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

(21) **PI 0618427-8 A2**

BRPI0618427A2

(22) Data de Depósito: 20/11/2006
(43) Data da Publicação: 17/04/2012
(RPI 2154)

(51) Int.Cl.:
E05B 39/00
G09F 3/03
G06K 19/06
E05B 73/00

(54) Título: LACRE DE ALTA SEGURANÇA - REUTILIZÁVEL E A PROVA DE ADULTERAÇÕES

(30) Prioridade Unionista: 23/11/2005 FR 0511835

(73) Titular(es): Novatec S.A

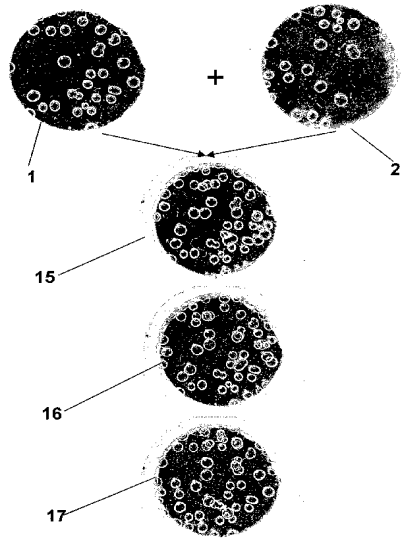
(72) Inventor(es): Clément Kaiser, Francis Bourrieres, Franck Bourrieres

(74) Procurador(es): Brasil Sul Marcas e Patentes S/C Ltda.

(86) Pedido Internacional: PCT FR2006002564 de 20/11/2006

(87) Publicação Internacional: WO 2007/060323de 31/05/2007

(57) Resumo: LACRE DE ALTA SEGURANÇA- REUTILIZÁVEL E A PROVA DE ADULTERAÇÕES, lacre de extrema segurança que pode ser reutilizado indefinidamente porque o elemento de autenticação evolve de maneira caótica cada vez que o lacre é aberto e, assim, o reabilita para o uso. Esse lacre é composto de, pelo menos. dois autenticadores (1) e (2), onde pelo menos um é móvel com relação ao outro, na posição aberto. Esses dois autenticadores ficam fixos e estáveis na posição fechada. Em cada nova posição fixa, os dois autenticadores cooperam para gerar uma nova característica autenticadora que é armazenada em um banco de dados, para que possa ser comparada durante uma verificação. Essa característica será cancelada e substituida por outra quando o lacre for fraudulentamente ou deliberadamente aberto e, assim, oferecerá prova de que foi aberto.



"LACRE DE ALTA SEGURANÇA – REUTILIZÁVEL E A PROVA DE ADULTERAÇÕES".

Campo de aplicação da invenção

A invenção propõe um lacre de alta segurança – reutilizável e a prova de adulterações, sem qualquer deterioração ou destruição do mecanismo e com isso possibilita a detecção de qualquer tentativa de adulteração. Esse tipo de lacre pode ser usado para: controlar e verificar tentativas de violação em uma conexão ou sistema e tentativas sem sucesso de adentrar um local protegido, ambos mantendo a integridade do objeto e seu conteúdo e os protegendo de pessoas não autorizadas; ou, por outro lado, permitir que sejam abertos por um agente e essa abertura seja devidamente registrada.

Histórico

Existem vários diferentes tipos de sistemas para verificar tentativas de intrusão em um sistema ou local protegido contra a entrada de pessoas não autorizadas, que autenticam e identificam os objetos como sendo os originais. Os métodos modernos mais comuns são:

- alarmes eletrônicos, esses sistemas disparam um alarme quando da tentativa de intrusão e esses alarmes não param de soar até que seja usado um código secreto, determinado previamente, por exemplo, ou uma impressão biométrica autorizada.

- sistemas de vigilância por vídeo que possibilitam o registro e controle, em tempo real, do acesso ou pontos cruzados,

- cartões (com chip, magnéticos ... etc.), códigos secretos ou biometria, tornando possível o controle do acesso ao local ou sistema protegido.

Todos esses métodos são adaptados para funcionarem como controles da entrada e saída de pessoas, de locais públicos ou particulares. Lacres de segurança, para a segurança de acesso ao sistema ou mesmo para prevenir o acesso em geral ao local ou sistema, exceto por pessoal autorizado, são usados, muito comumente. Os lacres também são usados para garantir a integridade ou mesmo a autenticidade de um determinado objeto. Esses lacres podem variar em sua forma,

dependendo da aplicação. A inspeção da integridade física do lacre assegura, em teoria, a não violação do sistema ou objeto. O nome "sistema" é considerado em seu sentido mais amplo, pode ser, por exemplo, uma montagem de elementos associados, uma unidade ou condições não especificadas como, por exemplo, um frasco que precisa preservar a integridade de seu conteúdo, também pode ser um sistema de informações.

