gerenciamento de direitos (103), quando a devolução for mal sucedida. Após a iniciação de uma devolução, um dispositivo eletrônico (101) transmite estruturas de dados probabilísticos (226, 228) para o emissor de direitos (102). As estruturas de dados probabilísticos (226, 228) têm índices ali de objetos de gerenciamento de direitos dispostos dentro do dispositivo eletrônico (101). O dispositivo eletrônico (101) encripta o objeto de gerenciamento de direitos (103), envia-o para o emissor de direitos (102), e o remove do dispositivo eletrônico (101). Ao consultar as estruturas de dados probabilísticos (226, 228), as quais podem ser filtros de Bloom, o emissor de direitos (102) é capaz de confirmar que o objeto de gerenciamento de direitos (103) foi apagado do dispositivo eletrônico (101).