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

(21) **PI0711042-1 A2**

BRPI0711042A2

(22) Data de Depósito: 25/04/2007
(43) Data da Publicação: 23/08/2011
(RPI 2120)

(51) Int.Cl.:
G06F 21/00 2006.01

(54) Título: **MÉTODO PARA POSSIBILITAR QUE UMA ENTIDADE CRIE UM OBJETO QUE PODE SER AUTENTICADO E/OU DESCRIPTOGRAFADO USANDO UMA CHAVE DE DOMÍNIO COMUM, SISTEMA, E, DISPOSITIVO**

(30) Prioridade Unionista: 02/05/2006 EP 06113373.2

(73) Titular(es): Koninklijke Philips Eletronics N. V., Stichting Telematica Instituut, Vodafone Libertel N.V.

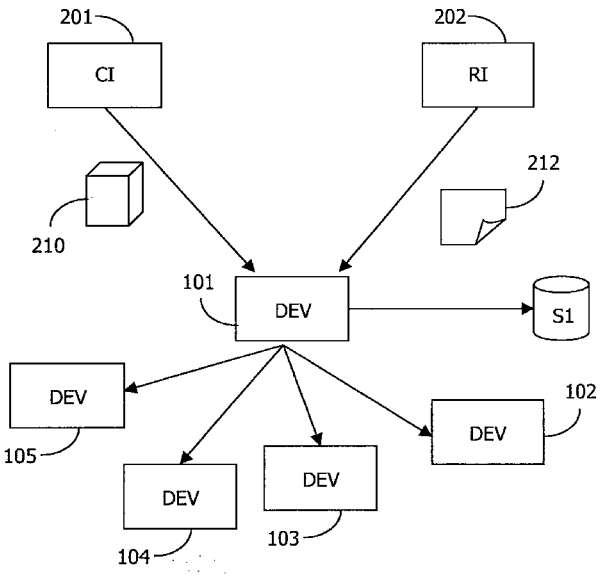
(72) Inventor(es): Javier Montaner, Najib Koraichi, Robert P. Koster, Sorin M. Iacob

(74) Procurador(es): Momsen, Leonardos & CIA.

(86) Pedido Internacional: PCT IB2007051533 de 25/04/2007

(87) Publicação Internacional: WO WO2007/125486de 08/11/2007

(57) Resumo: METODO PARA POSSIBILITAR QUE UMA ENTIDADE CRIE UM OBJETO QUE PODE SER AUTENTICADO E/OU DESCRIPTOGRAFADO USANDO UMA CHAVE DE DOMINIO COMUM, SISTEMA, E, DISPOSITIVO Em um domínio compreendendo uma pluralidade de dispositivos, os dispositivos no domínio compartilhando uma chave de domínio comum,um método para possibilitar uma entidade que não é um membro do domínio criar um objeto que pode ser autenticado e/ou ser descriptografado usando a chave de domínio comum, o método compreendendo fornecer para a entidade que não é um membro do domínio uma chave diversificada que é derivada usando uma função unidirecional a partir de pelo menos a chave de domínio comum para criar dados de autenticação relacionados ao mencionado objeto e/ou para criptografar o mencionado objeto, os dispositivos no domínio sendo configurados para autenticar e/ou descriptografar o mencionado objeto usando a chave diversificada.



"MÉTODO PARA POSSIBILITAR QUE UMA ENTIDADE CRIE UM OBJETO QUE PODE SER AUTENTICADO E/OU DESCRIPTOGRAFADO USANDO UMA CHAVE DE DOMÍNIO COMUM, SISTEMA, E, DISPOSITIVO"

FUNDAMENTOS DA INVENÇÃO

Nos anos recentes, o número de sistemas de proteção de conteúdo disponíveis tem aumentado rapidamente. Alguns desses sistemas somente protegem o conteúdo contra cópia não autorizada, enquanto outros restringem a habilidade do usuário para acesso ou uso do conteúdo. Esses sistemas são freqüentemente referidos como sistemas de Gerenciamento de Direitos Digitais (DRM).

Consumidores querem desfrutar do conteúdo sem entraves e com poucas limitações tanto quanto possível. Eles querem colocar em rede seus dispositivos para possibilitar todos os tipos de diferentes aplicações e acessar de modo fácil qualquer tipo de conteúdo. Eles também querem ser capazes de compartilhar/transferir conteúdo em seu ambiente doméstico sem limitações.

O conceito de Domínios Autorizados (ADs) tenta encontrar uma solução para ambos, servir aos interesses dos proprietários de conteúdo (que querem proteção de seus direitos autorais) e dos consumidores de conteúdo (que querem uso não restrito do conteúdo). O princípio básico é ter um ambiente de rede controlado no qual o conteúdo possa ser usado relativamente de modo livre enquanto não cruzar a fronteira do domínio autorizado. Tipicamente, domínios autorizados são centrados em torno do ambiente doméstico, também referido como redes domésticas.

É claro que, outros contextos são também possíveis. Um usuário poderia, por exemplo, pegar um dispositivo portátil para áudio e/ou vídeo com uma quantidade limitada de conteúdo com ele em uma faixa, e usá-lo em seu quarto de hotel para acessar ou baixar conteúdo adicional

armazenado em seu sistema pessoal de áudio e/ou vídeo em casa. Mesmo embora o dispositivo portátil esteja fora da rede doméstica , ele é uma parte do domínio autorizado do usuário. Desta maneira, um Domínio Autorizado (AD) é um sistema que permite acesso ao conteúdo através dos dispositivos no domínio, mas não através de qualquer outros.

Domínios autorizados necessitam endereçar questões tais como identificação de domínio autorizados, dispositivo de verificação de entrada, dispositivo de verificação de saída, direitos de verificação de entrada, direitos de verificação de saída, conteúdo de verificação de entrada, conteúdo de verificação de saída, assim como gerenciamento de domínio. Para uma introdução mais extensa para o uso de um domínio autorizado, etc., ver S.A.F.A. van den Heuvel, W. Jonker, F.L.A.J. Kamperman, P.J. Lenoir, Secure Content Management in Authorised Domains, Philips Research, The Netherlands, IBC 2002 publicação de conferência, páginas 467- 474, ocorrida em 12-16 September 2002.

Em certas arquiteturas para Domínios Autorizados, as entidades, e. g. dispositivos, no domínio compartilham uma chave de domínio simétrica que é usada, entre outras coisas, para criar, acessar e/ou autenticar objetos tal como conteúdo ou licenças (diretos de objetos) que estão disponíveis no domínio. Um exemplo é a versão 2 da Open Mobile Alliance's DRM Architeture : Approved Version 2.0, OMA-AD-DRM-V2 0-20060303-A, 03 Mar 2006, daqui em diante chamado OMA DRM v2 de forma abreviada. Este documento está disponível na Internet em member.openmobilealliance.org/ftp/public_documentos/bac/DLDRM/Permanent_documents/ e é incorporado para referência no presente documento. Um outro exemplo é WO 2005/088896 (certificado de procuração PHNL040288).

