



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

(11) PI 0511313-0 B1



(22) Data do Depósito: 01/06/2005

(45) Data de Concessão: 26/12/2018

(54) Título: BEM DE CONSUMO E PROCESSO PARA PROVER O MESMO

(51) Int.Cl.: G08B 15/00; G07G 3/00; G08B 13/24; G06K 19/08.

(52) CPC: G08B 15/001; G07G 3/003; G08B 13/2417; G08B 13/2445; G06K 19/08.

(30) Prioridade Unionista: 18/06/2004 EP 04 014303.4.

(73) Titular(es): SICPA HOLDING S.A..

(72) Inventor(es): OLIVIER ROZUMEK; THOMAS TILLER.

(86) Pedido PCT: PCT EP2005052497 de 01/06/2005

(87) Publicação PCT: WO 2005/124673 de 29/12/2005

(85) Data do Início da Fase Nacional: 18/12/2006

(57) Resumo: BEM DE CONSUMO, USO DE UM PRIMEIRO E SEGUNDO ELEMENTOS DE ARMAZENAMENTO DE DADOS NO MESMO, PROCESSO PARA APLICAÇÃO DE INFORMAÇÃO CODIFICADA, PROCESSOS PARA LEITURA E PARA NOVA MONTAGEM DA INFORMAÇÃO SEGURA, PROCESSO PARA DETERMINAÇÃO DE MANIPULAÇÕES NÃO-AUTORIZADAS DA INFORMAÇÃO E PROCESSO PARA VERIFICAÇÃO DA AUTENTICIDADE DE UM CÓDIGO VISÍVEL. A invenção refere-se a um item que compreende pelo menos dois elementos de armazenamento de dados tal como, por exemplo, um transponder de RFID (2) e um código de barras (5), no qual o último é não-visível para o olho humano nu e compreende informação codificada. A invenção permite uma cópia da informação entre os dois elementos de armazenamento de dados, de modo a impedir a perda de dados inadvertida ou maliciosa. Aspectos adicionais da invenção estão relacionados com o uso interdependente ou cooperativo de ambos os elementos de armazenamento na estrutura de um esquema de localização e investigação de segurança do produto.

Relatório Descritivo da Patente de Invenção para **"BEM DE CONSUMO E PROCESSO PARA PROVER O MESMO"**.

A presente invenção refere-se a aperfeiçoamentos na segurança e confiabilidade no campo de marcação de produto, especialmente para
5 aplicações de localização e investigação em artigos, itens e/ou documentos de segurança.

Códigos de barra são geralmente usados para marcações de produto simples e confiável, tal como por exemplo o código EAN (numeração de artigo europeu) ou EAN 128, que é também adequado para informação
10 com base em ASCII. Códigos de barra são econômicos na aplicação - uma mera impressão - e facilmente lidos e decodificados com a ajuda de varredura ótica ou dispositivos de formação de imagem.

Para finalidades não-críticas, por exemplo, para marcação de artigos de supermercado ou similares, tais códigos de barra, tanto unidimensionais (1D) quanto bidimensionais (2D) são geralmente aplicados em uma
15 maneira de modo a ficarem visíveis pelo olho nu; a leitura é geralmente executada por scanners funcionando com iluminação vermelha ou perto do infravermelho (NIR), por razões de melhor contraste e disponibilidade comercial de diodos a laser de baixo custo. Sistemas de câmara de CCD ou
20 CMOS eletrônica são também cada vez mais usados em tais aplicações.

Para as finalidades que exigem um nível superior de segurança, entretanto, a informação codificada, tal como códigos de barra, pode ser aplicada em itens em uma forma, que não é visível para o olho humano nu sem a ajuda de iluminação específica e/ou dispositivos de detecção. Tintas
25 compreendendo corantes ativos com UV ou IV são conhecidas na técnica e, por exemplo, descritas em US 5.755.860, US 5.684.069 e EP 0 663 429. É para ser entendido que, no contexto da presente invenção, corantes ativos com UV ou IV compreenderão ambos corantes luminescentes ao UV ou IV, bem como absorptivos de UV ou IV. Tal informação codificada não-visível po-
30 de ser usada em aplicações de localização e investigação de produto, bem como em cédulas bancárias, papéis de segurança, por exemplo, documen-

tos de identidade ou cartões de crédito, ou em artigos de qualquer tipo.

Uma desvantagem principal dos códigos de barra, tanto do tipo visível quanto do não-visível, é sua capacidade de armazenamento limitada, que não é suficiente para certas finalidades. Além do mais, em dados casos, a adição de informação adicional seria desejável depois da aplicação do código de barras. Entretanto, nenhuma informação pode ser adicionada em um código de barra existente; somente um código de barra adicional poderia ser aplicado para essa finalidade. Finalmente, códigos de barra podem se tornar ilegíveis através de dano de superfície parcial pela abrasão (arranhões) ou pelo ataque de solventes ou outros produtos líquidos. Para lidar com esse problema, uma redundância suficiente de informação impressa deve ser geralmente provida.