A presente invenção, particularmente, se concentra na aplicação de proteção de dados de processamento importantes, como descrito abaixo.

O lacre mais antigo que se conhece é o lacre de cera que, geralmente, era marcado pelo selo de uma autoridade. Existem também lacres de metal e plástico que também servem como uma pulseira de identificação e que podem ser apertados progressivamente. Esses lacres não são reusáveis porque a destruição de um lacre desses é irremediável e mostra a violação do local ou sistema protegido. Existem também lacres metálicos com "contas" na forma de cordões com ranhuras ou fios trançados de metal onde as duas extremidades são unidas em uma seção de metal mais maleável, geralmente chumbo, que pode ser apertada com uma ferramenta especial, deixando uma marca específica no parte de chumbo, lacrando o objeto ou local; isso também é chamado de preenchimento. Esse tipo de lacre é muito usado em medidores de água, gás e energia elétrica. Similarmente, na grande gama de lacres existentes hoje em dia, podemos incluir placas de identificação ou suportes de todos os tipos, geralmente feitos em metal, gravadas, marcadas ou até impressas. Essas placas ou suportes, geralmente, identificam um objeto, sistema complexo, máquina ou indivíduo através de um cartão de identidade, esse suporte conterá o selo ou marca de uma autoridade, possibilitando sua autenticação. As aplicações que implementam placar e suportes de identificação são inúmeras e variadas, entre as mais freqüentes estão: motores de veículos com placas de identificação do fabricante do motor e do fabricante do veículo, assim como placas com números de inspeções; placas de identificação e homologação de ferramental; placas em materiais e em máquinas elétricas e eletrônicas, etc... Em geral, essas placas de identificação são listadas em arquivos ou bancos de dados administrativos ou dos fabricantes.

Todos esses tipos de lacres e suportes de identificação apresentam duas desvantagens significativas: a primeira é que todos eles são facilmente reproduzíveis, com sinopses médias idênticas, incluindo o elemento ou lacre de identificação e, ainda, são fáceis de adquirir e em grande quantidade; em segundo lugar, a substituição do objeto ou sistema protegido. Para alguns, a conexão entre o lacre e os suportes e as peças necessárias para prevenir a separação ou abertura é ineficiente e pode ser facilmente destruída enquanto se preserva intacto o lacre ou suporte; por exemplo, uma junta que pode ser dissolvida por um produto químico ou solvente apropriado e que permita a recuperação do lacre, o alcance de uma área fechada e a reposição do lacre original na mesma posição e, assim, permitir que os dados acessados e alterados não sejam detectados. Também é possível substituir o lacre original por uma cópia e, assim, fazer com que a cópia passe pela original.

Outro grande problema é a razão custo/segurança. Em geral, quanto mais seguro, mais caro, o que representa um problema significativo quando o lacre é usado em aplicações grandes que consumam muitos lacres, onde o ideal seria poder contar com lacres de baixo custo e com um alto nível de segurança, o que contradiz as soluções atuais.

Da mesma maneira, para proibir o acesso físico a sistemas eletrônicos, que contenham dados confidenciais, é muito comum o uso de hologramas muito específicos e mesmo sistemas de alta segurança. Porém, o qualificador de alta segurança era mais adaptado no passado do que hoje em dia, através de meios reais, permitindo que eles hoje sejam facilmente reproduzidos, identicamente, com um baixo nível de qualidade, se comparada com a qualidade do original.

Ainda, os hologramas não são individualizados, i.e., eles são idênticos nas mesmas séries e, assim, é fácil para uma pessoa não autorizada obter esses hologramas, abrir o gabinete protegido, destruindo o holograma e depois substituí-lo por um idêntico ao original. Se não for possível obter o holograma, um falsificador pode, facilmente, destacar o holograma do gabinete, sem destruí-lo e, mais tarde, colocá-lo na posição original. Assim, de uma maneira ou de outra, é muito fácil para certas pessoas violar um sistema e, fisicamente, acessar dados confidenciais, por

exemplo, uma caixa preta com memória de armazenamento e, também, substituir um objeto por outro. Em geral e seja lá qual for o método usado, o lacre de segurança deve evitar o comprometimento físico do recipiente e o acesso ao conteúdo desse recipiente e, por outro lado, expor imediatamente qualquer violação ou intrusão, se ela ocorrer. Um lacre de segurança não pode impossibilitar o ataque ao sistema ou acesso a um local ou recipiente; por outro lado, se bem concebido e integrado ao produto ou local, que precisa ser protegido, pode dissuadir o invasor e deixar evidências da tentativa de invasão. Ele age, acima de tudo, como um meio de defesa que, em geral, é capaz de evidenciar uma tentativa de ataque à integridade física do sistema ou objeto, onde ele foi instalado. Dependendo da aplicação, o lacre conhecido como lacre de segurança pode ter diferentes formas. Um lacre, na verdade, é uma junta que une o lacre a um ou mais elementos marcados por um selo de autorização (por exemplo, selo do Estado).