Em tais arquiteturas, a chave de domínio não pode se tornar disponível para entidades não membros já que as possibilitariam ter acesso a objetos protegidos mesmo embora eles não sejam membros do domínio.

Ainda, é desejável que certas entidades não membros sejam habilitadas a criar objetos para uso através das entidades no domínio. Alguém poderia é claro emitir essas chaves diferentes para as entidades não membros, mas que requer que cada dispositivo em cada domínio mantenha cópias de todas essas chaves.

SUMÁRIO DA INVENÇÃO

Um objeto da invenção é habilitar uma entidade que não é um membro de um domínio autorizado para criar objetos que são usáveis pelos membros do domínio autorizado, sem prover aquela entidade com o chave do domínio.

Este objeto é alcançado em um método como reivindicado na reivindicação 1. Através do fornecimento ao dispositivo ou outra entidade que não é membro do domínio, a chave diversificada que é derivada usando uma função unidirecional a partir de uma chave de domínio comum, se torna possível para este dispositivo criar dados de autenticação relacionados a esses objetos e/ou para criptografar esses objetos usando a chave diversificada. Os dispositivos no domínio podem criar a chave diversificada quando necessário para derivá-la usando a função unidirecional só a partir da chave de domínio, que está disponível para eles. Eles podem então usar a chave diversificada para autenticar e/ou descriptografar os objetos recebidos da entidade não membro.

De acordo com a invenção, a entidade não membro não tem acesso à chave do domínio, ainda é capaz para criar objetos que podem ser autenticados e/ou descriptografados através dos dispositivos no domínio. Isto fornece melhor controle no qual as entidades podem emitir tais objetos, tal como OMA DRM Objeto de Direitos, para o domínio.

De forma preferencial, a chave diversificada é derivada usando a função unidirecional só a partir da chave de domínio comum e a partir da representação de uma identidade da entidade que não é um membro do domínio. Isto tem a vantagem que diferentes entidades diferentes recebem

chaves diversificadas diferentes.

Em uma modalidade preferida, a função unidirecional só compreende uma função de cálculo de valor numérico criptográfica chaveada. Como entrada nesta função alguém pode usar a representação de uma identidade da entidade que não é um membro do domínio, tal como uma chave pública associada com o dispositivo. Quando o algoritmo de autenticação ou de criptografia requer que as chaves sejam de um comprimento específico, alguém pode truncar a saída da função unidirecional só par ao número requerido de bits. Por exemplo, quando usando uma chave diversificada com o algoritmo de criptografia de AES usando chaves de 128 bit, a chave gerada usando a função de cálculo de valor numérico de um sentido só SHA-I deve ser truncada a partir de 160 à 128 bits.

Em uma modalidade preferida, a entidade não membro é um Emissor de Direitos configurada para emitir direitos digitais associados com itens de conteúdo. Nesta modalidade os objetos, compreendendo os direitos digitais são descriptografados usando as chaves diversificadas.

Em uma modalidade o método ainda compreende criar um indicador de validação assinado de modo digital compreendendo a representação de uma identidade da entidade que não é um membro do domínio.

Em ainda uma modalidade o método compreende criar um código de autenticação de mensagem para os objetos fornecidos através da entidade que não é um membro do domínio usando a chave de domínio comum. Dispositivos que recebem tal um objeto a partir de um outro dispositivo agora também requer a presença de um código de autenticação de mensagem. Isto previne a entidade não membro de gerar objetos válidos para um domínio particular e tornar aquele disponível através de diferentes canais.

A invenção ainda fornece um sistema e dispositivo para executar o método.

Outras modalidades vantajosas são configuradas nas reivindicações dependentes.

DESCRIÇÃO BREVE DAS FIIGURAS

Esses e outros aspectos da invenção será aparente e elucidada com referência às modalidades ilustrativas mostradas nos desenhos, nos quais:

Fig. 1, de forma esquemática, mostra um sistema compreendendo os dispositivos interconectados através de uma rede;

Fig. 2 mostra um diagrama de arquitetura esquemático de acordo com o padrão de OMA DRM v2, e

Fig. 3 mostra um diagrama de arquitetura esquemático de acordo com a invenção, compreendendo um Emissor de Domínio separado e múltiplos Emissores de Direitos.

Do começo ao fim das figuras, mesmos numerais de referência indicam características similares ou correspondentes. Algumas das características indicadas nos desenhos são tipicamente implementadas em software, e como tal representam entidades de software, tal como módulos ou objetos de software.

DESCRIÇÃO DETALHADA DE CERTAS MODALIDADES

Fig. 1, de forma esquemática, mostra um sistema 100 compreendendo os dispositivos 101-105 interconectados através de uma rede 110. Uma típica rede doméstica digital inclui um número de dispositivos, e. g. um rádio receptor de rádio, um sintonizador/decodificador, um tocador de CD, um par de alto-falantes, uma televisão, um VCR, um gravador digital, um telefone móvel, um toca fita, um computador pessoal, um assistente digital pessoal, uma unidade de exibição portátil, um sistema de entretenimento de carro, e assim por diante. Esses dispositivos são usualmente interconectados para permitir um dispositivo, e. g. a televisão, controla um ao outro, e. g. o VCR. Em algumas modalidades, um dispositivo, tal como e. g. o sintonizador/decodificador ou uma caixa de topo de aparelho (STB), opera

como dispositivo central, fornece controle central sobre os outros.

O conteúdo, que tipicamente compreendem coisas como, música, canções, filmes, animações, falas, videoclipes para musica, programas de TV, figuras, jogos, tons de campainha, livros falados e o similar, mas que também pode incluir serviços interativos, é recebido através de diferentes fontes, tal como uma rede de cabo de banda larga, uma conexão de Internet, um elo de comunicação de descida de satélite, redes de telefone móvel, mídia de armazenamento como discos ou dispositivos portáteis. O conteúdo pode então ser transferido através da rede 110 para um recipiente para representação. Um recipiente pode ser, por exemplo, o visor de televisão 102, o dispositivo de exibição portátil 103, o telefone móvel 104 e/ou o dispositivo de reprodução de áudio 105.

A maneira exata na qual um item de conteúdo item é representado depende do tipo do dispositivo e do tipo do conteúdo. Por exemplo, um receptor de rádio, representação compreende gerar sinais de áudio e alimentá-los aos alto-falantes. Para um receptor de televisão, representação de modo geral, compreende gerar sinais de áudio e vídeo e alimentá-los a uma tela de exibição e alto-falantes. Para outros tipos de conteúdo uma ação apropriada similar precisa ser tomada. Representação pode também incluir operações tal como descriptografar ou desembaralhar um sinal recebido, sincronizar os sinais de áudio e vídeo e assim por diante.