Em uma tentativa diferente, uma etiquetagem de produto com base em sinal de rádio, geralmente citada como identificação de radiofrequência (RFID) é conhecida. Um sistema de RFID exige que o artigo seja etiquetado com um 'transponder', isto é, um circuito eletrônico, implementado como um microcircuito integrado de silício, que é conectado em uma antena. A dita antena pode ser, dependendo da frequência de operação, uma bobina de fio, um arco de metal fechado compreendendo uma ou várias voltas ou uma antena bipolar com extremidade aberta. O dito circuito eletrônico compreende recurso de memória com informação armazenada nele. O dito sistema de RFID também compreende pelo menos um dispositivo leitor, capaz de interagir com o transponder e ler ou escrever informação de ou para o dito recurso de memória. A distinção é feita entre transponders ativos tendo sua própria fonte de força (que deve ser mantida), e transponders passivos sem uma fonte de força própria.

No processo de leitura/gravação de um transponder passivo, o transponder é suprido com energia por um campo de radiofrequência (RF) do dispositivo leitor, assim tornando o transponder autônomo e isento de manutenção. Transponders com recurso de memória estendida permitem que uma maior quantidade de dados seja armazenada do que é possível através de códigos de barra convencionais; além do mais, a adição de in-

formação adicional ou a modificação da informação já armazenada é igualmente possível em um transponder projetado para tais finalidades. Vantagens adicionais de transponders sobre códigos de barra incluem a faixa mais estendida de cobertura para a leitura (que depende, entre outros fatores, da configuração do dispositivo leitor e da frequência do campo de RF), bem como da possibilidade de ser legível através de uma ampla variedade de materiais óticamente opacos, contanto que eles não sejam eletricamente condutores ou de outra forma absorvedores fortes de RF.

Por outro lado, uma desvantagem principal dos transponders de RFID é sua sensibilidade muito alta às influências ambientais adversas, tal como, por exemplo, intensos campos eletromagnéticos que podem eletricamente destruir o circuito no microcircuito integrado, bem como calor excessivo, ataque químico ou quebra mecânica. A resistência mecânica do conjunto do transponder de RFID é freqüentemente muito pequena; em particular, as conexões entre o microcircuito integrado e a antena são propensas à quebra. Um evento de quebra impede a leitura adicional dos dados no microcircuito integrado por recurso comum, ou até mesmo causa perda completa (destruição) dos dados.

Conseqüentemente, uma desvantagem principal do uso único dos transponders de RFID é que uma perda completa de informação devido à destruição inadvertida ou intencional do transponder pode ocorrer. Uma fraqueza adicional do uso único dos transponders é que, com uma avaria acidental de um elemento na logística de respaldo eletrônica (servidor, ligação de transferência de dados, rede, grade de energia), nenhum código de artigo pode ainda ser determinado. Um sistema de codificação com base em transponder robusto conta com uma segunda maneira paralela de reserva de informação, isto é, a duplicação não-eletrônica da parte mais importante da informação armazenada no transponder em uma segunda localização do artigo.

O Modelo de Utilidade Alemão DE 203 01 463 U1 descreve a combinação de um código de barra e um transponder em termos gerais. O transponder é planejado para melhorar a segurança do código de barras e

para permitir um processamento de máquina rápido. Entretanto, a tentativa descrita nele tem desvantagens em um contexto orientado para a segurança, onde uma remoção intencional da informação é temida: primeiro, os códigos de barra são aplicados em etiquetas ou diretamente no transponder de RFID; assim, o código de barra é óbvio como uma etiqueta e pode ser maliciosamente removido, ou o código de barras na etiqueta de RFID é perdido junto com o transponder de RFID, se o transponder é, por exemplo, maliciosamente removido ou destruído. Segundo, os próprios códigos de barra são impressos visíveis, assim tornando óbvias a existência e a localização da informação de reserva.

É um objetivo da presente invenção superar as desvantagens da técnica anterior, em particular melhorar a segurança da informação provida em um item. É um objetivo adicional da invenção prover um aspecto de segurança que permite um máximo de segurança e flexibilidade da manipulação da informação armazenada nele, para impedir a perda irrecuperável de dados, e para prover uma trajetória mais segura de acesso à informação sensível. Objetivos adicionais da presente invenção se tornarão evidentes da descrição e das reivindicações independentes.

Esses objetivos são particularmente satisfeitos por um item equipado com pelo menos dois elementos de armazenamento de dados de acordo com a reivindicação 1 e relacionado com ela, reivindicações de uso e processo independentes adicionais.

Um item de acordo com a invenção é equipado com pelo menos dois elementos de armazenamento de dados, onde o dito primeiro elemento de armazenamento de dados compreende um transponder de RFID e o dito segundo elemento de armazenamento de dados compreende um código preferivelmente impresso, que é pelo menos em parte não-visível para o olho humano nu.