Em todas essas aplicações, o problema é justamente a possibilidade de reprodução idêntica desses lacres, para um acesso fraudulento aos conteúdos do local ou sistema.

A patente protegida FR2848698, do mesmo requerente e inventor, relaciona-se a um processo de identificação e autenticação, sem um leitor específico, de um objeto ou ser vivo. Nesse documento, recomenda-se a anexação de um identificador de difícil ou impossível reprodução, dentro do objeto ou ser vivo, para essa identificação ou autenticação. Como notado, esse documento não se refere a um sistema de monitoramento de não-intrusões em um local protegido ou da integridade de um objeto e esse é, precisamente, o objeto dessa invenção. O processo descrito no documento FR2848698 não possibilita, em qualquer caso, uma garantia para o sistema ou proteção do local. Na verdade, a inserção de um identificador no objeto não evita o acesso do invasor ao objeto, modificando-o, analisando-o e substituindo o mesmo identificador sem detecção, mesmo que isso não seja reproduzível. No pior dos casos, é até possível retirar o autenticador sem destruir o objeto e inseri-lo em outro objeto.

O documento WO 01/11591 descreve um dispositivo que possibilita a identificação de objetos. Esse identificador tem o efeito de englobar uma matriz de lentes que geram um efeito visual em três dimensões, o que não quer reivindicar que não é reproduzível. O que é revelado nesse documento é completamente diferente dessa invenção, primariamente porque:

- seguindo o exemplo da patente FR2848698, esse identificador não permite a garantia da descrição da abertura ou intrusão do objeto ou local protegido.

- O identificador descrito nesse documento é reproduzível *ad infinitum* já que repousa em um processo de fabricação, complexo, mas totalmente controlado. Conseqüentemente, a singularidade desse identificador não pode ser assegurada.

- O identificador não é associado com um banco de dados.

O documento EP 1087334 descreve um sistema de lacres ligado à um transponder que possibilita o controle remoto eletrônico e uma identificação questionável. Esse tipo de transponder não é único já que é perfeitamente possível para qualquer pessoa ou organização ter meios de produção para eles e fabricar diversas unidades com o mesmo número. Conseqüentemente, é totalmente possível abrir o dispositivo descrito e acessar seu conteúdo e de completamente reconstituir duas cápsulas idênticas para as primeiras respostas com um transponder dando as mesmas respostas do primeiro. Na verdade, a falha nesse tipo de dispositivo está da cadeia de fornecimento de cápsulas e transponders, se uma pessoa ou organização inescrupulosa quiser desviar peças e reconstituir um lacre idêntico ao original. Ainda, esse tipo de lacre não é reusável depois de aberto. Na presente invenção, como será visto mais adiante, o processo de não-intrusão repousa em um autenticador singular que não pode ser identicamente reproduzido e registrado em um banco de dados e, conseqüentemente, mesmo que ache um jeito de subutilizar os autenticadores, o autenticador original não será de utilidade já que não pode ser registrado em qualquer banco de dados.

A patente WO02/3368A descreve um lacre reutilizável onde a passagem da posição fechada para a posição aberta implica na ativação de um gerador aleatório de código eletrônico. A leitura desse código mostra se o lacre foi

aberto, se o código mudou ou não e, se não aberto, se o código não mudou. Os objetivos dessa patente são idênticos aos objetivos dessa invenção, mas os meios são diferentes e também os resultados em termos de segurança – muito mais alta na invenção desenvolvida. Assim, prova de não violação, nessa patente, é dada pela leitura de um mostrador eletrônico, mas tal leitura pode ser identicamente produzida se os algoritmos de geração de código forem conhecidos. Da mesma maneira, sem conhecer os algoritmos de geração de código, esse lacre reutilizável pode ser substituído por outro, em todos os sentidos, idêntico, onde o código lido pode ser idêntico ao original, mas a programação terá sido feita por um sistema eletrônico interno que falsifica os códigos. É assim, portanto, completamente impossível trocar esse tipo de lacre por outro com as mesmas características de autenticação.

A patente US-A-4118057 descreve um lacre reutilizável onde as características de autenticação são dadas por um dispositivo com várias esferas coloridas que aparecem em uma janela. O grande número de possíveis combinações faz com que seja impossível reproduzir duas combinações idênticas para assegurar a abertura ou quebrar o lacre. O sistema é completamente mecânico, não existem elementos eletrônicos, a substituição de um lacre por outro lacre, idêntico em todos os sentidos e com a mesma combinação de esferas é, teoricamente, possível em razão de até as esferas serem reproduzíveis perfeitamente em tamanho e cor. Portanto, a única coisa que é preciso fazer é alcançar o mostrador e posicionar as esferas. Dessa maneira, se parece difícil modificar o dispositivo durante o uso, é sempre fácil preparar um dispositivo similar, com antecedência, com uma combinação idêntica ao do lacre original, i.e., com o mesmo posicionamento das esferas coloridas.

