República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) BR 112015013770-9 B1

(22) Data do Depósito: 16/12/2013

(45) Data de Concessão: 01/02/2022

(54) Título: MÉTODO E APARELHO PARA MARCAÇÃO DE ITENS FABRICADOS USANDO-SE CARACTERÍSTICAS FÍSICAS

(51) Int.Cl.: G09C 5/00; H04L 9/00.

(30) Prioridade Unionista: 17/12/2012 EP 12197525.4.

(73) Titular(es): PHILIP MORRIS PRODUCTS S.A..

(72) Inventor(es): PATRICK CHANEZ; ERWAN FRADET.

(86) Pedido PCT: PCT EP2013076725 de 16/12/2013

(87) Publicação PCT: WO 2014/095737 de 26/06/2014

(85) Data do Início da Fase Nacional: 11/06/2015

(57) Resumo: MÉTODO E APARELHO PARA MARCAÇÃO DE ITENS FABRICADOS USANDO-SE CARACTERÍSTICAS FÍSICAS. A presente invenção refere-se a um método para marcar um item fabricado , compreendendo este: a criação de um identificador de produto único para um item fabricado; a criação de uma ou mais chaves de criptografia; a geração de uma chave secreta usando-se o identificador de produto único e a uma ou mais chaves de criptografia; a geração de um valor de ruído de sistema ao realizar uma função hash na chave secreta e no identificador de produto único; a geração de uma chave física a partir de uma propriedade física medida do item fabricado; a geração de um valor de ruído físico desempenhando-se uma função hash na chave física e no identificador de produto único; a geração de um identificador seguro derivado de ou incorporando o valor de ruído de sistema e o valor de ruído físico; e a colocação de uma marca no item fabricado, compreendendo a marca do identificador seguro ou um identificador derivado do identificador seguro. Igualmente descritos são métodos de autenticação de itens em conformidade com o método descrito.

Relatório Descritivo da Patente de Invenção para **"MÉTODO E APARELHO PARA MARCAÇÃO DE ITENS FABRICADOS USANDO-SE CARACTERÍSTICAS FÍSICAS".**

[001] A presente invenção refere-se a métodos e aparelhos para marcar itens fabricados. Em particular, a presente invenção refere-se à marcação de mercadorias embaladas.

[002] Mercadorias falsificadas e contrabandeadas representam um problema global para clientes, fabricantes e autoridades governamentais. Mercadorias falsificadas, que são produções não autorizadas de mercadorias, geralmente de qualidade inferior, são vendidas ilegalmente por todo o mundo. Estas mercadorias são prejudiciais ao cliente, porque podem ser de qualidade inferior, o que pode ser perigoso (isto é particularmente importante para produtos como fármacos ou outros bens de consumo). Mercadorias falsificadas são prejudiciais para os fabricantes pois eles podem sofrer perdas em sua reputação, aumento em competição da parte de fabricantes ilegais que fabricam seus produtos, e infração de outros direitos legais. Mercadorias contrabandeadas, que são bens produzidos para fins de sonegação de impostos ou regulamentos governamentais, também são um problema considerável para fabricantes e autoridades governamentais. Estes bens são ilegalmente desviados, negociados ou importados, o que resulta em perdas significativas de receita para as autoridades governamentais devido à coleta indevida de direitos ou impostos.

[003] É vantajoso ser capaz de autenticar itens fabricados usando marcações únicas em itens sem a necessidade de armazenar cada marcação única na localidade em que os itens devem ser autenticados. É também desejável ser capaz de detectar mercadorias falsificadas, ou itens para os quais foi copiada a marcação única de um produto autêntico, sem a necessidade de armazenar um registro de

autenticação de cada marcação única.

[004] Em um aspecto da divulgação, fornece-se um método de marcação de um item fabricado, compreendendo:

[005] a criação de um identificador de produto único para um item fabricado;

[006] a criação de uma ou mais chaves de criptografia;

[007] a geração de uma chave secreta a partir do identificador de produto único e a uma ou mais chaves de criptografia;

[008] a geração de uma chave física a partir de uma propriedade física medida de um produto fabricado;

[009] a geração de um identificador seguro derivado de ou incorporando a chave secreta e a chave física; e

[0010] a colocação de uma marca no item fabricado, compreendendo a marca o identificador seguro ou um identificador derivado do identificador seguro.

[0011] O identificador seguro pode incorporar o identificador de produto único.

[0012] De preferência, o método inclui adicionalmente a etapa de gerar um valor de ruído de sistema usando a chave secreta e o identificador único de produto, em que o identificador seguro é derivado do ou incorpora o valor de ruído de sistema. De preferência, a etapa de gerar um valor de sistema de ruído compreende desempenhar uma função hash na chave secreta e no identificador de produto único.

[0013] De preferência, o método inclui adicionalmente a geração de um valor de ruído físico usando-se a chave física e o identificador de produto único, em que o identificador seguro é derivado de ou incorpora o valor de ruído de sistema. De preferência, a etapa de gerar o valor de ruído físico compreende desempenhar uma função hash na chave física e no identificador de produto único.

[0014] Tal como utilizado aqui, "identificador de produto único"

significa um identificador que identifica exclusivamente um item fabricado. Dá-se a cada item fabricado um identificador de produto único diferente. O identificador de produto único é tipicamente uma sequência numérica ou alfanumérica ou valor.

[0015] Tal como utilizado aqui, "criptografia" significa o processo de transformar informações mediante o uso de um algoritmo para tornar esta informação ilegível a qualquer um, exceto aqueles que possuírem conhecimento especial na forma de uma chave de criptografia. Descriptografia é o processo inverso. Uma "chave de criptografia" é uma parte de informação usada em conjunto com um algoritmo de criptografia para criptografar ou descriptografar informações. Uma chave de criptografia é, tipicamente, uma sequência numérica ou alfanumérica ou valor.

[0016] Tal como utilizado neste documento, o termo "chave secreta" é usado para descrever uma chave usada em um hash chaveado que é gerado mediante o uso de um identificador de produto único e uma ou mais chaves adicionais ou partes de informação. No momento de sua geração, a chave secreta não é conhecida por ninguém afora o indivíduo que criou a chave secreta. O termo "chave secreta", neste contexto, não se limita a significar uma chave privada no contexto de um esquema assimétrico de criptografia.

[0017] Tal como utilizada neste documento, uma "função hash" é uma função que mapeia informações de chegada a uma saída de tamanho fixo (geralmente menor que as informações de entrada) chamada de valor de hash. Uma função hash tipicamente substituiu ou transpõe, ou substitui e transpõe, a informação de modo a criar o valor hash ou valor de ruído. De preferência, a função hash é uma função hash criptográfica. A função hash criptográfica produz uma digital ou soma de controle das informações de chegada. Duas informações podem ser consideradas idênticas se, usando-se a mesma função hash

criptográfica, produzirem o mesmo valor hash. Vantajosamente, a função hash é uma função hash de mão-única, o que significa que é computacionalmente impossível derivar do valor de hash a informação de entrada. Essas propriedades podem ser usadas em um processo de autenticação, conforme será descrito. Uma função hash pode ser chaveada mediante a combinação de uma chave de secreta a uma mensagem de entrada, de modo a criar um valor hash ou ruído chaveado.

[0018] Tal como utilizado neste documento, o termo "valor de ruído" significa um valor hash, ou valor hash chaveado, ou um valor ou sequência de caracteres derivado diretamente de uma valor hash e uma chave secreta.

[0019] A propriedade física medida do item fabricado pode ser qualquer propriedade física medida, e pode ter base em massa, peso, formato, textura superficial ou padronagem, cor, composição química ou resposta a um estímulo, tal como resposta a estímulos elétricos, magnéticos ou óticos. A propriedade física medida preferencialmente escolhida e medida para uma resolução que é susceptível de ser exclusivo para cada item fabricado, ou pelo menos, é mais provável que seja diferente do que o mesmo para qualquer dos dois itens fabricados. A propriedade física medida preferencialmente fornece uma assinatura física para o item fabricado. Em uma modalidade preferencial, a propriedade física medida é uma imagem de uma porção da embalagem do item fabricado.

[0020] O identificador seguro pode ser qualquer tipo de identificador; porém, de preferência, é uma sequência numérica ou alfanumérica ou valor. A marca pode também ser uma sequência de caracteres ou números, ou pode ser uma representação gráfica tal como um código de barras uni ou bidimensional.

[0021] Em uma modalidade, a etapa de gerar o identificador seguro

compreende a geração de um primeiro identificador criptografando-se o identificador de produto único conjuntamente com o valor de ruído de sistema e gerando o identificador seguro mediante a criptografia o primeiro identificador conjuntamente com o valor de ruído físico.

[0022] Nesta modalidade, o método pode compreender adicionalmente a autenticação de um item fabricado em um centro de verificação, a etapa de autenticação compreendendo: a identificação da marca no produto; a descriptografia da marca para extrair o primeiro identificador e o valor de ruído físico; descriptografar o primeiro identificador para originar o identificador de produto único e o valor de ruído do sistema; a geração de uma nova chave física a partir de uma propriedade física medida de um item fabricado; a geração de uma nova cópia de um valor de ruído físico mediante o desempenho de uma função hash na nova chave física e no identificador de produto único originado; a comparação da nova cópia do valor de ruído físico ao valor de ruído físico originado; e o fornecimento de uma indicação de que o valor de ruído físico originado é idêntico ou correlato à nova cópia do valor de ruído físico.