A caixa de topo de aparelho 101, ou qualquer outro dispositivo no sistema 100, pode compreender um meio de armazenamento S1 tal como um, de forma adequada, disco rígido grande, permitindo a gravação e reprodução posterior do conteúdo recebido. Um meio de armazenamento S1 poderia ser um Gravador Digital Pessoal (PDR) de algum tipo, por exemplo, um gravador de DVD+RW, ao qual o conjunto de caixa de topo 101 é conectado. O conteúdo pode também entrar no sistema 100 armazenado em um portador 120 tal como um Disco Compacto (CD) ou disco Versátil Digital

(DVD).

O dispositivo de exibição portátil 103 e o telefone móvel 104 são conectados por meio de fio à rede 110 usando uma estação base 111, por exemplo, usando Bluetooth ou IEEE 802.1 Ib. Os outros dispositivos são conectados usando uma conexão com fio convencional. Para permitir os dispositivos 101-105 interagirem, vários padrões de interoperabilidade estão disponíveis, que permitem aos diferentes dispositivos trocar mensagens e informação e controlar cada um ao outro. Um padrão bem conhecido é o padrão Universal Plug e Play (http://www.upnp.org).

O sistema 100 é configurado para gerenciar o acesso ao conteúdo operando como um Domínio Autorizado (AD), preferencialmente de acordo com o padrão OMA DRM v2 padrão ou um sucessor dele. Fig. 2 mostra um diagrama de arquitetura esquemático de acordo com o padrão OMA DRM v2.

Na Fig. 2, um Emissor de Conteúdo (CI) 201 torna o conteúdo 210 disponível na forma protegida (" Conteúdo de DRM " na terminologia OMA) para os dispositivos no AD, aqui para o dispositivo 101. Para acessar o conteúdo 210, o dispositivo 101 necessita de um Objeto de Direitos (RO) 212 que é fornecido por um Emissor de Direitos (RI) 202. O aprovisionamento do RO 212 pode ocorrer, de forma simultânea, com o aprovisionamento do Conteúdo de DRM 210, mas isto não é necessário. Por exemplo, alguém pode obter conteúdo em um certo tempo e depois adquirir um RO para acessar aquele conteúdo. De modo alternativo alguém pode obter um RO e somente mais tarde obter o conteúdo ao qual o RO se aplica.

Em OMA DRM, um RO é um documento XML especificando permissões e restrições associadas com um pedaço do Conteúdo de DRM. O Conteúdo de DRM não pode ser usado sem um RO associado, e pode somente ser usado de acordo com as permissões e restrições especificadas em um RO. Os ROs contêm as expressões e chaves de direito necessárias para representar

o conteúdo efetivo. A aquisição de RO, registro de dispositivo, e gerenciamento de domínio são especificados por meio de um conjunto de protocolos chamado ROAP.

Cada um dos dispositivos 101-105 tem um Agente de DRM, usualmente incorporado como um componente de software sendo executado no dispositivo em questão. O Agente de DRM assegura que as permissões e restrições especificadas em um RO são aderidas. Um Objeto de Direitos é amarrado por criptografia a um Agente de DRM específico, então somente aquele Agente de DRM pode usá-lo.

O Conteúdo de DRM 210 pode ser distribuído livremente entre os dispositivos 101-105 e pode também ser armazenado, e. g. no meio de armazenamento S1, ou ser distribuído para outro partes. Contudo, sem um RO válido, o Conteúdo de DRM 210 não pode ser acessado. Se o dispositivo 105 estava para adquirir uma cópia do Conteúdo de DRM 210, por exemplo, ele ainda teria de obter um RO que é amarrado a seu Agente de DRM. O RO 212 é somente usável pelo Agente de DRM do dispositivo 101.

Para criar acesso com base no domínio ao conteúdo, OMA DRM também permite a criação e distribuição de Objeto de Direitos que são amarrados a um grupo de Agente de DRMs, mais propriamente do que um único agente. Tal um grupo é referido como um domínio, e Objeto de Direitos amarrados a um domínio são referidos como Objeto de Direitos do domínio. Para se juntar ao domínio, primeiro dispositivo 101 precisa perguntar ao Emissor de Direitos 202 se ele é permitido se juntar a um domínio. Se o dispositivo 101 é permitido se juntar, o RI 202 vai fornecer o dispositivo 101 com um Contexto de Domínio (DC). O DC contém as chaves do domínio que pode ser usado para descriptografar o Objeto de Direitos do domínio. Ver seção 6.4 da especificação do OMA DRM v2 para detalhes.

As especificações de OMA DRM ainda definem o formato e o mecanismo de proteção para o Conteúdo de DRM, o formato (linguagem de

expressão) e o mecanismo de proteção para os Objeto de Direitos, e o modelo de segurança para gerenciamento chaves de criptografia. As especificações de OMA DRM também definem como o Conteúdo de DRM e Objetos de Direitos podem ser transportados para dispositivos usando uma gama de mecanismos de transporte , incluindo puxar (HTTP Pull, OMA Download), empurrar (WAP Push, MMS) e dar seqüência. Transporte de RO usa um protocolo de 1 passo ou de 2 passos chamado Protocolo de Aquisição de Objeto de Direitos (ROAP) que é executado entre um RI e um Agente de Usuário de DRM. De modo alternativo, o transporte de RO pode ser efetuado sem executar o ROAP entre dois Agentes de Usuários de DRM ou entre um RI e Agente de Usuário de DRM.

Note que o Emissor de Conteúdo 201 e o Emissor de Direitos 202 podem ser um e a mesma entidade. Na terminologia de OMA esta entidade é então referida como um distribuidor de conteúdo.

Os inventores da presente invenção realizaram que há uma necessidade para a separação funcional de Emissão de Direitos e Gerenciamento de Domínio na solução de OMA. Um principal empecilho da arquitetura descrita acima é que os domínios não podem ser facilmente compartilhados ou usados entre diferentes RIs.

De acordo com a presente invenção, um Emissor de Domínio (DI) separado é introduzido. Dispositivos que querem se juntar a um domínio agora contatam o DI em vez de um RI. Como um resultado, múltiplos RIs podem agora ser usados para fornecer ROs do domínio para o mesmo domínio. Isto é ilustrado, de forma esquemática, na Fig. 3. Dois RIs 202a, 202b são fornecidos, ambos emitindo ROs do domínio 212a, 212b para o dispositivo 101. Em adição um Emissor de Domínio (DI) 301 gerencia que dispositivos se juntam e deixam o domínio.

A chave do domínio, daqui em diante abreviada como K_D, é agora fornecido pelo DI 301 em vez do RI 202 para os dispositivos 101-105.