De acordo com modalidades especialmente preferidas da presente invenção, o dito item é um bem de consumo, tais como, por exemplo, uma garrafa, jarro, frasco, lata, caixa, pacote, caixa de papelão, blister, saco, peça de roupa, parte sobressalente, etc.. A invenção oferece especialmente

aspectos de localização e investigação vantajosos para tais bens de consumo, que não poderiam ser obtidos de outra forma.

De modo mais preferível, o primeiro elemento de armazenamento de dados é provido no item através de uma etiqueta adesiva, de preferência na parte posterior de uma etiqueta adesiva.

Para a finalidade dessa invenção, um transponder de RFID é para ser entendido como um dispositivo de armazenamento de dados microeletrônico que pode ser remotamente lido ou gravado através de um dispositivo de interrogação de radiofrequência (RF). O transponder do dito primeiro elemento de armazenamento de dados pode ser aplicado no item tanto como tal, quanto de preferência embutido de maneira não-óbvia em cápsulas, camadas intermediárias, folhas metálicas ou similares. As várias tentativas de fixar/embutir transponders em itens diferentes são por exemplo revisadas em (a) "RFIF Handbook: Fundamentals and Applications in Contactless Smart Cards" e (b) "RFID Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten", ambos por Klaus Finkenzeller (autor), Hanser Fachbuchverlag. Com relação às várias tentativas de fixar/embutir transponders, a descrição desse documento é aqui explicitamente incorporada.

De preferência, o segundo elemento de armazenamento de dados compreende um código impresso, por exemplo um código 1D ou, mais preferivelmente, um 2D tal como códigos de barra, códigos (de barra) empilhados ou códigos de matriz, que não é visível para o olho nu. Para aplicações especiais, por exemplo, quando não é necessário ou desejado que o código de barra fique completamente escondido para o olho nu, códigos combinados compreendendo seção visível e não-visível podem ser vantajosamente aplicados. Um código 2D preferido é, por exemplo, um código de matriz 2D DataMatrix especificado pelos padrões ANSI/AIM BC11-1997 e ISO/IEC 16022. Através da redundância dos dados e uma correção de erro tais códigos como, por exemplo, o ECC-200 de RVSI (Robotic Vision Systems, Inc.) permitem o reconhecimento de códigos, que são significativamente danificados. Os ditos códigos são preferivelmente impressos, por e-

xemplo pela impressão com jato de tinta, usando por exemplo impressoras contínuas de bico único, tal como a série Domino® A, Linx 6200, Videojet Excel e Ipro, ou pelos sistemas de impressão térmico, tal como o IBM 4400, Kodak 8660 ou zebra série 110, ou pelos processos de impressão com toner, tal como impressão a laser, usando, por exemplo, LaserJet HP colorida.

De maneira mais preferível, o segundo elemento de armazenamento de dados é aplicado diretamente sobre o item, evitando com ele o uso de etiquetas adicionais ou similares, que poderiam ser facilmente arranhadas ou retiradas, acidental ou maliciosamente. No caso do transponder de RFID ser maliciosamente destruído, a informação armazenada no segundo elemento de armazenamento de dados, por exemplo, o código não-visível, permanece ainda disponível para processamento fora de linha. Assim, a aplicação da informação codificada diretamente sobre o item, em particular na forma de um código, que não é visível para o olho nu, melhora mais a segurança da informação codificada.

De acordo com uma modalidade da presente invenção, o segundo elemento de armazenamento de dados é aplicado, preferivelmente por jato de tinta ou outro recurso de impressão, diretamente sobre o item, ao invés de sobre o primeiro elemento de armazenamento de dados. Entretanto, a aplicação do segundo elemento de armazenamento de dados sobre o primeiro elemento de armazenamento de dados não é excluída, já que essa pode ser a única tentativa adequada para itens que têm uma superfície muito limitada disponível para aplicar a ambos um transponder e um código impresso ao lado um do outro.

De acordo com uma outra modalidade particularmente preferida, a informação codificada, em particular o código impresso, é também ligada a um elemento de segurança com base em material, que é por exemplo provido por corantes específicos incorporados na tinta, material de transferência térmica ou toner usado para imprimir o código. Corantes adequados são luz absorvente em áreas de comprimento de onda particular, de preferência fora da faixa visível do espectro, e ficam preferivelmente reemitindo luz sob iluminação específica. Além do mais, eles devem ser aplicáveis em uma den-

sidade de modo a aparecer não-visível para o olho humano nu. Em termos gerais, como a não-visibilidade é almejada, tais corantes devem ser ativos, isto é, absorver, emitir ou ser excitáveis na faixa UV (comprimentos de onda entre cerca de 200nm a cerca de 400nm) e na faixa perto do IV (comprimentos de onda entre cerca de 700nm a cerca de >1100nm) ou até mesmo além de 1100 nm; entretanto, corantes adequados podem também ser excitados ou emitir na faixa visível (comprimentos de onda entre cerca de 400nm a cerca de 700nm), contanto que eles não absorvam significativamente nessa faixa. Categorias adequadas de corantes incluem, mas não são limitadas a polimetinas, cianinas, fenoxazinas, ftalo e naftalocianinas, terilenos, coumarinas, triarilmetanos, derivados de squarylium e crocomium e complexos de terra rara.