[0023] A etapa de comparação pode compreender a originação de uma tabela de correlação e a etapa de fornecer uma indicação compreender o fornecimento de uma indicação quanto à tabela de correlação ser maior que o valor de limiar.

[0024] Na presente modalidade, a etapa de autenticação pode ainda compreender: a geração de uma nova cópia da chave secreta a partir do identificador de produto único e uma ou mais chaves de criptografia; a geração de uma nova cópia do valor de ruído de sistema mediante o desempenho de uma função hash na nova cópia da chave secreta e identificador de produto único; a comparação da nova cópia do valor de ruído de sistema ao valor de ruído de sistema originado; e o fornecimento de uma indicação quanto à nova cópia do valor de ruído

de sistema e o valor de ruído do sistema originado serem idênticos.

[0025] Em outra modalidade, a etapa de gerar um identificador seguro compreende a geração de um primeiro identificador seguro criptografando-se o identificador de produto único conjuntamente ao valor de ruído do sistema; a geração de um segundo identificador seguro criptografando-se o identificador de produto único conjuntamente ao valor de ruído físico; e a colocação de uma marca que compreende o primeiro e o segundo identificador seguro ou um identificador ou identificadores originados a partir dos identificadores seguros primeiro e segundo.

[0026] Nesta modalidade, o método pode compreender adicionalmente a autenticação de um item fabricado em um centro de verificação, a etapa de autenticação compreendendo: a identificação da marca no produto; a descriptografia da marca para extrair o primeiro identificador, o valor de ruído de sistema e o valor de ruído físico; a geração de uma nova cópia da chave secreta a partir do identificador de produto único e a uma ou mais chaves de criptografia; a geração de uma nova cópia do valor de ruído do sistema mediante o desempenho de uma função hash na nova cópia da chave secreta e identificador de produto único; a comparação da nova cópia do valor de ruído do sistema ao valor de ruído de sistema originado; a geração de uma nova chave física a partir de uma propriedade física medida do item fabricado; a geração de uma nova cópia do valor de ruído físico e do identificador de produto único originado; a comparação da nova cópia do valor de ruído físico ao valor de ruído físico originado; e o fornecimento de uma indicação quanto a se o valor de ruído de sistema é idêntico ao valor de ruído de sistema originado e se a nova cópia do valor de ruído físico é idêntica ou correlata ao valor de ruído físico originado.

[0027] Tanto em uma modalidade quanto em outra, a etapa de gerar o primeiro identificador seguro pode compreender a criptografia do

identificador de produto único e o valor de ruído do sistema mediante o uso de uma chave geradora de código, em que a etapa de geração do segundo identificador seguro compreende a combinação do primeiro identificador seguro e do valor de ruído físico conjuntamente a um identificador de gerador de código, e em que a chave geradora de código pode ser originada ou obtida a partir de uma tabela de consulta em um centro de verificação usando-se o identificador de gerador de código.

[0028] Tanto em uma modalidade quanto em outra, o método pode ainda compreender a etapa de armazenar a uma ou mais chaves de criptografia em um centro de verificação. A uma ou mais chaves de criptografia podem compreender uma chave estática e uma chave dinâmica, e em que uma nova chave dinâmica é criada para cada lote de itens fabricados ao passo que a mesma chave estática é usada para lotes plurais de itens fabricados.

[0029] O identificador de produto único pode inclui informações que identifiquem um lote de item a que o item pertence.

[0030] A invenção fornece a habilidade de autenticar tanto com base em informações do fabricante, isto é, as várias chaves de criptografia, e com base na propriedade física do item. Isto fornece duas camadas de autenticação, e permite a detecção de clonagem de identificadores em itens genuínos, mas não requer armazenamento em larga escala de códigos de autenticação.

[0031] Em outro aspecto da invenção, fornece-se um aparelho para marcar um item fabricado, compreendendo:

[0032] um gerador de chaves, configurado para gerar chaves de criptografia;

[0033] um gerador de código configurado para gerar um identificador de produto único para cada item fabricado;

[0034] um gerador de chave físico configurado para gerar chaves

físicas a partir de uma propriedade física medida de cada item fabricado;

[0035] os meios de processamento configurados para:

[0036] a geração de uma chave secreta para cada item fabricado usando-se o identificador de produto único e a uma ou mais chaves de criptografia;

[0037] a geração de um identificador seguro derivado de ou incorporando a chave secreta e a chave física; e

[0038] um marcador para marcar cada item fabricado com o identificador seguro ou um identificador derivado a partir do identificador seguro.

[0039] De preferência, o processador é configurado para gerar um valor de ruído de sistema para cada item fabricado usando a chave secreta e um identificador de produto único, em que o identificador seguro é derivado do ou incorpora o valor de ruído de sistema. De preferência, o processador está configurado para gerar o valor de ruído de sistema para cada item fabricado através da realização de uma função de hash na chave secreta e no identificador de produto único.

[0040] De preferência, o processador é configurado para gerar um valor de ruído físico para cada item fabricado usando a chave física e o identificador de produto único, em que o identificador seguro é derivado do ou incorpora o valor de ruído físico. De preferência, o processador está configurado para gerar o valor de ruído físico para cada item fabricado através da realização de uma função hash na chave física e no identificador de produto único.

[0041] Em uma modalidade, os meios de processamento estão configurados para: gerar um primeiro identificador para cada item fabricado criptografando-se o identificador de produto único conjuntamente com a chave secreta ou o valor de ruído do sistema; e gerar o identificador seguro para cada item fabricado criptografando o primeiro identificador juntamente com o valor de ruído físico.

[0042] Em outra modalidade, os meios de processamento são configurados para: gerar um primeiro identificador seguro criptografando-se o identificador de produto único conjuntamente à chave secreta ou ao valor de ruído de sistema e gerar um segundo identificador seguro para cada item fabricado criptografando-se o identificador de produto único conjuntamente à chave física ou ao valor de ruído físico; e o marcador é configurado para marcar cada item fabricado com o primeiro identificador seguro e o segundo identificador seguro ou um identificador ou identificador derivado a partir dos identificadores seguros primeiro e segundo.

[0043] O item fabricado pode ser um recipiente contendo um produto de tabaco. Exemplos de produtos de tabaco são cigarros, tabaco de folhas soltas, e cartuchos ou refis para sistemas fumígenos eletricamente aquecidos ou outros sistemas de cigarro eletrônico.

[0044] A invenção permite que itens fabricados sejam autenticados sem necessidade de armazenar grandes volumes de informação. Isto é importante para qualquer sistema prático adequado para autenticação de itens produzidos em grandes volumes. Além disso, o uso de uma chave física em combinação com um identificador de produto único (UPI) aumenta a segurança e torna mais difícil a produção de mercadorias falsificadas ou de contrabando. O acréscimo de uma chave física fornece um sistema que pode detectar clonagem e é difícil de replicar. Ainda que um falsificador tivesse conhecimento da ferramenta específica usada na geração da chave física, a combinação da chave física com um UPI para produzir um identificador torna a clonagem quase impossível. A invenção permite também que a autenticação seja desempenhada online, isto é, em conexão com um centro de verificação através de uma rede de comunicações com base no valor de ruído do sistema, permitindo igualmente que a autenticação seja desempenhada offline com base no valor de ruído físico. A marcação necessária em

cada item é simplesmente um ou mais códigos e, portanto, adiciona muito pouca despesa a cada item, quando comparado a algumas outras soluções, que dependem de etiquetas caras tecnicamente difíceis de reproduzir.

[0045] Modalidades da invenção serão descritas a seguir, exclusivamente a título de exemplo, tendo como referência os desenhos anexos em que:

[0046] A Figura 1 é uma vista esquemática de um sistema de marcação de acordo com uma modalidade da invenção;

[0047] A Figura 2 ilustra como o valor de ruído do sistema e o valor de ruído físico são derivados;

[0048] A Figura 3 é um fluxograma que apresenta um método de marcação de uma modalidade da invenção, que pode ser desempenhada no sistema da Figura 1;

[0049] A Figura 4 é um fluxograma que apresenta um método de autenticação para a modalidade da invenção representada na Figura 3, que pode ser desempenhada no sistema da Figura 1;

[0050] A Figura 5 é um fluxograma que apresenta um método de marcação de uma outra modalidade da invenção, que pode ser desempenhada no sistema da Figura 1; e

[0051] A Figura 6 é um fluxograma que apresenta um método de autenticação para a modalidade da invenção representada na Figura 5, que pode ser desempenhada no sistema da Figura 1.