A Patente US2003/04647 descreve autenticadores com bolhas, sempre únicas e impossíveis de ser reproduzidas e com os meios associados para serem interpretadas. Esse autenticador com bolha, embora impossível de reproduzir, não pode agir sozinho dentro da estrutura dessa invenção de um lacre reutilizável já que não pode provar que um lacre foi aberto e fechado mais uma vez. Por outro lado, como será visto na descrição dessa invenção, esse tipo de autenticador é

particularmente bem adaptado à presente invenção como um autenticador individual, associado com outro autenticador de tipo comparável, mas inevitavelmente diferente nessas características. Essa unidade coopera de maneira caótica para obter um número infinito de novas posições estáveis não reproduzíveis.

Descrição da invenção

A invenção tem como propósito uma solução total para três dificuldades que aparecem com o uso do lacres conhecidos:

1) fazer com que os lacres não sejam intercambiáveis

2) fazer com que o lacre do sistema, local ou objeto protegido seja fisicamente interdependente, de maneira que em caso de intrusão, ou tentativa de intrusão ou substituição o lacre fique visivelmente alterado.

3) fazer com que o lacre seja reutilizável para reduzir custos e preserva o alto nível de segurança do dispositivo.

4) poder controlar, no local, se o lacre foi aberto ou se houve tentativa de abrir o lacre.

De acordo com uma primeira característica particularmente inovadora e inventiva, o lacre de alta segurança dessa invenção é indefinidamente reutilizável e também permite a detecção e prova de que foi aberto ou fechado, o que corresponde à uma nova utilização. Essa característica essencial constitui o coração da invenção, sustentado pelo fato que ela obtém uma nova característica de autenticação a cada vez que o lacre é aberto e, conseqüentemente, fechado novamente. O lacre integra um dispositivo que permite a evolução, não controlada, de sua característica de autenticação, em cada estado de mudança, i.e., no movimento da posição fechada para a posição aberta (Figura 1A), cancelando a característica de autenticação anterior da posição aberta para a posição fechada (Figura 1B), restaurando uma nova característica de autenticação graças à auto-geração caótica de novas características de autenticação causadas pela mudança de estado, já mencionada. Cada característica de autenticação é armazenada em uma memória protegida ou banco de dados benchmark, que comprovará a abertura ou tentativa de abertura do lacre.

Outra característica da invenção faz uso de, pelo menos, dois autenticadores 1, 2 que sempre mostram características idênticas únicas e não reproduzíveis para evitar a duplicação. Pelo menos um dos autenticadores conhecidos age em separado, de maneira instável, quando o lacre está na posição de desbloqueio (Figura 1A) ou aberto e age em conjunto de maneira estável e possível de ser lida quando o lacre está fechado ou na posição de bloqueado (Figura 1B).

Outra característica da invenção é a ação conjunta e estável dos autenticadores individuais não reproduzíveis 1, 2 que permitem a geração de novos autenticadores comuns 15, 16, 17, completamente aleatórios, dependendo da posição relativa conhecida dos autenticadores individuais 1, 2.

Outra característica da invenção é a ação em separado e instável dos autenticadores 1, 2 gerados, pelo menos, por um movimento relativo de um autenticador comparado ao (com) o(s) outro(s).

Outra característica da invenção são os autenticadores comuns 15, 16, 17 gerados pela nova posição dos autenticadores individuais 1, 2 que tornam possível a criação de um novo código ou assinatura de onde a representação é armazenada em um banco de dados local e/ou remoto. Outra característica importante é a característica de autenticação, única e impossível de ser reproduzida, dos autenticadores individuais 1, 2, resultado de um processo caótico.

De acordo com outra característica da invenção, as características de autenticação são bolhas visíveis auto-geradas dentro do material. Como exemplo, esse processo caótico pode ser a formação de bolhas durante o endurecimento do material, mencionado acima, que constitui o autenticador. Assim, diferente dos dispositivos anteriores, que são resultado de um processo de fabricação, perfeitamente controlado pelo homem e, portanto, reproduzível por outro homem usando as mesmas ferramentas, cada autenticador usado na presente invenção é único e impossível de ser reproduzido porque é resultado de um processo não controlado. Essa característica torna possível livrar-se finalmente da possibilidade de obtenção de autenticadores e lacres idênticos aos originais. Com a segurança

intrínseca de cada autenticador, a segunda segurança é adicionada pela soma, ou melhor, combinação da ação conjunta dos autenticadores.