É particularmente preferido que o código impresso seja aplicado em uma maneira de modo a não permitir uma visualização usando uma fonte de iluminação geralmente disponível; corantes ativos com UV comuns que emitem na faixa visível (400 a 700 nm) são dessa forma evitados como uma escolha não-perfeita, enquanto que os corantes ativos com IV são preferidos. De maneira mais preferível, uma leitora adequada tanto permite a iluminação com uma faixa específica de comprimentos de onda de excitação, preferivelmente entre 200 e 1100 nm, quanto possui recurso de detecção sensível a uma faixa específica de comprimentos de onda de emissão preferidos, de preferência entre 200 nm e 400 nm, ou entre 700 nm e 1100 nm.

De preferência, o item de acordo com a invenção adicionalmente transporta uma marcação de segurança. Tal marcação de segurança pode ser baseada, por exemplo, em uma tinta óticamente variável, tinta magnética, tinta luminescente e/ou tinta absorvedora de IV. Dependendo do uso planejado da marcação de segurança, ela pode ser projetada não-visível, parcialmente visível ou visível para o olho nu. De preferência, a dita marcação de segurança é aplicada sobre a etiqueta transportando o primeiro elemento de armazenamento de dados, e mais preferivelmente serve como um identificador de autenticidade do dito item e/ou etiqueta. A marcação de segurança adicional pode compreender ou consistir em um terceiro elemento de arma-

zenamento de dados, que preferivelmente é pelo menos parcialmente, de maneira mais preferível completamente não-visível para o olho humano nu; além do mais, a marcação de segurança pode servir como um identificador de autenticidade do dito item, de preferência independentemente do dito primeiro e dito segundo elemento de armazenamento de dados.

Um outro aspecto da presente invenção é o uso de um primeiro e um segundo elemento de armazenamento de dados em um item, como recurso de armazenamento de reserva mútuo para a informação contida no dito primeiro e dito segundo elemento de armazenamento de dados preso no dito item. Assim, um código de barras pode servir como um recurso de armazenamento de reserva para a informação armazenada em um transponder de RFID, ou o transponder pode servir como um recurso de armazenamento de reserva para a informação codificada por um código de barras, respectivamente. Assim, algumas das desvantagens principais de ambos os recursos de armazenamento são com isso superadas: o transponder de RFID é por exemplo propenso à avaria, com a perda simultânea de dados, em campos de RF eletromagnéticos fortes, o que, por sua vez, não prejudica o código impresso. Por outro lado, o código impresso não pode ser novamente editado e não tem capacidade de armazenamento suficiente para algumas aplicações; ele pode ser além disso acidentalmente esfregado, danificado por arranhão ou retirado por solventes; tais influências ambientais, entretanto, geralmente prejudicam menos o transponder de RFID.

Mesmo se é possível aplicar o segundo elemento de armazenamento de dados sobre o primeiro elemento de armazenamento de dados, por exemplo, um código de barras sobre um transponder de RFID, é preferido para a maior parte das aplicações separar fisicamente ambos os recursos de armazenamento de modo a melhorar a segurança do sistema: se um transponder e um código de barras não-visível são colocados em um item em localizações fisicamente distintas, um dano malicioso ou acidental tem menos probabilidade de danificar ambos os recursos de armazenamento ao mesmo tempo e causar uma perda completa dos dados armazenados.

Um aspecto adicional da invenção está relacionado com um pro-

cesso de aplicação de informação codificada sobre um item 1, compreendendo as etapas de:

- pelo menos parcialmente ler a informação contida em um primeiro elemento de armazenamento de dados, de preferência compreendendo um transponder de RFID 2 que é preso no item 1;

- com base na informação de leitura, disparar a aplicação de um segundo elemento de armazenamento de dados sobre o dito item 1, de preferência recorrendo a uma impressora para aplicar a informação codificada sobre o dito item 1.

Assim, o processo facilmente permite recorrer a uma impressora para aplicar um registro de informação codificada no item, o dito registro somente dependendo de um transponder de RFID previamente preso e preferivelmente uma leitura parcial da informação armazenada na memória do transponder.

Isso abre novas possibilidades para descentralização: por exemplo, transponders de RFID pré-fabricados podem ser despachados para uma instalação onde eles são presos em artigos (itens), e, subseqüentemente, os transponders presos permitirão a impressão do dito registro de informação codificada, independente de contato adicional com um computador hospedeiro remoto ou similar. É para ser entendido que a informação provida pelo transponder de RFID e a utilização da impressora devem ser vantajosamente criptografadas.

É também preferido que o registro da informação codificada, aplicada no item como descrito acima, pelo menos parcialmente compreenda informação que já está contida no transponder. Assim, a informação codificada impressa satisfaz uma função de reserva para a informação mais sensível que está armazenada no transponder, impedindo a perda completa de dados no caso de dano acidental, bem como uma segunda segurança no caso de falsificação.