[0052] Marcações únicas em itens fabricados podem ser usadas para rastrear itens. Por exemplo, uma ordem do consumidor pode ser ligada à etiqueta ou etiquetas identificadoras de uma caixa ou caixas de transporte específicos contendo as mercadorias encomendadas. "Mercadorias", neste contexto, significa itens fabricados ou outros artigos destinados à distribuição ou venda para consumidores. Isso permite que o consumidor, o fabricante e quaisquer intermediários

rastreiem constantemente a localização das mercadorias necessárias. Isto pode ser obtido usando scanners para escanear os identificadores e comunicar-se com um centro de verificação. Alternativamente, os identificadores podem ser lidos por um humano, que pode então manualmente se comunicar com um centro de verificação. Os identificadores também podem ser usados por consumidores, autoridades nacionais e outras partes, para verificar que um item específico contém produtos genuínos. Por exemplo, um terceiro pode usar um scanner para ler o identificador em uma caixa de transporte (ou o identificador pode ser lido por um humano, como discutido acima). Os detalhes do identificador podem ser enviados para um centro de verificação. O centro de verificação pode então consultar ou processar de alguma outra maneira os detalhes do identificador, determinar os detalhes de produção da caixa de transporte e enviar esses detalhes para o scanner, permitindo, desse modo, que o terceiro verifique a caixa de transporte, e os produtos contidos nela, como genuínos. No caso do banco de dados central não reconhecer o identificador, o terceiro pode supor que os artigos em questão são falsificados. Os identificadores também podem ser usados para localizar os itens. Por exemplo, se o fabricante precisar retirar os produtos de um número de caixas de transporte selecionado, essas caixas de transporte podem ser localizadas usando seus identificadores.

[0053] A Figura 1 é uma vista esquemática de um sistema de marcação de acordo com uma modalidade da invenção; Nesta modalidade, o sistema 101 compreende um ou mais centros de produção 103, 105, 107, para produzir itens fabricados 109. Cada centro de produção pode compreender uma linha de produção ou instalação que pode ser uma linha de fabricação ou embalagem de cigarros. De preferência, a produção é desempenhada em lotes, cada lotes sendo dedicado à produção de um certo número de itens fabricados

individuais. Se houver dois ou mais centros de produção, estes podem ser fisicamente situados tanto no mesmo sítio de fabricação quanto em outro diferente. Nesta modalidade preferencial, o sistema inclui os centros de produção 103, 105, 107, mas a invenção pode ser, na realidade, desempenhada em um ponto de importação, um ponto de distribuição, um comprador, um atacadista ou qualquer outro ponto na cadeia de fornecimento.

[0054] Cada centro de produção inclui um gerador de código 111 para gerar códigos para os itens fabricados 109. De preferência, o gerador de código 111 é um computador plenamente autônomo ou microcontrolador dedicado a um centro de produção particular. Cada centro de produção inclui igualmente um gerador de chave física 112 que mede ou codifica uma propriedade física de cada item fabricado e a converte em uma chave física 207. O gerador de código 111 usa as chaves físicas para gerar códigos para marcação nos itens.

[0055] Nesta modalidade, o gerador de chave física é do tipo descrito em WO2007/071788. Uma porção da embalagem de cada item é iluminada e uma imagem da parte iluminada, capturada por um sensor de imagem digital. A parte da embalagem é escolhida por sua microestrutura caótica temporalmente estável. Materiais como papel e papelão têm uma microestrutura caótica que pode ser usada como uma "impressão digital" do item. A imagem da microestrutura da parte do item é convertida em uma chave física ou assinatura, conforme descrito em WO2007/071788, sob a forma de um valor alfanumérico ou matriz. Um gerador de chaves físicas deste tipo está disponível pela Signoptic Technologies, Savoie Technolac, 5 allée Lac d'Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, França. No entanto, qualquer tipo de gerador de chaves físicas pode ser utilizado e pode depender de outras propriedades físicas do item, tais como massa ou forma ou pode mesmo confiar em propriedades químicas ou biológicas do item.

[0056] Nesta modalidade, cada centro de produção também inclui um marcador 113 para marcar os códigos gerados nos itens fabricados 109. O marcador 113 pode compreender qualquer meio adequado de marcação, por exemplo, mas não limitado a, uma impressora jato de tinta contínuo, uma impressora jato de tinta *drop-on-demand*, uma impressora holográfica, uma impressora a laser, ou qualquer outra impressora ou marcador que permita a impressão ou a marcação dos códigos gerados nos produtos fabricados individuais. A impressão ou marcação dos códigos gerados pode encontrar-se em cada item, em um pacote externo, em etiquetas ou de qualquer outra forma conveniente. Em uma modalidade, os códigos gerados são impressos em etiquetas adesivas ou rótulos para serem aplicados aos itens fabricados, preferivelmente de uma maneira não removível. Em uma modalidade, os códigos gerados são impressos por um facho de laser em uma camada de material sensível a laser depositada no item fabricado ou na embalagem do item. Estes métodos permitem que um código seja impresso através de uma camada transparente de invólucro.

[0057] O sistema 101 compreende adicionalmente um centro de verificação 114 que inclui um gerador de chave 115 para gerar chaves 209, 211 para uso na marcação e autenticação de produtos fabricados e um servidor central 117. Nesta modalidade, o gerador de código 111 pode se comunicar com o centro de verificação 114 por meio de uma conexão de Internet segura 119 e um servidor 121 local ao centro de produção, ou por outros meios de comunicação de informações. Alternativamente, o gerador de código 111 pode se comunicar com o centro de verificação por meio de um portal de fabricação dedicado a um ou mais centros de produção.

[0058] O gerador de chave 115 gera uma chave criptográfica, designado neste documento como uma chave estática. O gerador de

chave 115 gera uma versão não criptografada da chave estática e uma versão criptografada da chave estática. A versão não criptografada da chave estática, designada neste documento como chave estática ativa 209, é mostrada com uma borda sólida na Figura 1. A versão criptografada da chave estática, designada neste documento como chave estática inativa 211, é mostrada com uma borda pontilhada na Figura 1. A chave estática ativa 209, o que equivale a dizer a versão não criptografada da chave estática, é gerada no gerador de chave 115 e é, portanto, acessível ao servidor central 117. O gerador de chave 115 envia a chave estática inativa 211 para o gerador de código 111 no centro de produção 103, 105, 107.

[0059] A chave estática inativa 211 pode ser enviada a partir do gerador de chave 115 ao gerador de códigos 111 em um suporte de dados não volátil, por exemplo, um CD-ROM, um DVD-Rom ou um disco rígido removível. O suporte de informações é fisicamente transferido para o gerador de código 111, no centro de produção 103, 105, 107. Alternativamente, a chave estática inativa 211 pode ser enviada do gerador de chave 115 ao gerador de código 111 por meio de uma conexão de rede segura, por exemplo, uma que envolva criptografia. Isto pode ocorrer sob demanda do gerador de código 111. Isto garante a autenticidade, a confidencialidade e a integridade da chave estática.

[0060] O gerador de chave 115 gera também o código de ativação 213, que compreende a chave ou código para descriptografar a chave estática inativa 211 para formar a chave estática ativa 209. Este código de ativação 213 também é acessível ao servidor central 117. De preferência, a chave estática ativa 209 e código de ativação 213 são armazenados conjuntamente com a identificação do centro de produção 103, 105, 107 para o qual são remanejados.

[0061] Em uma modalidade, a chave estática compreende um

número de porções. A parte principal pode ser uma pluralidade de códigos secretos, por exemplo, uma matriz salina. Uma matriz salina pode ser, por exemplo, uma longa sequência de dígitos numéricos randômicos ou pseudorrandômicos. O número de partes adicionais pode incluir um identificador único para a chave estática, um código seriado definindo como a chave estática deve ser combinada com uma chave dinâmica (discutido abaixo), um certificado criptográfico digital associado ao identificador único da chave estática e uma apólice ou licença que contém o certificado criptográfico gerado acima.

[0062] De preferência, a chave estática inativa, o que equivale a dizer a versão criptografada da chave estática, e particularmente a pluralidade de códigos secretos, é criptografada usando-se uma cifra forte. Um exemplo de uma cifra apropriada é a cifra de bloco Triple DES (Data Encryption Standard) ou o bloco cifrado DES/Rijandel. Ambos aplicam o algoritmo de cifra DES três vezes a cada bloco de informação e o Triplo DES / Rijandel é uma variação menor do Triplo DES que foi desenvolvido pela IBM. Nesse caso, a chave Triplo DES ou Triplo Des/Rijandel compreende o código de ativação 213. Assim, em uma modalidade preferencial, a chave estática ativa 209 é decodificada, a chave inativa 211 é criptografada usando-se a chave Triplo DES ou Triplo Des/Rijandel, e o código de ativação 213 compreende essa chave Triplo DES ou Triplo Des/Rijandel.

[0063] Na próxima etapa 203, a chave estática inativa 211 recebida pelo gerador de código 111 é registrada. Isto é realizado pelo gerador de códigos 111 ao enviar para o centro de verificação 114 uma informação 215 sobre o a chave estática recebida e qualquer outra informação de maquinários relevantes (não exibido). Isto é preferencialmente enviado por meio de uma conexão segura de internet 119, tal como representado na Figura 1, mas pode ser enviado por outra rota apropriada. O centro de verificação 114 envia de volta para o

gerador de código 111 o código de ativação 213. O código de ativação 213 permite que a chave estática inativa 211 seja ativada, e isso é esquematicamente representado em 217. O código de ativação 213 é, de preferência, igualmente enviado por meio de uma conexão segura de internet 119, como representado na Figura 1. O processo de registro é, de preferência, arranjado de tal maneira que a chave estática ativa 209 nunca é transferida pela internet.