Os RIs 202a, 202b não mais tem acesso à chave do domínio. Isto vai significar que eles não podem mais emitir Objeto de Direitos do domínio para os dispositivos 101-105 já que de acordo com OMA DRM v2, os Objeto de Direitos de domínio precisam ser protegidos usando a chave do domínio.

De acordo com a invenção, cada RI emite sua própria Chave Diversificada, daqui em diante abreviada como K_{Di} onde i é o identificador do RI para quem uma chave diversificada K_{Di} é emitida. A chave diversificada é derivada da chave do domínio, preferencialmente em conjunto com a identidade do Emissor de Direitos em questão.

Em uma modalidade preferida, a chave diversificada é criada computando o código de autenticação de mensagem de cálculo de valor numérico (HMAC) chaveado de uma representação da identidade, preferencialmente uma chave pública, do Emissor de Direitos usando uma chave de domínio como uma chave secreta. De forma preferencial a função de cálculo de valor numérico criptográfica SHA1 é usada, embora muitas outras funções de cálculo de valor numérico também poderiam ser usadas. O valor numérico chaveado computado é preferencialmente truncado para reter somente os primeiros 128 bits, os quais 128 bits então servem como uma chave diversificada.

De forma alternativa, uma função de cálculo de valor numérico criptográfica pode ser usada para computar um valor numérico da chave do domínio, o qual valor numérico então serve como uma chave diversificada. De novo o valor numérico pode ser truncado se necessário. Preferencialmente a entrada da função de cálculo de valor numérico criptográfica não é somente uma chave de domínio mas também uma representação da identidade, Preferencialmente a chave pública, do Emissor de Direitos. Esta modalidade preferida fornece diferentes RIs com diferentes chaves. Por exemplo, alguém pode calcular a concatenação da Chave de Domínio e da chave pública.

Em uma outra modalidade a chave K_{Di} é obtida como uma criptografia de uma representação da identidade do RI usando a chave de domínio DK como chave de criptografia . A representação da identidade do RI pode ser criada em diferentes maneiras, dependendo em que tipo de nomes, números seriais, etc. são usados dentro da implementação de sistema de DRM. Por exemplo, o DM pode designar a cada RI que pode se comunicar com o domínio, um rótulo de identificação único Lbi que é exatamente de comprimento de 128 bits (16 bytes). Isto poderia ser uma número de séria de certificado. Se os rótulos são mais curtos do que 16 bytes, então o DM deve preencher antecipadamente cada rótulo com 0 bits, até 16 bytes, para formar o Lbi .

Uma opção para criar a Chave Diversificada agora é uma criptografia de AES deste rótulo Lbi usando a Chave de Domínio DK como a chave de criptografia. Uma vantagem desta é que é muito simples, e as chaves resultantes são garantidas para serem únicas.

Se cada RI tem um, de forma arbitrária, nome único e escolhido, então tal nome poderia ser preenchido para criar um seqüência do comprimento do direito. Técnicas padrão para preenchimento estão disponíveis, ver e. g. ISO/IEC padrão 9797. Uma opção preferida é a seguinte. Primeiro preenche o nome com um bloco que tem comprimento de 128 bits e que é a representação binária do (não preenchido) comprimento do nome em bits. Então preencher a posterior o resultado com bits de valor " 0 " até a mensagem completa alcançar um comprimento múltiplo de 128 bits. No resultado pode ser feito a criptografia usando AES com a Chave de Domínio DK como a chave de criptografia. Isto tem a vantagem que de forma arbitrária, nomes escolhidos podem ser usados pelo RI.

Muitas opções alternativas podem ser pensadas. Vários exemplos serão agora dados. Na maioria das circunstâncias, uma função de MAC chaveada pode ser aplicada em vez de criptografar usando a Chave de

Domínio DK como chave.

Para obter sua Chave Diversificada K_{Di}, o Emissor de Direitos em uma modalidade preferida emite uma solicitação para o Emissor de Domínio. Se o Emissor de Direitos é para ser permitido emitir ROs para dispositivos no domínio em questão, o Emissor de Domínio emite uma resposta compreendendo o contexto relevante. Este contexto compreende a Chave Diversificada para o Emissor de Direitos e preferencialmente, também identificadores para o Emissor de Domínio, o próprio domínio, um tempo de validade expirada (expresso como ponto no tempo ou duração a partir de um tempo corrente) e preferencialmente um Indicador de validação de RI, elaborado abaixo. O tempo de expiração e o Indicador de validação pode tomar a forma de um certificado X.509v3 de uma chave pública para o Emissor de Direitos que foi gerado usando a chave privada para o Emissor de Domínio.

O Emissor de Direitos pode agora gerar Objetos de Direito se usar a Chave Diversificada para criptografar esses ROs. Isto é o mesmo que como com o padrão OMA DRM v2, exceto que agora a Chave Diversificada é usada em vez da Chave de Domínio.

Quando um dispositivo no domínio adquire um RO de domínio a partir de um Emissor de Direitos, ele constrói a Chave Diversificada para este Emissor de Direitos e usa aquela Chave Diversificada para descriptografar o RO de domínio. Para este fim, o dispositivo repete o processo como indicado acima para o Emissor de Domínio.

Em uma modalidade, o Emissor de Domínio cria um Indicador de validação de RI que permite ao RI provar que é permitido emitir Rostos de domínio para os dispositivos no domínio em questão. O indicador de validação compreende a identidade, e. g. uma chave pública, do Emissor de Direitos e preferencialmente também uma indicação de quanto tempo o indicador vai permanecer válido, e. g. indicando um data de expiração. O

indicador de validação deve ser assinado digitalmente pelo DI tal que sua autenticidade pode ser verificada.

Nesta modalidade o dispositivo pode usar um indicador de validação de RI para obter a identidade, i. e. a chave pública, do Emissor de Direitos. É claro que o dispositivo não deve usar o indicador de validação de RI se a assinatura digital não pode ser verificada com sucesso, ou se o indicador não é mais válido, e. g. se o tempo corrente está além da data de expiração indicada.

De acordo com OMA DRM v2, um Emissor de Direitos e um dispositivo devem executar um protocolo de Registro de RI antes que o dispositivo possa aceitar ROs proveniente do Emissor de Direitos. Um benefício da presente invenção é que este não é mais um requisito. Um dispositivo no domínio pode também obter ROs do domínio a partir de um outro dispositivo no domínio, e no qual caso não necessita para registrar a si próprio com o RI que originalmente gerou aquele RO do domínio .

Em certos intervalos a chave de domínio pode ser substituída com uma nova chave do domínio. Nesta ocasião o Emissor de Domínio deve também gerar novas Chaves Diversificadas para todos os Emissores de Direitos que emitiram Chaves Diversificadas derivadas a partir da chave do domínio anterior. O Emissor de Domínio deve então preferencialmente fornecer essas novas Chaves Diversificadas para esses Emissores de Direitos automaticamente. Alternativamente elas podem ser fornecidas quando solicitadas.