Um aspecto adicional da presente invenção está relacionado com um processo de permitir a leitura da informação segura em um item compreendendo dois elementos de armazenamento de dados, o dito pro-

cesso compreendendo as etapas de:

- pelo menos parcialmente ler a informação de um primeiro elemento de armazenamento de dados;

- com base na informação de leitura, depois do processamento opcional da dita informação, prover acesso para a informação contida em um segundo elemento de armazenamento de dados.

É para ser entendido que dentro dessa finalidade um código impresso pode conter informação necessária para prover acesso à informação contida no transponder de RFID, ou vice-versa, que o transponder pode conter informação para prover acesso à informação contida no código impresso. De preferência, a informação inicialmente lida de um dos elementos de armazenamento de dados, por exemplo, tanto um código impresso quanto um transponder de RFID, provê um recurso tal como um código ou uma chave criptográfica ou um complemento para um código ou uma chave criptográfica, ou similar, que subsequente permite acesso aos dados no segundo elemento de armazenamento de dados.

Dentro desse aspecto da invenção, o primeiro elemento de armazenamento de dados pode ser projetado somente como um recurso para prover acesso ao segundo elemento de armazenamento de dados, sem ele próprio conter qualquer informação adicional com relação ao item marcado de forma alguma; ou alternativamente, tal informação crítica por si própria, que está armazenada em um dos elemento de armazenamento de dados, poderia também depender da informação de complemento armazenada no outro elemento de armazenamento de dados.

Um aspecto adicional da invenção está relacionado com um processo de nova montagem da informação segura em um item transportando dois elementos de armazenamento de dados, compreendendo as etapas de:

- pelo menos parcialmente ler a informação de um primeiro elemento de armazenamento de dados;

- pelo menos parcialmente ler a informação de um segundo elemento de armazenamento de dados;

- combinar a dita informação de leitura do dito primeiro e dito se-

gundo elementos de armazenamento de dados, por meio do que a dita informação segura é novamente montada.

Um outro aspecto da presente invenção está relacionado com um processo para determinação de manipulações não-autorizadas da informação contida em um primeiro elemento de armazenamento de dados, de preferência um transponder de RFID que é preso em um item, o dito processo compreendendo as etapas de:

- determinar um verificador, por exemplo uma resenha de mensagem ou soma de verificação de pelo menos parte da informação contida no dito primeiro elemento de armazenamento de dados;

- aplicar um segundo elemento de armazenamento de dados sobre o dito item, contendo o dito verificador, por exemplo, resenha de mensagem ou soma de verificação;

- verificar manipulações de informação contidas no dito primeiro elemento de armazenamento de dados, comparando o verificador, por exemplo, a resenha de mensagem ou soma de verificação, determinado diretamente do primeiro elemento de armazenamento de dados com o verificador, por exemplo, a resenha de mensagem ou soma de verificação, contido no segundo elemento de armazenamento de dados.

De acordo com essa modalidade da presente invenção, manipulações não-autorizadas da informação contida em um transponder de RFID são facilmente detectadas.

Um verificador, no contexto da presente invenção, é para ser entendido como qualquer conjunto de dados derivado da informação original, que permite, através da aplicação de um esquema de processamento de dados algorítmicos, verificar a integridade da informação que foi originalmente armazenada. Um exemplo típico de um verificador elementar é uma soma de verificação. Um verificador é também para ser entendido como o próprio verificador, quando obtido a partir do esquema de processamento de dados algorítmicos, ou como uma forma criptografada do dito verificador.

Assim, a informação contida em um transponder de RFID preso em um item pode, em uma tal maneira, ser verificada com relação a manipu-

lações não-autorizadas. Isso acrescenta um nível adicional de segurança na informação em um item.

De acordo com uma modalidade adicional, a invenção permite verificar a autenticidade de um código visível em um item, em um processo compreendendo as etapas de:

- armazenar uma indicação do dito código visível em um primeiro ou um segundo elemento de armazenamento de dados, de preferência um transponder de RFID preso ou a ser preso no dito item;
- determinar a autenticidade do dito código visível, comparando o código visível e/ou a informação contida nele, com a indicação do dito código visível, contido no dito primeiro ou segundo elemento de armazenamento de dados.

Dessa maneira, manipulações maliciosas de códigos geralmente aplicados, tal como códigos EAN, podem ser facilmente detectadas, assim adicionando um aspecto de segurança a mais em um item protegido de acordo com a invenção.

A invenção será agora também explicada por meio de um exemplo ilustrativo, sem a invenção ser limitada a essa modalidade específica.

Figura 1: item com dois elementos de armazenamento de dados (código de barras e RFID).

Figura 2: item com dois elementos de armazenamento de dados e marcação de segurança adicional.