[0064] O procedimento de registro pode tomar a forma de um mecanismo convencional de troca de pares de chave públicas/privadas. Isto pode usar um par assimétrico de chaves associado ao certificado criptográfico digital que faz parte da chave estática, tal como discutido acima. Nesse caso, a chave pública do par assimétrico de chaves por vir na forma de uma chave emitida por um terceiro, por exemplo, uma autoridade governamental. A informação 215 sobre a chave estática recebida que é enviada do gerador de código 111 ao centro de verificação 114 pode compreender o identificador único para a chave estática que faz parte da chave estática, tal como discutido acima. As informações de maquinário relevantes (não exibidas), que são igualmente enviadas do gerador de código 111 ao centro de verificação 114 pode compreender um identificador único ou certificado para o gerador de código 111 ou centro de produção. Esse identificador único pode incluir informações acerca da locação e identidade do gerador de código ou centro de produção, que foi pré-autorizado para produção. De preferência, o identificador único de chave estática e o identificador de gerador de código ou centro de produção são criptografados usando-se a chave pública do par assimétrico de chaves associado ao certificado de chave estática.

[0065] Uma vez que o centro de verificação 114 recebe o identificador único de chave estática criptografada e o identificador de código gerador ou centro de produção, o centro de verificação 114 pode

descriptografar utilizando a chave privada do par assimétrico de chave associado ao certificado da chave estática. O centro de verificação pode então verificar se o identificador único de chave estática e o identificador de gerador de código ou centro de produção são válidos. Então, o centro de verificação 114 envia de volta para o gerador de código 111 o código de ativação 213. Como já mencionado, de preferência, o código de ativação 213 é sob a forma de uma cifra Triple DES ou Triple DES/Rijandel. O centro de verificação criptografa o código de ativação (por exemplo, a cifra Triplo DES ou Triplo DES/Rijandel) com a chave pública do par assimétrico de chaves associado ao certificado de chave estática. Isso permite que o código de ativação (por exemplo, a cifra Triplo DES ou Triplo DES/Rijandel) a ser decodificado pelo gerador de código usando a chave privada do par assimétrico de chaves associado ao certificado de chave estática. Em seguida, a chave estática inativa 211 pode ser ativada usando o código de ativação decodificado 213 para formar a chave estática ativa 209.

[0066] Uma vez ativada a chave estática 211 ao fim do gerador de código 111, o centro de produção é capaz de fabricar itens e produzir códigos para os itens fabricados no gerador de código 111.

[0067] O gerador de código 111 gera uma nova chave, designada neste documento como chave dinâmica 219, para cada lote de itens fabricados. A chave dinâmica 219 é, de preferência, um código secreto randômico, tal como um número randômico. O gerador de código usa a chave dinâmica 219 para um lote, juntamente com a chave estática ativa 209, para gerar uma chave secreta 223. A chave secreta 223 é o n usado em combinação com as chaves físicas e um identificador de produto único (UPI) para que cada item gere códigos 221 (por exemplo, códigos alfanuméricos) que devem ser marcados nos itens fabricados naquele lote. Na presente modalidade, o UPI para cada item compreende detalhes de produção que identificam o tempo de produção

conjuntamente a um contra valor suplementar para diferenciar itens produzidos dentro dos limites de um mesmo período de tempo por um mesmo centro de produção.

[0068] O gerador de código usa uma função hash criptográfica em uma combinação do UPI com a chave secreta e uma combinação do UPI com uma chave física. Isto cria impressões digitais digitalizadas, designadas neste documento como "valores de ruído", para o item, e estes valores de ruído são usados para gerar os códigos 221 que são marcados nos itens pelo marcador 113. Além das funções hash criptográficas tipicamente usadas, uma variedade de técnicas encontra-se disponível para gerar os valores de hash ou valores de ruído, incluindo, mas não limitando-se a: transposição, substituição, substituição por tabela e indexação.

[0069] A Figura 2 ilustra o método de gerar os valores de ruído desempenhado pelo gerador de código 111 Para gerar o valor de ruído de sistema 225, a chave secreta é primeiramente originada a partir da chave estática ativa 209, a chave dinâmica 219 e o UPI 221. A chave dinâmica 219 e a chave estática ativa 209 são conhecidas apenas para o centro de verificação 114 e o gerador de código 111. Na etapa 301 a chave dinâmica e o UPI são usados para extrair a chave secreta da matriz salina contida na chave estática, em conformidade com o código seriado dentro da chave estática. A chave secreta 223 e o UPI 221 são então hasheados na etapa 303 para produzir o ruído do sistema para o item. Para gerar o valor de ruído físico 227, a chave física 207 é hasheada com o UPI 221 na etapa 305. A função hash usada para gerar o valor de ruído de sistema pode ser a mesma ou diferente da função de hash usado para gerar o valor de ruído físico.

[0070] A Figura 3 ilustra um método para usar o valor de ruído de sistema e um valor de ruído físico para gerar um identificador seguro para cada item em conformidade com uma primeira modalidade da

invenção. Na etapa 311 são combinados o valor de ruído do sistema 225 e o UPI 221. Na etapa 313 o valor de ruído de sistema combinado e UPI são criptografados pela chave de ofuscação do código de gerador (CGOK) 231 para produzir um primeiro identificador 241. O CGOK é específico ao gerador de código e é pré-carregado no gerador de código. O primeiro identificador 241 é então combinado com o valor de ruído físico 227 e um identificador de gerador de código 233. O identificador de gerador de código (CGID) 233 permitirá que o CGOK seja obtido durante a autenticação. A combinação do primeiro identificador, o valor de ruído físico e o CGID é então criptografado usando-se uma chave global 235 na etapa 317 para produzir o identificador seguro 251. A chave global 235 é comum a todos os centros de produção e pode ser parte de um par simétrico ou assimétrico de chaves conhecido pelo centro de verificação. O identificador seguro 251 é então marcado no item na etapa 319 pelo marcador 113.

[0071] O gerador de código 111 ou centro de produção 103, 105, 107 mantém uma contagem dos códigos que são marcados nos itens fabricados. Além disso, o gerador de código 111 envia a chave dinâmica 219 de cada lote, conjuntamente a informações acerca do lote (não exibido), ao centro de verificação 114. Isto pode ser realizado por meio de uma conexão segura de internet 119. As informações acerca do lote podem incluir diversas partes de informação, por exemplo, mas não limitando-se a, marca, mercado destinado ou destino pretendido. As chaves dinâmicas 219 não precisam ser enviadas ao centro de verificação 114 em tempo real e podem ser comunicadas ao centro de verificação em qualquer momento apropriado, por exemplo, mensalmente. As chaves dinâmicas 219 enviadas ao centro de verificação 114 são armazenadas em um banco de dados (por exemplo, em um servidor central 117) no ou acessível em um centro de

verificação 114. A chave dinâmica 219 para cada lote é, de preferência, armazenada junto às informações de lote enviadas para o centro de verificação 114 ao mesmo tempo.

[0072] De preferência, a chave estática ativa 209 é excluída quando o gerador de código 111 em um centro de produção específico 103, 105, 107 é colocado fora de serviço. Isso impede que um usuário mal-intencionado acesse a chave estática ativa 209 sem registro apropriado. Meios adicionais para desabilitar o gerador de código 111 e impedir utilização não autorizada do gerador de código 111 e do centro de produção podem ser fornecidos.

[0073] A Figura 4 ilustra as etapas realizadas pelo centro de verificação 114 e pelo usuário 601, quando um usuário 601 deseja autenticar um item fabricado individual marcado em conformidade com o processo da Figura 3. O usuário 601 lê o código 221 no item e o envia para o centro de verificação 114. Isso é ilustrado na Figura 1. O usuário 601 pode enviar o código para o centro de verificação 114 por qualquer meio apropriado, tal como uma conexão de internet segura ou não segura.

[0074] O centro de verificação recebe o identificador seguro na etapa 321. O identificador seguro é decodificado usando-se a chave global 235 (ou a chave correspondente no par de chaves, em caso de chaves assimétricas) na etapa 323 para revelar o valor de ruído físico 227 e o primeiro identificador 241. O CGID também é revelado. Usando uma tabela de consulta, o CGOK 231 é então obtido a partir do CGID. O primeiro ID é então decodificado na etapa 325 usando o CGOK 231 para revelar o ruído do sistema 225 e UPI 221. Com esta informação, em conjunto com a chave estática ativa 209 e chave dinâmica 219 e uma nova chave física, tanto o valor de ruído físico e o valor de ruído de sistema podem ser recriados para autenticar o item.

[0075] Para recriar o valor de ruído físico uma nova chave física

deve ser obtida pelo usuário 601 na etapa 327 ao registrar-se uma imagem da porção do item da mesma maneira e sob as mesmas condições que foram utilizadas na geração da chave física original 207. A UPI e nova chave física são então hasheadas para gerar um novo valor de ruído físico na etapa 329. Na etapa 331, o novo ruído físico é comparado ao valor de ruído físico extraído revelado na etapa 323. Se o novo valor de ruído físico for suficientemente semelhante ao valor de ruído físico extraído, então conclui-se uma parte do processo de autenticação. Se o novo valor de ruído físico não for suficientemente semelhante ao valor de ruído físico extraído, então o item é determinado como inautêntico na etapa 339.