De acordo com outra característica, já que a singularidade e individualidade física de cada autenticador não podem ser reproduzidas de maneira idêntica, ou seja, é impossível ou extremamente difícil clonar um autenticador, podem ser usadas heterogeneidades aleatórias dispersadas em um volume transparente. Essas heterogeneidades visivelmente distintas são capturadas, por exemplo, na forma de uma fotografia ou outras representações, caracterizando a forma do identificador e armazenadas em uma memória ou banco de dados, na forma de imagens bi-dimensionais ou de forma numérica, calculada com base nos elementos marcantes de posicionamento, dimensões, etc., das heterogeneidades inundadas em volume. As duas formas de representação, imagem ou numérica, podem coexistir. Da mesma maneira, é possível integrar partículas magnéticas nessa forma de identificação, tornando possível fazer a codificação de outra maneira.

Outra característica e um modo preferível são autenticadores individuais transparentes volumais, feitos de vidro, cerâmica, plástico ou polímeros contendo bolhas visíveis, de onde o número, a forma e a provisão são resultado de uma auto-geração caótica, não controlável. Esse tipo de autenticador é particularmente interessante porque será sempre único e impossível de ser clonado pelas pessoas. A patente EP0l 904039.3 do mesmo requerente e inventor sugere esse tipo de autenticador de bolha com um sistema de leitura adequado. No caso dessa invenção, é uma questão de usar esse autenticador de bolha em um processo particular onde a finalidade ou meta é bloquear ou proibir o acesso à sistemas e locais ou verificar a integridade com as informações associados com o objeto original. Da mesma maneira que previamente explicado, uma representação na forma de imagem e/ou representação numérica é armazenada em um banco de dados para permitir a verificação da integridade da característica de autenticação.

De acordo com outra característica, a memória e/ou banco de dados, onde a representação da característica de autenticação é armazenada, ficam, fisicamente, no sistema e/ou local e/ou suporte protegido(s), mas o conteúdo pode

ser lido remotamente, de um ponto externo, por pessoa autorizada. Essa representação do autenticador constitui uma chave de acesso para o sistema físico e/ou informações lógicas. De maneira prática e para muitos usos, o leitor das características autenticadas memoriza a leitura feita no momento do último movimento e, automaticamente, compara as novas informações. Em caso de discordância, um sinal sonoro ou luminoso informa ao controlador que ocorreu uma abertura do lacre. Sem sair da estrutura dessa invenção, um identificador como um código de barras ou um identificador eletrônico (RFID) pode ser associado a cada lacre, assim, apresentando um endereço no banco de dados, para que as comparações sejam feitas mais facilmente.

De acordo com outra característica, a imagem e/ou representação numérica do autenticador pode ser consultada por uma rede de telecomunicações padrão, como a Internet.

Em outra característica, o conteúdo armazenado na representação numérica e/ou imagem pode ser consultado por um controlador ou agente autorizado, de diferentes maneiras. Uma das maneiras consiste em uma comparação visual da representação em imagem, armazenada em um banco de dados remoto e/ou no local com o autenticador físico, analisando a similaridade do posicionamento das bolhas e heterogeneidades. Existem diversos métodos para visualizar a imagem: tanto diretamente na tela, integrado ao sistema ou local protegido ou em tela dissociada ou anexa (telefone celular com acesso a Internet), ou impressa em papel por uma impressora integrada ou usando uma impressora dissociada do sistema ou local protegido. Se o banco de dados não for local, mas remoto, pode ser usado um código de chamada constituindo o identificador do autenticador lá no banco de dados distante, o código de chamada pode ser numérico, alfa-numérico, código de barras, tira magnética, microchip, etc. Fica óbvio que o banco de dados, tanto remoto como local, serão seguros e protegidos de qualquer tentativa de modificação ou substituição de informações.

Outra característica da invenção é o processo de monitoramento de não-intrusão em um sistema ou local protegido ou a integridade de um objeto,

executado por comparação automática do autenticador, usando um leitor adaptado com representação digital armazenada em banco de dados local ou remoto.

No caso do lacre reutilizável, de acordo com a presente invenção, a representação de autenticação armazenada em um banco de dados mudará com cada novo uso do lacre, é essa correspondência que é armazenada no banco de dados e aquilo realmente levantado no lacre e que torna possível atestar que o lacre não foi aberto.