Em vez de criptografar os ROs com as Chaves Diversificadas, as Chaves Diversificadas também podem ser usadas para criar e verificar os dados de autenticação associados com os Objeto de Direitos. Alguém pode e. g. usar a chave diversificada como chave para uma função de cálculo de valor numérico chaveada ou função de código de autenticação de mensagem a ser aplicada ao Objeto de Direitos. A saída desta função então serve para

autenticar o Objeto de Direitos.

É desejável prevenir RIs de gerarem ROs do domínio válidos para um particular domínio sem se envolver em um Protocolo de Aquisição de RO (ROAP) com um dispositivo que é um membro do domínio. Para alcançar isto, em uma modalidade preferida, dispositivos no domínio, após receberem o RO durante o ROAP, computam um MAC de Dispositivo usando a Chave de Domínio principal e anexam o MAC de Dispositivo para um RO do domínio quando eles recebem tal um RO do domínio a partir de um RI. O MAC de Dispositivo assim sendo serves como prova que o RO do domínio foi adquirido a partir de um RI autorizado. Note que esta abordagem funciona também para ROs que foram produzidos usando a Chave do Domínio, mais propriamente do que a Chave Diversificada. Esta abordagem assim sendo não é restrita para ROs nos quais são feitos criptografia com as Chaves Diversificadas.

O MAC de Dispositivo pode ser computado como a MAC do RO usando a Chave de Domínio K_D como a chave. Isto permite a qualquer dispositivo no domínio estabelecer a autenticidade do dispositivo MAC. O MAC de Dispositivo deve acompanhar o RO, preferencialmente o adicionando como um novo elemento de XML no RO do domínio .

Nesta modalidade o MAC de Dispositivo é requerido para subseqüente troca de Dispositivo - RO de Dispositivo e instalação no dispositivo de destinação. Quando um dispositivo recebe um RO do domínio, este dispositivo precisa primeiro validar o MAC de Dispositivo antes de aceitar e/ou instalar o RO do domínio no dispositivo.

Note que uma vez que a Chave de Domínio K_D muda, o MAC de Dispositivo pode não mais ser validado usando a nova Chave do Domínio. E um RO do domínio sem um MAC de Dispositivo anexado válido deve preferencialmente ser rejeitado pelos dispositivos no domínio. De forma alternativa, um dispositivo que aceitou e instalou um RO do domínio com um

MAC de Dispositivo válido pode re-computar o MAC de Dispositivo usando a nova Chave do Domínio.

A segurança da solução proposta acima é baseada na suposição que a Chave de Domínio K_D é somente conhecida pelos dispositivos que são membro do domínio e do Emissor de Domínio. Contudo, se a Chave de Domínio K_D de alguma forma se torna disponível para uma terceira parte não autorizada, se torna possível para um RI emitir ROs do domínio mesmo após sua autorização para fazer isso tenha expirada.

Para resolver este problema, um dispositivo que gera um MAC de Dispositivo deve gerar uma assinatura digital usando sua chave privada para este MAC de Dispositivo. Esta assinatura, DeviceSign, será distribuído junto com o RO do domínio e o MAC de Dispositivo. O DeviceSign permite outros dispositivos no domínio para identificar o dispositivo que recebeu o RO do domínio a partir do RI.

De forma subseqüente, se a Chave de Domínio K_D se torna compromissada e ROs não autorizados são emitidos, o domínio dispositivo que aceita esses ROs podem ser identificados. Este dispositivo então provavelmente age em conivência com o RI não autorizado. O dispositivo em questão pode de forma subseqüente ser revogado, por exemplo, adicionando seu identificador de dispositivo a uma lista de revogação de dispositivo (DRL) que é distribuída para todos os dispositivos no domínio. Dispositivos compatíveis somente aceitam e instalam ROs do domínio que incluem o DeviceSign apropriado gerado por um dispositivo que não está incluído no DRL.

Para suportar o acima, o Emissor de Domínio em uma modalidade preferida gera um objeto assinado que informa a cada dispositivo no domínio que um particular dispositivo, daqui em diante dispositivo$_x$, é permitido criar assinaturas de DeviceSign. O indicador contém a chave pública do dispositivo$_x$ e é assinado pelo DI tal que ele pode ser validado por

qualquer dispositivo membro do domínio. Preferencialmente o indicador é tornado disponível para dispositivo$_x$ tal que este dispositivo pode distribuí-lo para outros dispositivos.

Nesta modalidade, quando um dispositivo recebe um RO do domínio, ele necessita efetuar a validação do DeviceSign e do indicador para dispositivo$_x$ em adição a outros passos já discutidos.

Nesta modalidade ainda cada dispositivo no domínio tem acesso a uma lista de revogação de dispositivo, DRL para dispositivos no domínio. Esta DRL pode ser armazenada nos dispositivos ou e. g. ser acessível através de uma rede. A DRL é preferencialmente realizada como um lista negra, listando os dispositivos cujas DeviceSign não devem ser aceitas. Alternativamente a DRL pode ser realizada como uma lista branca listando somente os dispositivos cujas DeviceSign devem se aceitas.

A invenção também pode ser usada para proteger e/ou autenticar outros objetos do que Objetos de Direitos. Por exemplo, ao conteúdo pode ser feito criptografia usando as Chaves Diversificadas.

A invenção não é apenas aplicável para domínios de acordo com OMA DRM. Várias proposições existem que implementam o conceito de domínios autorizados par alguma extensão. Nos assim chamado ADs baseados em dispositivos, o domínio é formado por um conjunto específico de dispositivos de hardware ou aplicações de software (referido coletivamente como clientes daqui em diante) e conteúdo. Um gerenciador de domínio, que pode ser um ou mais dos clientes, um cartão inteligente ou um outro dispositivo, controla que clientes podem se juntar ao domínio. Somente o conjunto específico de clientes no domínio (os membros) é permitido fazer uso do conteúdo daquele domínio, e. g. abri-lo, copiá-lo, executá-lo ou exportá-lo. Exemplos de tais ADs baseados em dispositivos são dados no pedido de patente internacional WO 03/098931 (certificado de procuração PHNL020455), pedido de patente internacional WO 05/088896 (certificado

de procuração PHNL040288) e pedido de patente internacional WO 04/027588 (certificado de procuração PHNL030283) pelo mesmo requerente, todas as quais são aqui incorporadas para referência.

Um tipo de AD baseado em dispositivo permite um conjunto de clientes amarrados a um domínio para acessar conteúdo amarrado àquele domínio. A dupla amarração assegura que todos os membros podem acessar o conteúdo. Esta estrutura é freqüentemente estabelecida implementando as amarrações através de uma chave secreta compartilhada. Esta chave é escolhida através de um gerenciador de domínio e distribuída parta todos os membros. Quando o conteúdo é amarrado ao domínio, a licença é ligada do domínio em forma de criptografia por meio da criptografia com a chave compartilhada. De forma alternativa o conteúdo pode ser diretamente amarrado a um cliente, e os clientes permanecem amarrados ao AD.