[0076] Para que o item seja considerado autêntico, o novo valor de ruído físico pode precisar ser idêntico ao valor de ruído físico extraído. No entanto, é possível permitir algumas diferenças entre o novo valor de ruído físico e o valor de ruído físico extraído usando-se uma pontuação de correlação e exigindo-se uma pontuação de correlação de limiar para que o item seja considerado autêntico. US2005/0257064 descreve um método estatístico adequado para calcular um grau de correlação ou similitude entre duas assinaturas digitas derivadas de propriedades físicas medidas de um meio fibroso.

[0077] É tão possível para o usuário 601 desempenhar as etapas 329 e 331 quanto para o centro de verificação 114. Se ao usuário 601 for concedido o UPI por parte do centro de verificação, o usuário final pode autenticar o item com base no valor de ruído físico. Da mesma forma, se a nova chave física for fornecida ao centro de verificação 114, o centro de verificação pode autenticar o item com base no valor de ruído físico.

[0078] Para recriar o valor de ruído de sistema, a chave secreta deve ser novamente gerada. Na etapa 333, usando-se o UPI e o CGID, o centro de verificação 114 é capaz de recuperar a chave dinâmica 219

e a chave ativa estática 209 de registros mantidos no centro de verificação. A chave secreta pode então ser novamente gerada usando-se o UPI 221, a chave dinâmica 219 e a chave estática ativa 209. Na etapa 335 um novo valor de ruído do sistema é recriado ao hashear-se o UPI e a chave secreta. Na etapa 337, o novo valor de ruído do sistema é comparado ao valor de ruído do sistema extraído na etapa 325. Se o novo valor de ruído do sistema e o valor de ruído de sistema de sistema extraído forem idênticos, o item então pode ser determinado como autêntico na etapa 339.

[0079] Em uma modalidade, tanto as comparações de valor de ruído físico quanto de valor de ruído de sistema são requeridas para que o item seja considerado autêntico. No entanto, é possível permitir autenticação com base em apenas uma dessas checagens, caso assim se deseje.

[0080] A partir da chave estática ativa derivada 209, o centro de produção 103, 105, 107 em que o item foi fabricado pode ser determinado, já que as chaves estáticas ativas são, de preferência, armazenadas no centro de verificação em conjunto com detalhes de seus centros de produção associados. A partir da chave dinâmica derivada 219, a informação de lote correspondente ao item pode ser determinada, já que as chaves dinâmicas são, de preferência, armazenadas no centro de verificação conjuntamente com as informações de lote associadas. Deste modo, o centro de verificação 114 pode derivar, a partir do código 221 enviado ao usuário 601, várias partes de informação 603 acerca do item individual bem como checar a autenticidade do item. Em seguida, todas as partes, ou apenas partes selecionadas da informação 603, incluindo uma indicação quanto à autenticidade ou inautenticidade do item, podem ser remetidas ao usuário 601. Isso é representado na Figura 1. As informações 603 são, de preferência, enviadas ao usuário 601 através dos mesmos meios

pelos quais o código original foi enviado.

[0081] A Figura 5 ilustra um processo de marcação em conformidade com uma segunda modalidade da invenção. No método da Figura 5, dois identificadores seguros são produzidos, um com base no valor de ruído de sistema 225 e outro, com base no valor de ruído físico 227. O valor de ruído do sistema 225 é combinado ao UPI 221 na etapa 341. A combinação do valor de ruído de sistema e o identificador único de produto é então criptografado com o CGOK 231 na etapa 343 para produzir o primeiro ID 241 tal como na primeira modalidade da Figura 3. O primeiro ID 241 é então combinado com a CGID na etapa 345 e criptografado com a chave global 235 na etapa 347 para produzir um primeiro ID seguro 271. O valor de ruído físico 227 é então combinado com o UPI na etapa 221 para produzir um segundo ID 261. O segundo ID é criptografado com a chave global 235 na etapa 353 para produzir um segundo ID seguro. O item pode então ser marcado na etapa 355 com o primeiro ID seguro 271 e o segundo ID seguro 281, ou com uma marca ou marcas derivadas a partir de uma combinação entre o primeiro ID seguro 271 e o segundo ID seguro 281.

[0082] A Figura 6 ilustra as etapas realizadas para autenticar um item marcado usando-se o processo ilustrado na Figura 5. Na etapa 401, a marca ou marcas são lidas pelo usuário e o usuário deriva o primeiro identificador seguro 271 e o segundo identificador seguro 281. Na etapa 403, a chave global 235 é usada para derivar o valor de ruído físico 227, uma primeira cópia de UPI 221, o primeiro ID 241 e CGID 233. Se o usuário tiver a chave global 235, o usuário pode autenticar o item com base no segundo identificador seguro off-line, ou seja, sem a necessidade de conexão ao centro da verificação. O usuário gera uma nova chave física na etapa 407 e isto é hasheado com o UPI para gerar um novo valor de ruído físico na etapa 409. O usuário pode então comparar o novo valor de ruído físico ao valor de ruído físico extraído

na etapa 403 na etapa 411. Conforme descrito em referência à Figura 3, o item pode ser considerado autêntico na etapa 419 se o novo valor de ruído físico for igual ou suficientemente similar ao valor de ruído físico extraído.

[0083] Na etapa 405, o CGID é usado pelo centro de verificação para recuperar o CGOK 231, e o CGOK é usado para descriptografar o primeiro ID 241 para revelar o ruído de sistema e uma segunda cópia do UPI. Na etapa 408, a segunda cópia do UPI pode opcionalmente ser comparada à primeira cópia da UPI a título de checagem. Na etapa 413, o centro de verificação 114 recupera a chave dinâmica 219 e a chave estática ativa 209 usando o CGID e UPI. Na etapa 415, um novo valor de ruído de sistema é gerado primeiro ao gerar-se novamente uma chave secreta a partir do UPI, da chave dinâmica e da chave estática, e hasheando-se então a chave secreta com o UPI. Na etapa 417, o novo valor de ruído de sistema é comparado ao valor de ruído de sistema extraído na etapa 405. Se forem idênticos, o item pode ser autenticado na etapa 419. Assim como a modalidade da Figura 3, a autenticação com base tanto no valor de ruído do sistema como no valor de ruído físico pode ser exigida para que um item possa ser considerado autêntico.

[0084] Embora a invenção tenha sido descrita tendo como referência à fabricação de cigarro, deve ficar claro que a invenção é aplicável a quaisquer produtos que requeiram autenticação, tais como fármacos, bebidas alcoólicas e mercadorias de luxo.

REIVINDICAÇÕES

1. Método para marcação de um item fabricado, sendo o método caracterizado por compreender:

a criação de um identificador de produto único (UPI) para um item fabricado;

a criação de uma ou mais chaves de criptografia (209, 219);

a geração de uma chave secreta (223) a partir do identificador de produto único e a uma ou mais chaves de criptografia;

a geração de um valor de ruído de sistema (225) usando a chave secreta e o identificador de produto único

a geração de uma chave física (207) a partir de uma propriedade física medida de um produto fabricado;

a geração de um valor de ruído físico (227) usando a chave física e o identificador de produto único;

em que, para criar o valor de ruído de sistema e o valor de ruído físico, o método utiliza transposição, substituição por tabela e indexação, ou uma função hash criptográfica em uma combinação do identificador de produto único com a chave secreta e uma combinação do identificador de produto único com a chave física;

a geração de um identificador seguro derivado (251, 271, 281) de ou incorporando a chave secreta e a chave física, em que o identificador seguro é derivado do ou incorpora o valor de ruído de sistema, e em que o identificador seguro é derivado do ou incorpora o valor de ruído físico; e

a colocação (319, 355) de uma marca no item fabricado, compreendendo a marca o identificador seguro ou um identificador derivado do identificador seguro.

2. Método, de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador seguro incorpora o identificador de produto único.

3. Método, de acordo com a reivindicação 2, caracterizado pelo fato de que a etapa de geração do identificador seguro compreende a geração (311, 313) de um primeiro identificador criptografando o identificador de produto único juntamente ao valor de ruído do sistema e a geração de um identificador seguro criptografando (317) o primeiro identificador juntamente ao valor de ruído físico.

4. Método, de acordo com a reivindicação 3, caracterizado pelo fato de que:

- a etapa de geração do primeiro identificador criptografando o identificador único de produto junto com o valor de ruído físico é realizado criptografando (313) por uma chave de ofuscação de gerador de código (CGOK);

- o primeiro identificador é então combinado com o valor de ruído físico e um identificador de gerador de código (233);

- a combinação do primeiro identificador, do valor de ruído físico e do identificador de gerador de código é então criptografada (317) utilizando uma chave global (235) para produzir o identificador seguro.

5. Método, de acordo com a reivindicação 4, caracterizado pelo fato de que a chave de ofuscação de gerador de código é particular a um gerador de código (111) no qual é pré-carregado e em que a chave global é comum para todos dos um ou mais centros de produção.

6. Método, de acordo com a reivindicação 3, caracterizado pelo fato de que compreende adicionalmente a autenticação do item fabricado em um centro de verificação, compreendendo a etapa de autenticação:

a identificação (321) da marca no item;

a descriptografia (323) da marca para derivar o primeiro identificador e o valor de ruído físico;

a descriptografia (325) do primeiro identificador para derivar o identificador de produto único e o valor de ruído do sistema;

a geração (327) de uma nova chave física a partir de uma propriedade física medida de um item fabricado;

a geração (329) de uma nova cópia do valor de ruído físico, mediante o desempenho de uma função hash na chave física nova e no identificador de produto único derivado;

a comparação (331) da nova cópia do valor de ruído físico ao valor de ruído físico derivado; e

o fornecimento de uma indicação (339) quanto ao valor de ruído físico derivado ser idêntico a ou correlacionado à nova cópia do valor de ruído físico.