Na Figura 1, um dispositivo de acordo com o modo operacional da invenção de preferência é representado, isso constituindo apenas um exemplo não restritivo. A Figura 1A mostra o dispositivo aberto e livre. A Figura 1B mostra o dispositivo fechado e bloqueado. A Figura 1C é uma vista de cima do dispositivo, mostrando a parte de autenticação. Uma cobertura (4) engloba um autenticador (2) transparente com bolhas (8) geradas aleatoriamente. Esse autenticador (2) é fixado na cobertura (4) englobando um mostrador (7). O corpo (3) engloba um autenticador transparente (1), cujo fundo é refletor, por exemplo, uma placa de prata. Da mesma maneira que para o autenticador (2), as bolhas (8) foram geradas aleatoriamente. No corpo (3) é disposta uma face (10) onde esferas (11) podem circular livremente. O autenticador (1) é colocado nas esferas (11) e pode se mover livremente sobre as esferas dentro dos limites da caixa. A presilha (5) constitui o elo que permite a ligação do lacre de segurança, como um todo, com o objeto ou recipiente que precisa ser protegido. Esse elo (5) pode ser removido do lacre através do dispositivo intermediário (12) colocado cegamente na caixa (13). Para remover o elo (5), para abrir o recipiente ou alcançar o sistema protegido, é necessário alinhar a passagem (14) da cobertura (4) com a porção do corpo correspondente (3).

Na Figura 1A, a cobertura (4) é insuficientemente desparafusada do corpo (3) de maneira que, de um lado, seja possível remover o elo (5) do corpo (4), com o qual está ligado e alinhar a abertura (14) com a caixa (13) e, por outro lado, desunir os autenticadores (1) e (2). Durante essa operação, o autenticador (1), completamente livre das esferas (11), se moverá e ocupará uma posição aleatória instável que mudará permanentemente com a última ação exercida no sistema. Os

autenticadores (1) e (2) são inacessíveis de fora. Na Figura 1B, a cobertura (4) está na posição fechada e bloqueada. Nessa posição, o elo (5) fica completamente ligado ao corpo (3) fechado pela cobertura (4). Essa posição também permite o bloqueio dos autenticadores (1) e (2), por pressão e assim a estabilização do autenticador (1), que estava móvel na posição aberta. Assim, essa posição bloqueada corresponde necessariamente a uma nova relativa e estável posição dos autenticadores (1) e (2), o que é diferente da posição estável anterior, tornando possível provar que para alcançar uma nova posição de autenticação relativa e estável é necessário liberar a cobertura (4). Com cada posição estável sendo registrada em um banco de dados pela leitura da posição associada com as bolhas de dois autenticadores transparentes, fica fácil comparar todas as novas e relativas posições de bolha e, assim, provar a abertura que provocou essa mudança.

A Figura 2 representa uma fotografia tirada conforme a presente invenção, mostrando a posição inicial de cada autenticador (1) e (2), então, sucessivamente associado em (15), (16) e (17), depois de três liberações e três fechamentos, assim, mostrando as várias combinações e oferecendo diferentes assinaturas.

A Figura 3 representa a mesma coisa da Figura 2 exceto pelo fato de que a iluminação é diferente, criada de outra maneira pelas bolhas associadas.

Esse lacre reutilizável, de alta segurança, de acordo com a invenção encontrará seu lugar não só em aplicações que demandem um extremamente alto nível de segurança, por exemplo, para o transporte de substâncias perigosas, mas também para aplicações mais banais onde o nível de segurança é certamente menor, mas onde o investimento inicial pode ser amortizado por um grande número de reutilizações que, numa análise final, custará muito menos que os lacres descartáveis. Nesse último caso e como exemplo podemos citar os medidores de água, gás, energia elétrica, etc.

Da mesma maneira esse tipo de lacre pode ser usado para o controle de acesso de agentes, em zonas supervisionadas, quando do retorno, por exemplo, usando um leitor, uma nova assinatura da abertura do lacre no banco de dados.

REIVINDICAÇÃO

1.) um lacre de alta segurança, reutilizável indefinidamente, que permite a detecção e comprovação da abertura do lacre e sua re-utilização, pela integração de um dispositivo permitindo a evolução não controlada de sua característica de autenticação a cada mudança de estado i.e., no momento da passagem da posição fechado para a posição aberto (Figura 1A) cancelando a precedente característica de autenticação e da posição aberto para a posição fechado (Figura 1B) restaurando novas características de autenticação graças à auto-geração caótica de novas características de autenticação in 15, 16, 17 causada pela mudança de estado já mencionada; cada característica de autenticação 15, 16, 17 é armazenada em uma memória de referência protegida, para provar uma abertura ou tentativa de abertura do lacre, **caracterizada pelas** características de autenticação 15, 16, 17 são resultado da ação de dois autenticadores 1, 2, únicos e não reproduzíveis, com os já mencionados autenticadores agindo separadamente de maneira instável, pelo menos um deles, quando o lacre está na posição desbloqueada ou posição aberta (Figura 1A) e agindo em conjunto, de maneira estável, quando o lacre está na posição fechado ou posição bloqueado (Figura 1B), tornando possível criar um novo código ou assinatura no banco de dados.