A Figura 1 mostra um item 1 compreendendo um primeiro elemento de armazenamento de dados 2 e um segundo elemento de armazenamento de dados 5. O item 1 pode ser um produto a ser localizado ou investigado, por exemplo, durante seu ciclo de serviço, ou um item de segurança tais como uma cédula bancária, um cartão de crédito, um documento de identidade ou similar. De acordo com essa modalidade exemplar, o elemento de armazenamento de dados 2 é personificado como um transponder de RFID comercialmente disponível, compreendendo um microcircuito integrado 3 para processar e armazenar informação e uma antena 4 para prover comunicação e abastecimento de energia em conjunto com uma leitora ex-

terna/dispositivo gravador (não mostrado). O segundo elemento de armazenamento de dados 5 dessa modalidade é um código de barras, por exemplo, um código de barras 2D do tipo DataMatrix.

De preferência, ambos o primeiro elemento de armazenamento de dados 2 e o segundo elemento de armazenamento de dados 5 são fisicamente separados um do outro, embora seja vantajoso dispô-los em proximidade, de modo a permitir uma leitura simultânea ou até mesmo, por exemplo, uma leitura disparada do código de barras pelo reconhecimento do transponder por uma leitora adequada. O código de barras 5 é preferivelmente aplicado (impresso) diretamente sobre o item em uma forma para torná-lo não-visível para o olho humano, por exemplo, por meio de um corante preferivelmente ativo com IV que pode ser incorporado na tinta de impressão. De preferência, ambos, o código de barras 5 e o transponder de RFID 2 são aplicados no item (ou até mesmo integrados no item no caso do transponder 2), tal que eles virtualmente não acrescentam para a altura do item 1.

Ambos o transponder de RFID 2 e/ou o código de barras 5 podem servir como uma fonte de reserva da informação para o outro elemento de armazenamento de dados 2 ou 5, respectivamente. Além do mais, o código de barras 5 e o transponder 2 podem compreender, cada um, informação relevante para prover acesso à informação no outro elemento de armazenamento de dados 2 ou 5, respectivamente, ou para a montagem da informação complementar provida de ambos os elementos de armazenamento de dados 2 e 5. É para ser entendido que o acesso à informação armazenada em ambos os elementos de armazenamento de dados 2 e 5 pode também ser protegida por uma chave criptográfica.

Uma modalidade prática adicional da invenção é fornecida na Figura 2, compreendendo uma etiqueta de localização de produto L (aqui: uma etiqueta de garrafa sensível à pressão) em um item 1, aqui uma garrafa. A etiqueta L, de dimensões 42 x 86 mm, compreende um identificador de RFID 2 de 64 bits, classe 0 (leitura somente), 900 MHz, suprido por MATRICS (agora Symbol Technologies Inc., Western Division Sales Office, 555 12th Street, Suite 1850, Oakland, Califórnia 94607, Estados Unidos). O identifica-

25

dor consiste de um circuito de silício (circuito integrado), conectado em uma antena bipolar plana do tipo meandro através de um arco de acoplamento (transformador de impedância). O identificador suporta a codificação de um código alfanumérico variável de 22 dígitos (no presente exemplo:

5 "0X0000C80507A000840CCD").

Além do identificador de RFID 2, o item 1 do presente exemplo compreende um código DataMatrix® de 16x16 invisível luminescente com infravermelho (marca SICPADATA®, 5), impresso com uma impressora de jato de tinta contínua, onde o código DataMatrix® é impresso diretamente

10 sobre o item, separado da etiqueta.

A marca SICPADATA® exemplarmente suporta um código alfanumérico variável de 16 dígitos. No exemplo, a marca SICPADATA® replica os últimos 16 dígitos do código de 22 dígitos do identificador de RFID (isto é, "C80507A000840CCD").

15 A etiqueta da garrafa sensível à pressão também compreende pelo menos uma marcação de segurança adicional 6 para identificação aberta, semi-secreta e/ou secreta. No presente exemplo, uma tinta de mudança de cor de vermelho para verde (SICPASHIFT®, para identificação pelo olho nu) é impressa em negativo em um fundo bi-luminescente ao UV, tal que

20 uma escrita luminescente aparece em positivo e em cores diferentes com a irradiação com luz UV de onda curta (254nm) ou onda longa (360nm). A marcação 6 aqui adicionalmente compreende SICPAGUARD®, um elemento de segurança secreto legível por máquina. É para ser observado que a marcação de segurança 6 pode ser aplicada, tanto sobre a etiqueta (como mos-

25 trado no exemplo), quanto diretamente sobre o item.

A etiqueta é produzida de acordo com a seqüência seguinte das etapas de operação:

(i) Impressão e acabamento da etiqueta sensível à pressão primária (impressão de leiaute decorativo com tintas padrões, eventualmente

30 impressão de marcações de segurança com tintas de segurança (aberta, secreta, "forense"; numeração estática), verniz, corte em matriz, divisão, enrolamento em um carretel;)

(ii) Aplicação do identificador de RFID na parte posterior da etiqueta, inscrevendo o código dentro do circuito integrado de RFID (se não feito já na fábrica), e verificação da parte de RFID para código e funcionamento correto (remoção de etiquetas ilegíveis do lote de produção);

5 (iii) Impressão da marca SICPADATA®, verificação e checagem cuidadosa dela com o código de RFID (remoção de etiquetas ilegíveis ou incorretas do lote de produção).