7. Método, de acordo com a reivindicação 6, sendo a etapa de autenticação caracterizada por compreender adicionalmente:

a geração (333) de uma nova cópia da chave secreta a partir do identificador de produto único e a uma ou mais chaves de criptografia;

a geração (335) de uma nova cópia do valor de ruído de sistema, mediante o desempenho de uma função hash na nova cópia da chave secreta e no identificador de produto único.

a comparação (337) da nova cópia do valor de ruído de sistema ao valor de ruído de sistema derivado; e

o fornecimento de uma indicação (339) quanto à nova cópia do valor de ruído de sistema e o valor de ruído de sistema derivado serem idênticos.

8. Método, de acordo com a reivindicação 2, caracterizado pelo fato de que a etapa de gerar o identificador seguro compreende a geração de um primeiro identificador seguro ao criptografar-se (241) o identificador de produto único conjuntamente ao valor de ruído do sistema;

a geração (261) de um segundo identificador seguro ao criptografar-se o identificador de produto único conjuntamente ao valor

de ruído físico; e

a colocação (355) de uma marca no item fabricado, compreendendo a marca dos identificadores seguros primeiro e segundo, ou um identificador ou identificadores derivados a partir dos identificadores seguros primeiro e segundo.

9. Método, de acordo com a reivindicação 8, caracterizado pelo fato de que:

- o valor de rúido de sistema é combinado com o identificador único de produto;

- a combinação do valor de ruído de sistema e do identificador único de produto é então criptografada (343) com uma chave de ofuscação de gerador de código (CGOK) para produzir (241) um primeiro identificador;

- o primeiro identificador é então combinado com um identificador de gerador de código (CGID) e criptografado (347) com uma chave global (235) para produzir um segundo identificador seguro;

- o valor de ruído físico é combinado (351) com o produto único para produzir um segundo identificador (261);

- o segundo identificador é criptografado com a chave global (235) para produzir um segundo identificador seguro (281).

10. Método, de acordo com a reivindicação 8, caracterizado pelo fato de que compreende adicionalmente a autenticação do item fabricado em um centro de verificação, compreendendo a etapa de autenticação:

a identificação (401) da marca no item;

a descriptografia (403, 405) da marca para derivar o identificador de produto único, o valor de ruído do sistema e o ruído físico;

a geração (413) de uma nova cópia da chave secreta a partir do identificador de produto único e a uma ou mais chaves de

criptografia;

a geração (415) de uma nova cópia do valor de ruído de sistema, mediante o desempenho de uma função hash na nova cópia da chave secreta e no identificador de produto único.

a comparação (417) da nova cópia do valor de ruído de sistema ao valor de ruído de sistema derivado;

a geração (407) de uma nova chave física a partir de uma propriedade física medida de um item fabricado;

a geração (409) de uma nova cópia do valor de ruído físico, mediante o desempenho de uma função hash na chave física nova e no identificador de produto único derivado;

a comparação (411) da nova cópia do valor de ruído físico ao valor de ruído físico derivado; e

o fornecimento (419) de uma indicação quanto a se a nova cópia do valor de ruído do sistema é idêntica ao valor de ruído do sistema derivado, e se a nova cópia do valor de ruído físico é idêntico a ou correlato ao valor de ruído físico derivado.

11. Método, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que uma ou mais chaves de criptografia compreendem uma chave estática (209) e uma chave dinâmica (219), e em que uma nova chave dinâmica é criada para cada lote de itens fabricados.

12. Método, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato que o identificador de produto único inclui informações que identificam um lote de itens ao qual o item pertence.

13. Método de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que um valor de ruído é um valor hash, um valor hash chaveado, ou um valor ou sequência de caracteres derivada diretamente de um valor hash e uma chave secreta.

14. Método de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que a propriedade física medida do item fabricado é baseada na textura de superfície do item fabricado.

15. Aparelho para marcação de um item fabricado, caracterizado pelo fato de que compreende:

um gerador de chaves (115), configurado para gerar chaves de criptografia;

um gerador de código (111) configurado para gerar um identificador de produto único para cada item fabricado;

um gerador de chave física (112) configurado para gerar chaves físicas a partir de uma propriedade física medida de cada item fabricado;

meios de processamento (111) configurados para:

a geração de uma chave secreta (223) para cada item fabricado usando-se o identificador de produto único e a uma ou mais chaves de criptografia;

a geração de um valor de ruído de sistema (225) para cada item fabricado realizando uma função hash na chave secreta e em um identificador único de produto;

a geração de um valor de ruído físico (227) para cada item fabricado realizando uma função hash na chave física e no identificador único de produto;

a geração de um identificador seguro (251, 271, 281) derivado de ou incorporando a chave secreta e a chave física, em que o identificador seguro é derivado do ou incorpora o valor de ruído de sistema, e em que o identificador seguro é derivado do ou incorpora o valor de ruído físico; e

um marcador para marcar (319, 355) cada item fabricado com o identificador seguro ou um identificador derivado a partir do identificador seguro.

16. Aparelho de acordo com a reivindicação 15, caracterizado pelo fato de que a propriedade física medida do item fabricado é baseada na textura de superfície do item manufaturado.

Figura 1

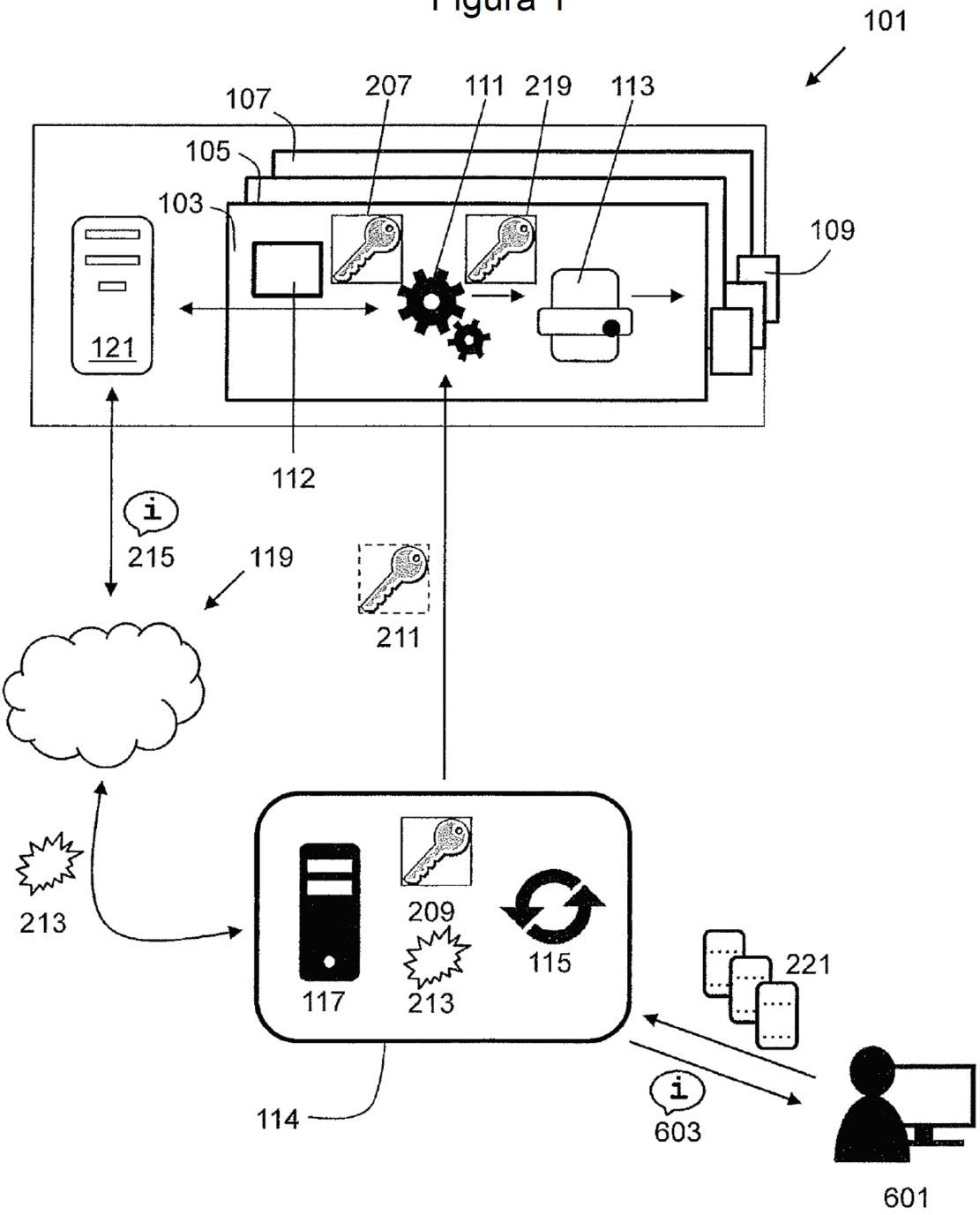
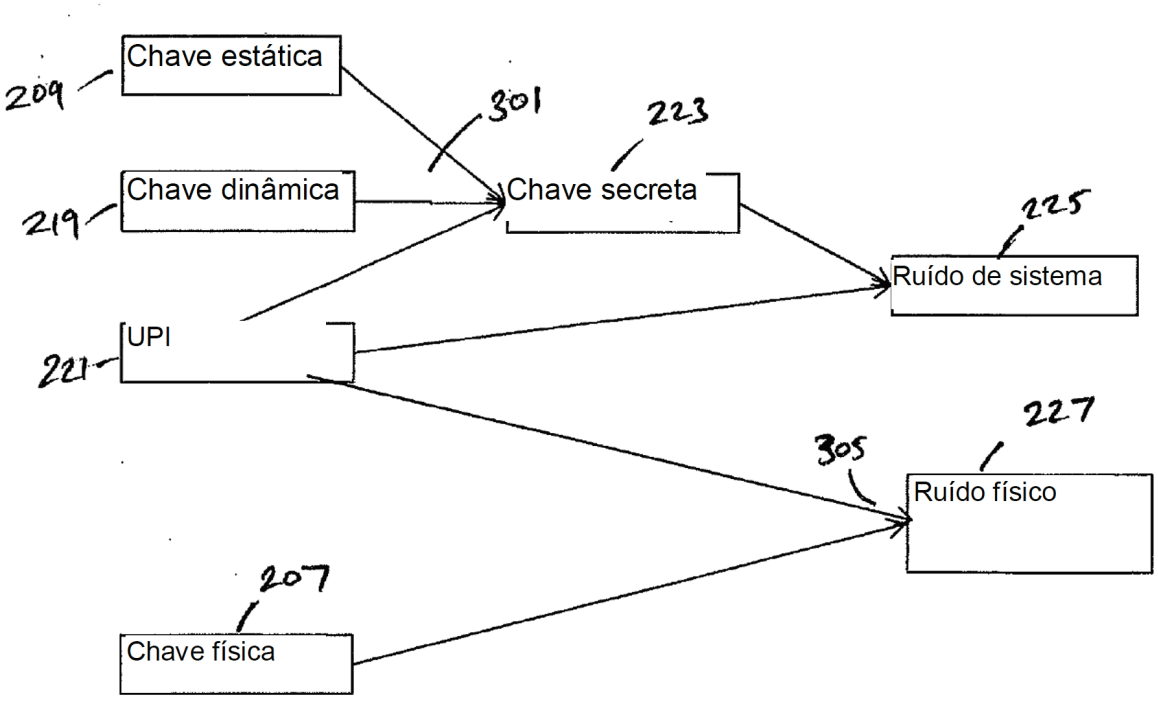