2.) Um lacre de alta segurança, reutilizável indefinidamente, que permite a detecção e comprovação da abertura do lacre e sua re-utilização, pela integração de um dispositivo permitindo a evolução não controlada de sua característica de autenticação a cada mudança de estado, de acordo com a reivindicação 1, **caracterizada pela** ação conjunta e estável dos autenticadores individuais não reproduzíveis 1, 2 tornando possível a geração de um novo autenticador 15, 16, 17 completamente aleatório, dependendo da posição relativa dos autenticadores individuais 1 e 2 conhecidos.

3.) Um lacre de alta segurança, reutilizável indefinidamente, que permite a detecção e comprovação da abertura do lacre e sua re-utilização,de acordo com as reivindicações 1 e 2, **caracterizada pela** ação separada e instável dos autenticadores 1, 2 gerada, pelo menos, pelo movimento relativo de um autenticador comparado ao

(com) o outro.

4.) Um lacre de alta segurança, reutilizável indefinidamente, que permite a detecção e comprovação da abertura do lacre e sua re-utilização, de acordo com as reivindicações de 1 a 3 **caracterizada pelo** novo comum autenticador gerado pela nova posição dos autenticadores individuais 1, 2, permitindo a criação de novos códigos 15, 16, 17 ou assinatura cuja representação é armazenada em um banco de dados local ou remoto.

5.) Um lacre de alta segurança, reutilizável indefinidamente, que permite a detecção e comprovação da abertura do lacre e sua re-utilização, de acordo com as reivindicações de 1 a 4, **caracterizada por** um autenticador característico, individual, único e impossível de ser reproduzido, resultado de um processo caótico.

6.) Um lacre de alta segurança, reutilizável indefinidamente, que permite a detecção e comprovação da abertura do lacre e sua re-utilização, de acordo com as reivindicações de 1 a 5, **caracterizada por** características de autenticação que são bolhas visíveis auto-geradas no material.