10 Em uma situação de produção, as etapas (ii) e (iii) são geralmente executadas em linha, em uma e a mesma máquina. A presente modalidade de exemplar foi realizada no laboratório, onde etiquetas com identificadores de RFID em série já aplicados, codificados e verificados, foram usadas. As marcas SICPADATA® foram aplicadas uma por uma, usando uma estação de impressão com jato de tinta, seguido por uma verificação e checagem cuidadosa dos códigos.

15 A etiqueta do presente exemplo pode ser usada em um número de maneiras diferentes; a ser mencionado de modo exemplar:

20 1) Para o processamento totalmente automatizado de bens de consumo, aqui garrafas (tal como preparações médicas) transportando a etiqueta, o código SICPATRACE® eletrônico pode ser exclusivamente usado. A informação alfanumérica de 22 dígitos é recuperada para cada garrafa com a sua passagem através de uma porta de RFID, e a garrafa pode então ser associada com um destino determinado, por exemplo, com a embalagem automatizada de garrafas de preparação médica, os códigos individuais das últimas são recuperados e armazenados juntos com a outra informação de
25 embalagem e despacho.

30 2) Para a simples verificação de autenticidade no ponto de vendas do bem de consumo, aqui a garrafa, a marcação de segurança 6 pode ser usada; por exemplo o consumidor final, que comprou uma garrafa da preparação médica, pode verificar a etiqueta 6 com, por exemplo, o aspecto de mudança de cor, eventualmente a comparando com a etiqueta de uma garrafa prévia que ele comprou. O varejista final poderia também eventualmente desejar verificar o aspecto luminescente ao UV no momento que ele

desempacota as garrafas.

- 3) Para inspeção da cadeia de varejo, o segundo elemento de armazenamento de dados 5 (aqui: um código SICPATRACE®) e o código de RFID eletrônico são lidos e comparados com a ajuda de um dispositivo de detecção preferivelmente combinado, que é capaz de detectar e decodificar o código de matriz de pontos de outra forma invisível. Os códigos recuperados podem também ser cruzados, em linha ou fora de linha, com a informação de embarque de embalagem que foi armazenada em uma localização central para os itens correspondentes no momento de sua fabricação, de modo a verificar o desvio do produto.

- 4) No caso de dados ou elementos de segurança incongruentes ou omissos, que é fortemente indicativo de uma falsificação, o aspecto secreto legível por máquina SICPAGUARD® da marcação de segurança 6, ou qualquer outro aspecto forense que está naturalmente presente na etiqueta ou no item, ou que foi propositadamente introduzido na etiqueta ou no item, pode ser usado como uma verificação final para evidência, antes de começar por exemplo, uma instauração legal.

REIVINDICAÇÕES

1. Bem de consumo (1) transportando pelo menos dois elementos de armazenamento de dados, em que um primeiro elemento de armazenamento de dados é um transponder de RFID (2) e um segundo
5 elemento de armazenamento de dados é um código preferivelmente impresso (5), que é pelo menos parcialmente não-visível a olho humano nu, e em que o segundo elemento de armazenamento de dados é provido diretamente no bem de consumo, **caracterizado** pelo fato de que o primeiro elemento de armazenamento de dados e o segundo elemento de armazenamento de
10 dados são colocados no bem de consumo em posições fisicamente distintas a fim de evitar que dano acidental ou proposital danifique simultaneamente ambos os elementos de armazenamento de dados.

2. Bem de consumo, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o código preferivelmente impresso (5) é
15 aplicado por um método selecionado do grupo consistindo na impressão a jato de tinta, impressão térmica e impressão com toner.

3. Bem de consumo, de acordo com qualquer uma das reivindicações 1 ou 2, **caracterizado** pelo fato de que o primeiro elemento de armazenamento de dados é provido no bem de consumo (1) através de uma
20 etiqueta adesiva, de preferência na parte posterior de uma etiqueta adesiva.

4. Bem de consumo, de acordo com qualquer uma das reivindicações de 1 a 3, **caracterizado** pelo fato de que dito bem de consumo (1) transporta adicionalmente uma marcação de segurança (6), em que dita
25 marcação de segurança (6) serve especialmente como um identificador de autenticidade de dito bem de consumo, de preferência independentemente dos ditos primeiro e segundo elementos de armazenamento de dados.

5. Bem de consumo, de acordo com qualquer uma das reivindicações de 1 a 4, **caracterizado** pelo fato de que o segundo elemento de armazenamento de dados compreende um corante ativo com
30 infravermelho (IV) ou ultravioleta (UV), de preferência escolhido do grupo consistindo em polimetinas, cianinas, fenoxazinas, ftalo e naftalocianinas, terilenos, cumarinas, triarilmetanos, derivados de squarylium e croconium, e

complexos de terra rara.