101
107
207
111
219
113
105
103
109
121
112
215
119
211
213
209
213
115
117
221
114
603
601

Figura 2


209
Chave estática
301
223
219
Chave dinâmica
Chave secreta
225
Ruído de sistema
221
UPI
227
305
Ruído físico
207
Chave física

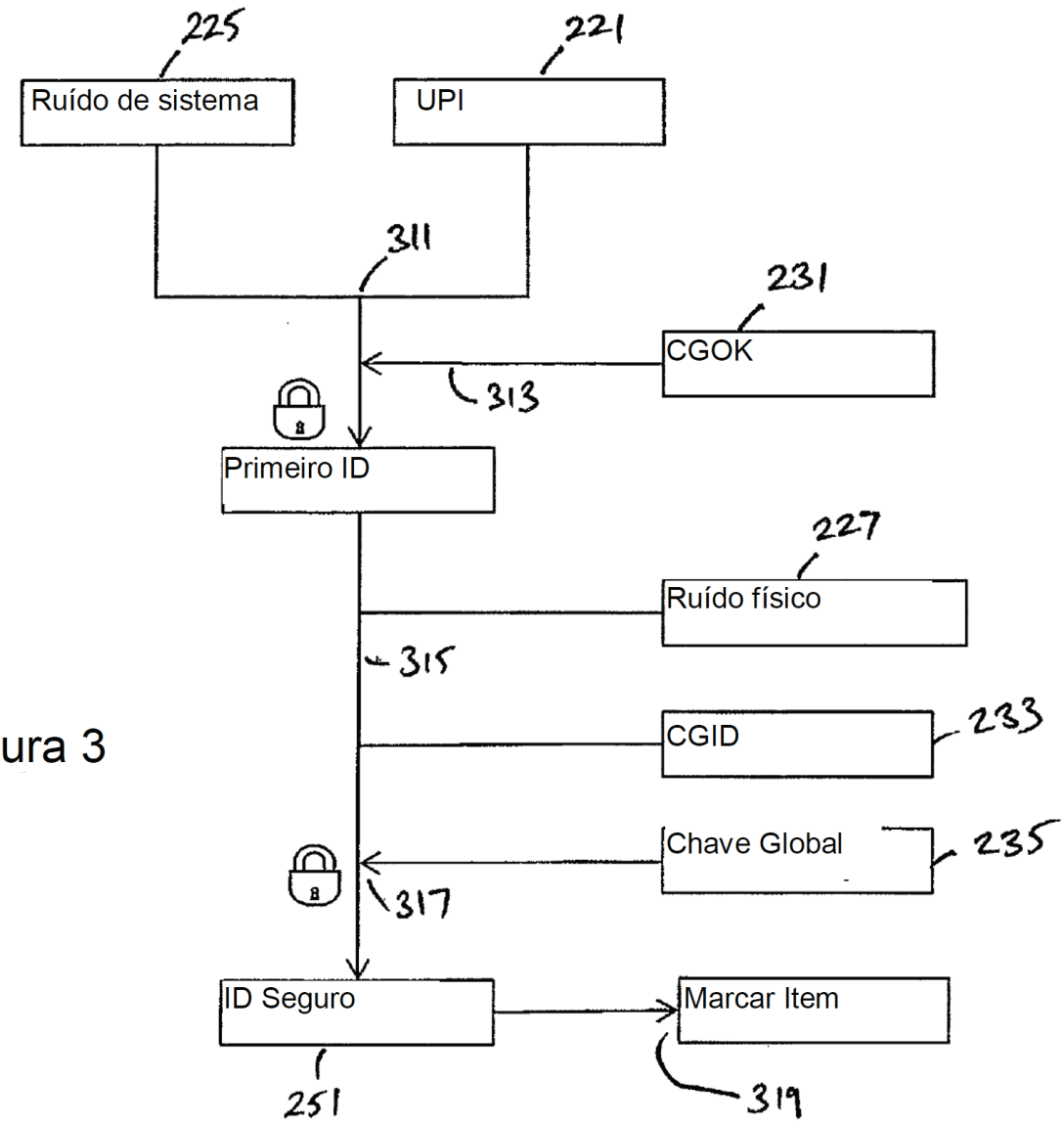

225
Ruído de sistema
221
UPI
311
231
CGOK
313
Primeiro ID
227
Ruído físico
315
CGID
233
Chave Global
235
317
ID Seguro
Marcar Item
251
319