Um outro tipo de AD é o assim chamado AD baseado em pessoas, onde o domínio é baseado em pessoas em vez de dispositivos. Um exemplo de tal um sistema é descrito no pedido de patente internacional WO 04/038568 (certificado de procuração PHNL021063) pelo mesmo requerente, incorporado aqui para referência, no qual o conteúdo é acoplado à pessoas, que então são agrupadas em um domínio.

Um assim chamado sistema Híbrido de DRM baseado em Domínio Autorizado vincula conteúdo a um grupo que pode conter dispositivos e pessoas. Este grupo é tipicamente limitado a um casa, tal que:

1. conteúdo pode ser visto em qualquer dos membros que pertencem à casa (e. g. TV na sala, TV no quarto de dormir, PC)

2. conteúdo pode ser visto por qualquer dos usuários que pertencem à casa após eles terem autenticados a si próprios em qualquer cliente (tal como uma televisão em um quarto de hotel). Tal autenticação normalmente envolve um dispositivo de autenticação de usuário tal como um cartão inteligente.

Exemplos de sistemas de AD híbridos podem ser encontrados no pedido de patente internacional WO 2005/010879 (certificado de procuração PHNL030926) e no pedido de patente internacional WO 2005/093544 (certificado de procuração PHNL040315), ambas incorporadas aqui para referência.

O número serial de pedido de patente internacional PCT/IB2005/053531 (certificado de procuração PHNL041254) descreve um método para permitir acesso a um domínio autorizado, o domínio autorizado sendo gerenciado por um gerenciador de domínio, compreendendo um passo no qual um dispositivo de autenticação de usuário, cujo dispositivo de autenticação de usuário é ligado a um dispositivo externo, declara para o gerenciador de domínio que um elo de comunicação local entre o dispositivo de autenticação de usuário e o dispositivo externo é limitado em distância, e um passo no qual o gerenciador de domínio permite ao dispositivo externo operar como um membro do domínio autorizado se a declaração é aceita como precisa.

O número serial de pedido de patente internacional PCT/IB2005/053687 (certificado de procuração PHNL041329) descreve um sistema de domínio autorizado compreendendo uma pluralidade de dispositivos incluindo pelo menos um dispositivo de recuperação, no qual o dispositivo de recuperação é configurado para recuperar informação de estado para dois ou mais dispositivos compreendidos no domínio e para distribuir a informação de estado de revogação recuperada para um ou mais dispositivos com os quais o dispositivo de recuperação está em contato.

O pedido de patente internacional WO 2004/077790 (certificado de procuração PHFR030018) descreve um sistema de telecomunicações para transmitir conteúdo de multimídia para um dispositivo de cliente. O mencionado sistema compreende um codificador para codificar dito conteúdo de multimídia em uma corrente de dados codificados. A

mencionada corrente de dados codificados é transmitida através de uma primeira conexão de rede a um servidor. O mencionado servidor é capaz de gerar metadados de dados de mídia contidos na corrente de dados codificados recebida e de criar um arquivo progressivo, no qual mencionados dados de mídia e metadados são intercalados. O mencionado arquivo progressivo é descarregado através de uma segunda conexão de rede para um dispositivo de cliente, que é capaz de iniciar reprodução do conteúdo de multimídia recebido antes do final do descarregamento, usando os dados de mídia e metadados intercalados.

Deve ser notado que as formas de realização acima mencionadas ilustram mais preferivelmente do que limitam a invenção, e que aqueles versados na técnica serão capazes de projetar muitas formas de realização alternativas sem divergir do escopo das reivindicações dependentes.

Nas reivindicações, qualquer sinal de referência colocado entre parênteses não deverá ser interpretado como limitante da reivindicação. A palavra "compreendendo" não exclui a presença dos elementos ou etapas diferentes daqueles listados em uma reivindicação. A palavra "o" ou "um" precedendo um elemento não exclui a presença de uma pluralidade de tais elementos. A invenção pode ser implementada por meio de hardware compreendendo diversos elementos distintos, e por meio de um computador programado adequadamente.

Em uma reivindicação de dispositivo enumerando diversos meios, vários desses meios podem ser abrangidos por um e o mesmo item do hardware. O mero fato que certas medidas são citadas em reivindicações dependentes mutualmente diferentes não indicam que a combinação dessas medidas não pode ser usada como vantagem.

REIVINDICAÇÕES

1. Método para possibilitar que uma entidade crie um objeto que pode ser autenticado e/ou descriptografado usando uma chave de domínio comum, em um domínio compreendendo uma pluralidade de dispositivos, os dispositivos no domínio compartilhando uma chave de domínio comum, a mencionada entidade sendo uma entidade que não é um membro do domínio, caracterizado pelo fato de compreender

- fornecer para a entidade que não é um membro do domínio uma chave diversificada que é derivada usando uma função unidirecional a partir de pelo menos uma chave de domínio comum para criar dados de autenticação relacionados ao mencionado objeto e/ou para criptografar pelo menos parte do mencionado objeto, e

- autenticar e/ou descriptografar o mencionado objeto usando a chave diversificada.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a função unidirecional compreende a função de cálculo de valor numérico criptográfica chaveada.

3. Método de acordo com a reivindicação 2, caracterizado pelo fato de que a entrada usada na função de cálculo de valor numérico criptográfica chaveada mencionada compreende uma representação de uma identidade da entidade que não é um membro do domínio e a chave usada é a chave de domínio comum.

4. Método de acordo com a reivindicação 1, caracterizado pelo fato de que uma chave diversificada é derivada truncando a saída da função unidirecional só para um pré-determinado número de bits.

5. Método de acordo com a reivindicação 1, caracterizado pelo fato de ainda compreender criar um indicador de validação assinado de forma digital compreendendo uma representação de uma identidade da entidade que não é um membro do domínio.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de ainda compreender criar um código de autenticação de mensagem para o objeto fornecido pela entidade que não é um membro do domínio usando a chave de domínio comum.

7. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os objetos compreendem direitos digitais para acessar conteúdo.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender derivar uma chave diversificada usando a função unidirecional a partir de uma chave de domínio comum e a partir de uma representação de uma identidade da entidade que não é membro do domínio.

9. Sistema, caracterizado pelo fato de que compreende um domínio compreendendo uma pluralidade de dispositivos, os dispositivos no domínio compartilhando uma chave de domínio comum, o sistema sendo configurado para possibilitar que uma entidade que não é um membro do domínio crie um objeto que pode ser autenticado e/ou descriptografado usando a chave de domínio comum compreendendo fornecer para a entidade que não é um membro do domínio uma chave diversificada que é derivada usando uma função unidirecional a partir de pelo menos uma chave de domínio comum para criar dados de autenticação relacionados ao mencionado objeto e/ou criptografar o mencionado objeto, os dispositivos no domínio sendo configurados para autenticar e/ou descriptografar o mencionado objeto usando a chave diversificada.