6. Bem de consumo, de acordo com qualquer uma das reivindicações de 1 a 5, **caracterizado** pelo fato de que o segundo elemento de armazenamento de dados é ou compreende um código 1D ou 2D.

5 7. Bem de consumo, de acordo com qualquer uma das reivindicações de 1 a 6, **caracterizado** pelo fato de que o dito segundo elemento de armazenamento de dados serve como um recurso de armazenamento de reserva para informação contida no dito primeiro elemento de armazenamento de dados preso ao dito bem de consumo.

10 8. Processo para prover um bem de consumo (1), conforme definido em qualquer uma das reivindicações de 1 a 7, **caracterizado** pelo fato de compreender as etapas de:

- pelo menos parcialmente ler a informação contida em um primeiro elemento de armazenamento de dados compreendendo um transponder de RFID (2) que é preso ao bem de consumo (1);

15

- com base na informação de leitura, disparar a aplicação de um segundo elemento de armazenamento de dados sobre dito bem de consumo (1), recorrendo a uma impressora para aplicar a informação codificada, especialmente um código (5) sobre dito bem de consumo (1), fisicamente separado do transponder de RFID (2).

20

9. Processo, de acordo com a reivindicação 8, **caracterizado** pelo fato de que o segundo elemento de armazenamento de dados aplicado no bem de consumo (1) pelo menos parcialmente compreende informação que já está contida no primeiro elemento de armazenamento de dados.

25

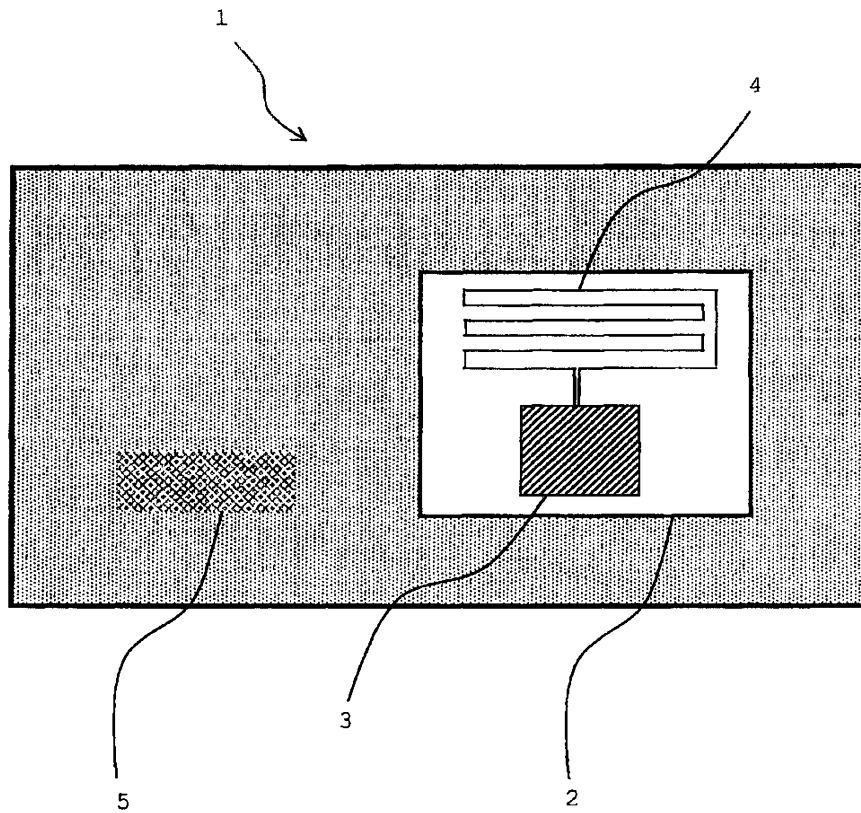
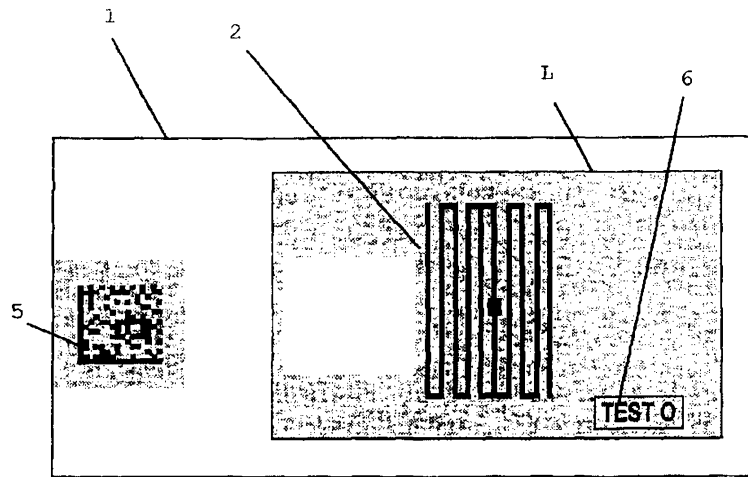


Fig.1

**Fig.2**