Figura 3

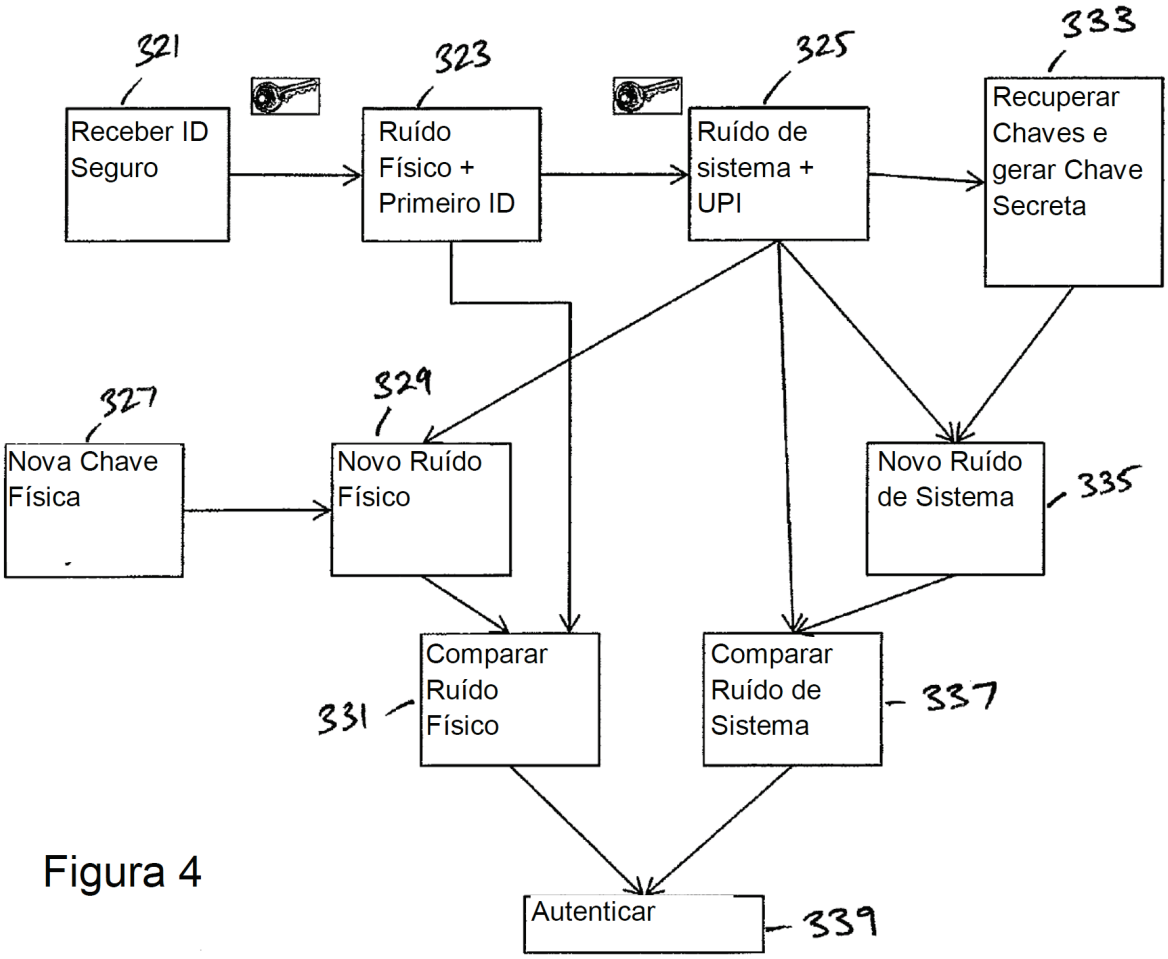

321
Receber ID Seguro
323
Ruído Físico + Primeiro ID
325
Ruído de sistema + UPI
333
Recuperar Chaves e gerar Chave Secreta
327
Nova Chave Física
329
Novo Ruído Físico
Novo Ruído de Sistema
335
331
Comparar Ruído Físico
Comparar Ruído de Sistema
337
Autenticar
339

Figura 4

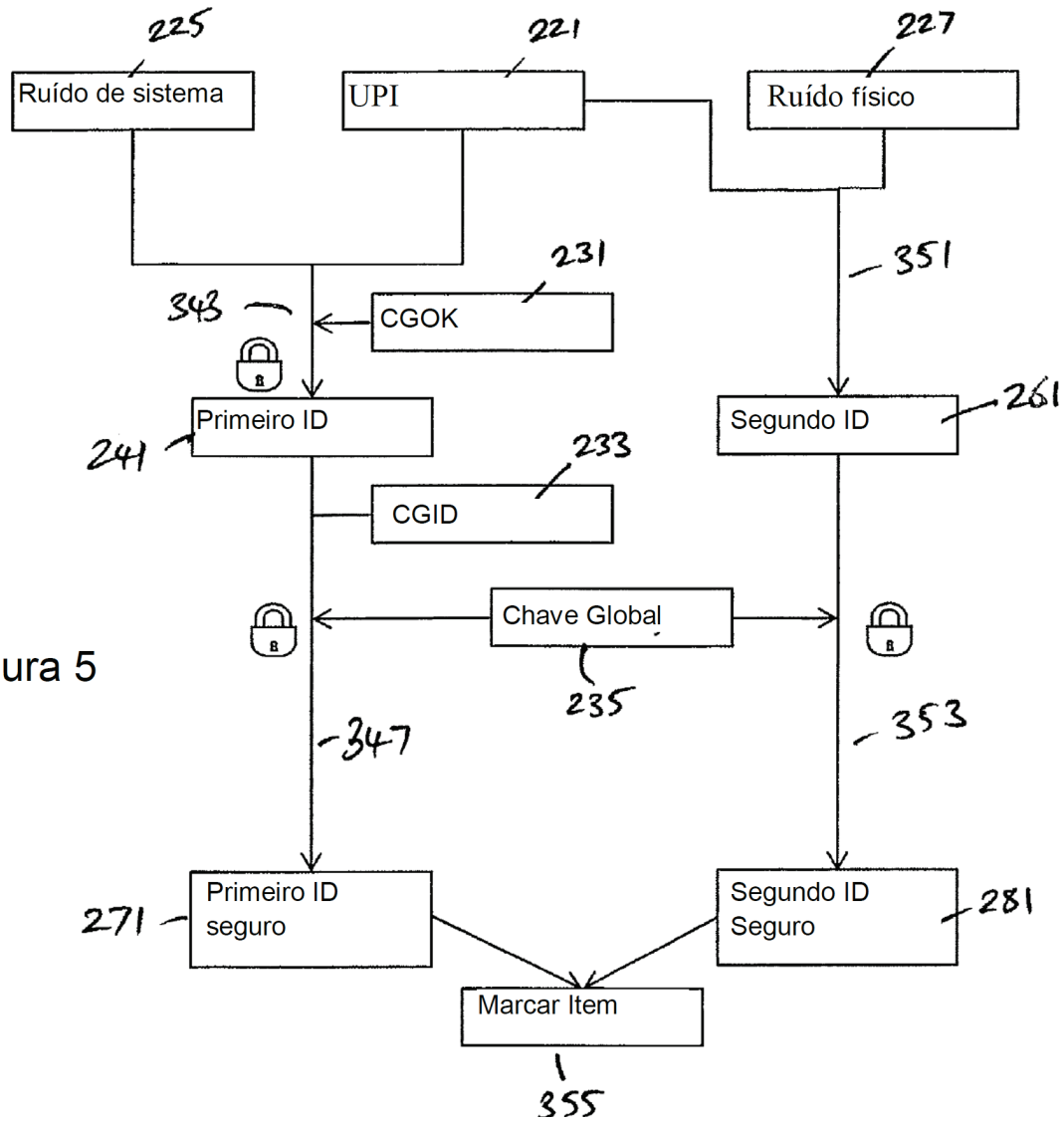

225
Ruído de sistema
221
UPI
227
Ruído físico
231
CGOK
343
351
Primeiro ID
241
Segundo ID
261
233
CGID
Chave Global
235
347
353
Primeiro ID seguro
271
Segundo ID Seguro
281
Marcar Item
355

Figura 5

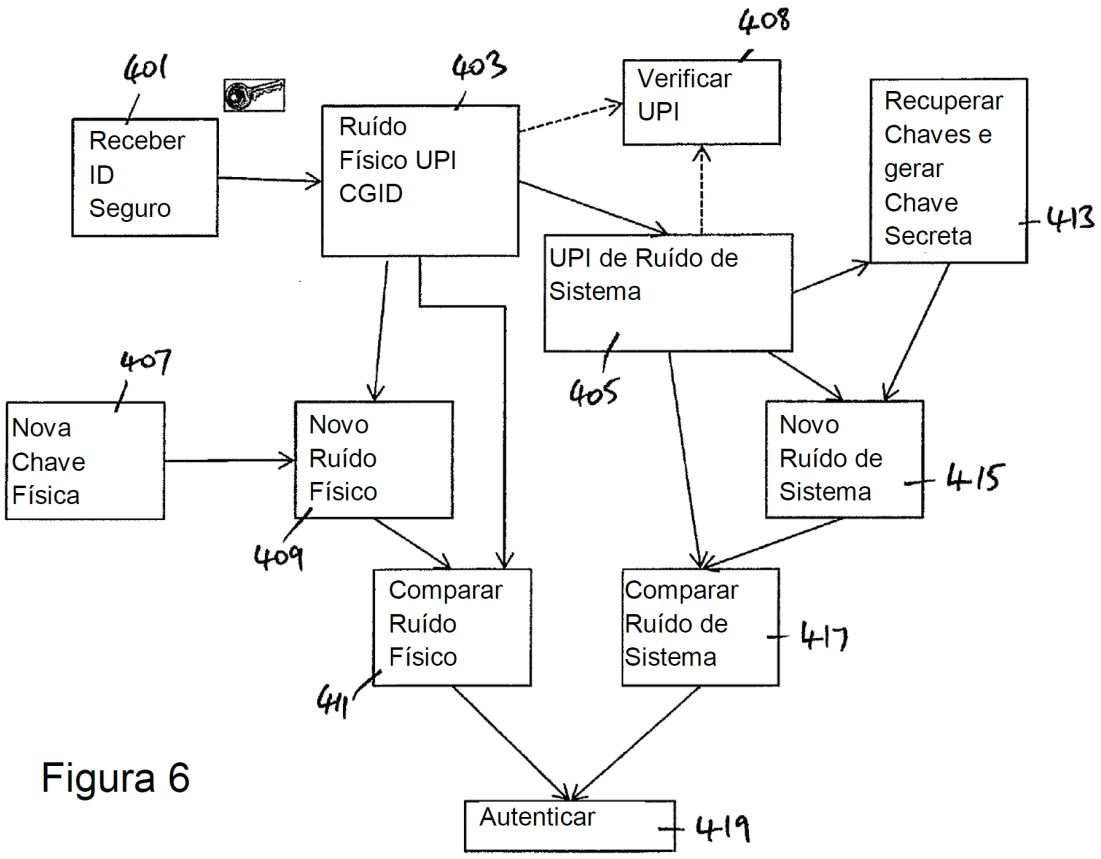

401
Receber ID Seguro
403
Ruído Físico UPI CGID
408
Verificar UPI
Recuperar Chaves e gerar Chave Secreta
413
UPI de Ruído de Sistema
405
407
Nova Chave Física
Novo Ruído Físico
409
Novo Ruído de Sistema
415
Comparar Ruído Físico
411
Comparar Ruído de Sistema
417
Autenticar
419

Figura 6