10. Dispositivo, caracterizado pelo fato de estar compreendido em um domínio, os dispositivos no domínio compartilhando uma chave de domínio comum, o dispositivo sendo configurado para receber um objeto de uma entidade que não é um membro do domínio, para derivar uma chave diversificada usando uma função unidirecional a partir de pelo menos uma chave de domínio comum, e para autenticar e/ou descriptografar o objeto usando a chave diversificada.

11. Dispositivo de acordo com a reivindicação 10, caracterizado pelo fato de ser configurado para computar um código de autenticação de mensagem para o objeto usando a chave de domínio comum e para distribuir o objeto para um outro dispositivo no domínio em conjunto com o código de autenticação de mensagem computado.

12. Dispositivo de acordo com a reivindicação 11, caracterizado pelo fato de ser configurado para receber uma nova chave de domínio comum, computando um novo código de autenticação de mensagem para o objeto usando a nova chave de domínio comum e distribuindo o objeto para um outro dispositivo no domínio em conjunto com o código de autenticação de mensagem computado.

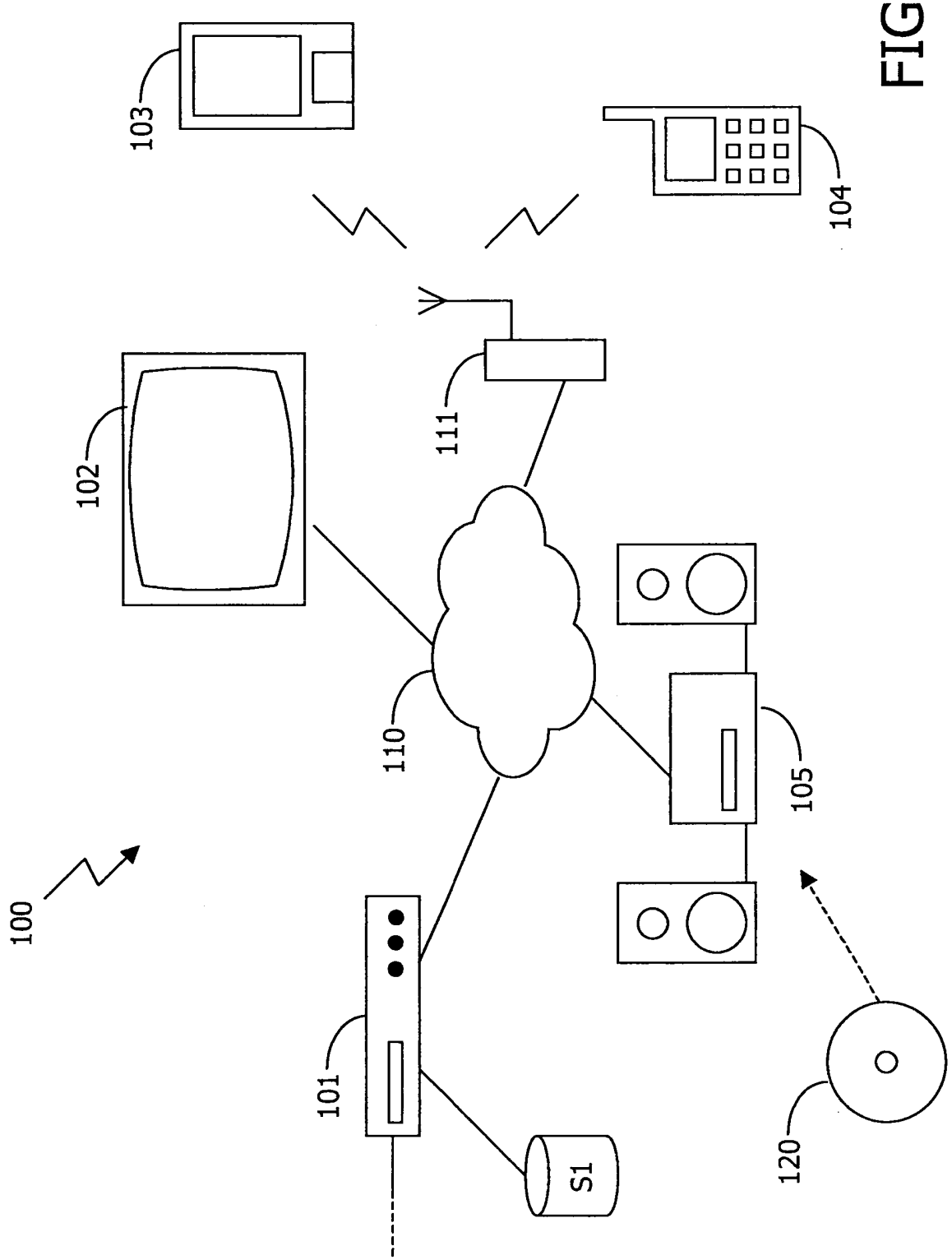


FIG. 1

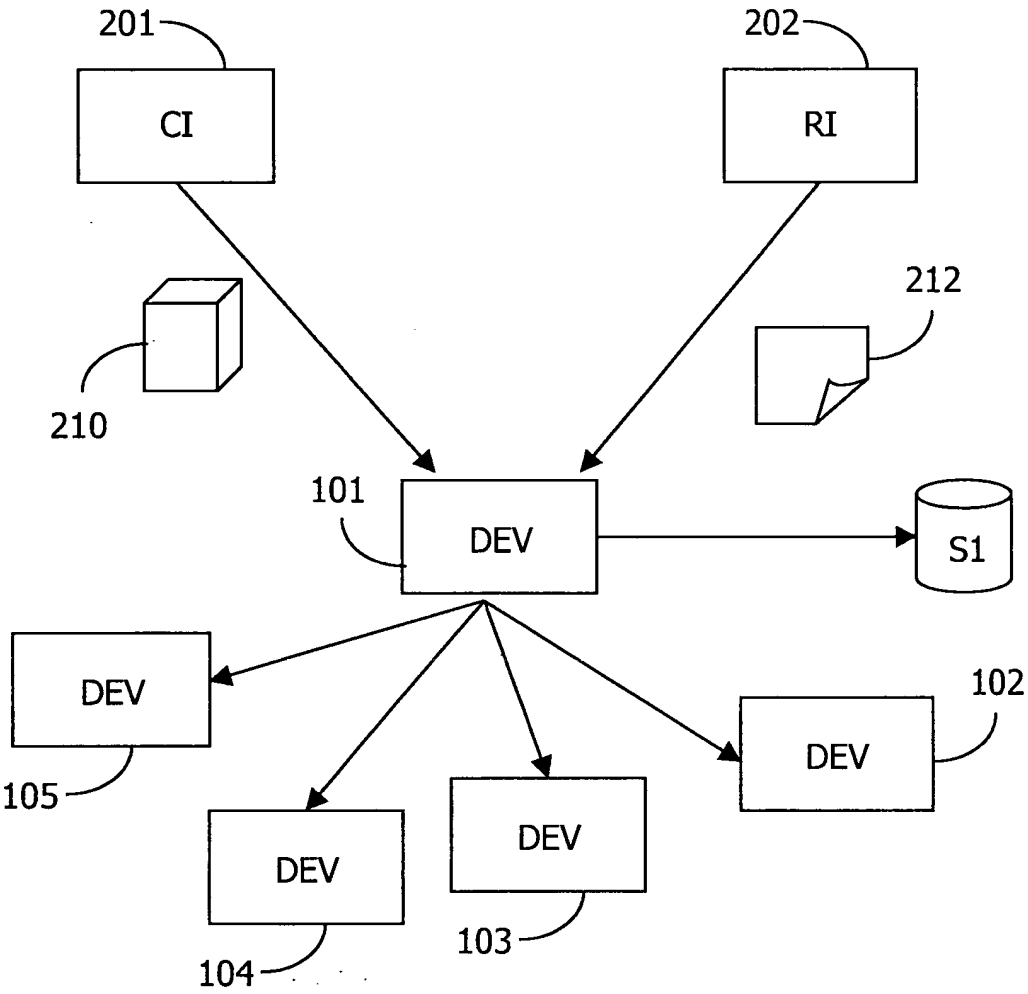


FIG. 2

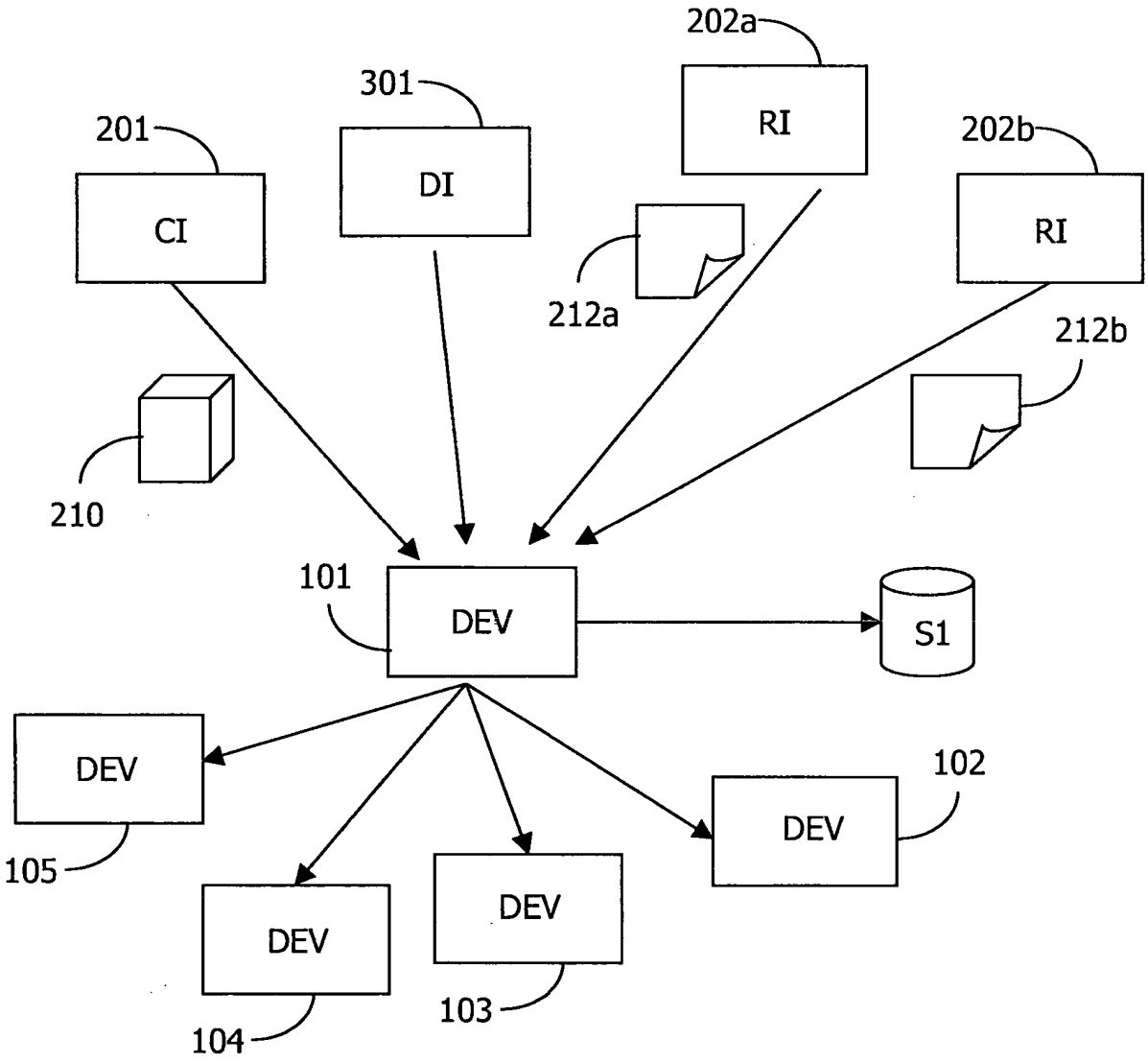

202a
301
RI
201
DI
202b
CI
RI
212a
212b
210
101
DEV
S1
DEV
102
DEV
105
DEV
DEV
104
103

FIG. 3

RESUMO

"MÉTODO PARA POSSIBILITAR QUE UMA ENTIDADE CRIE UM OBJETO QUE PODE SER AUTENTICADO E/OU DESCRIPTOGRAFADO USANDO UMA CHAVE DE DOMÍNIO COMUM, SISTEMA, E, DISPOSITIVO"

Em um domínio compreendendo uma pluralidade de dispositivos, os dispositivos no domínio compartilhando uma chave de domínio comum, um método para possibilitar uma entidade que não é um membro do domínio criar um objeto que pode ser autenticado e/ou ser descriptografado usando a chave de domínio comum, o método compreendendo fornecer para a entidade que não é um membro do domínio uma chave diversificada que é derivada usando uma função unidirecional a partir de pelo menos a chave de domínio comum para criar dados de autenticação relacionados ao mencionado objeto e/ou para criptografar o mencionado objeto, os dispositivos no domínio sendo configurados para autenticar e/ou descriptografar o mencionado objeto usando a chave diversificada.