Fig. 1A

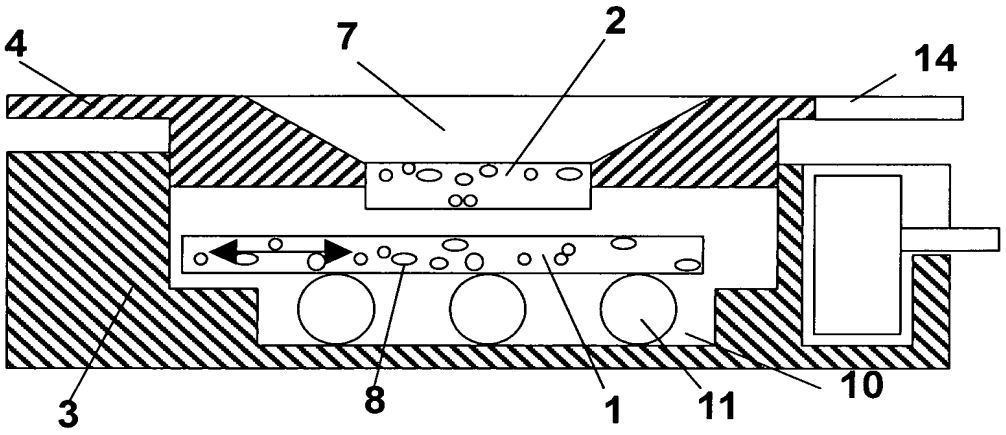


Fig. 1B

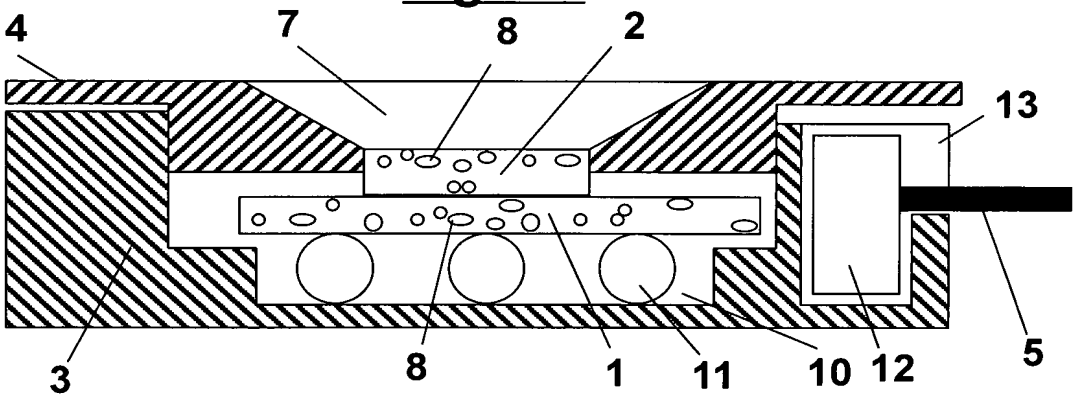


Fig. 1C

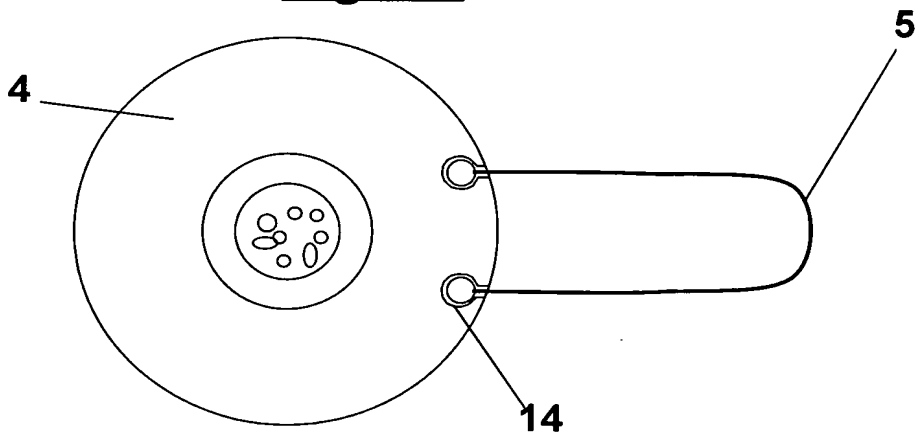


Fig. 2

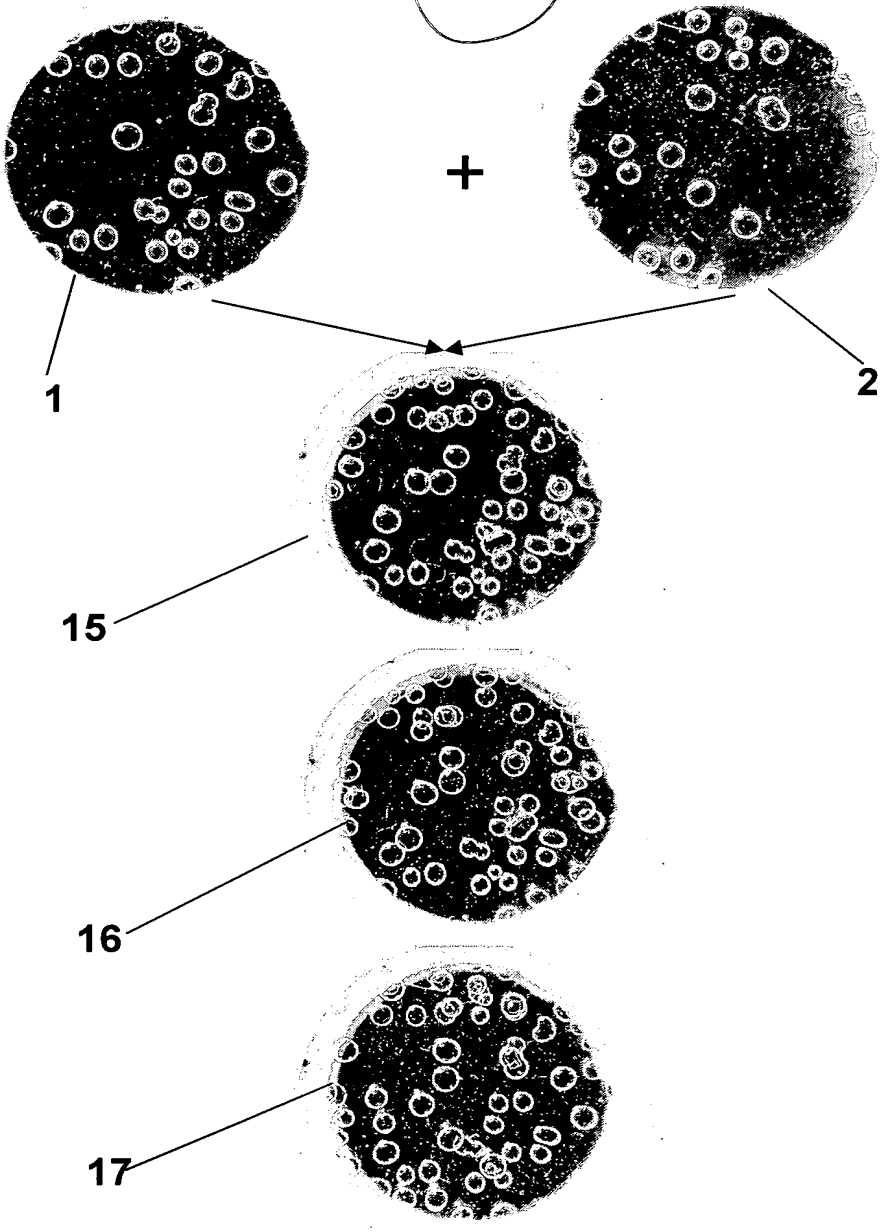
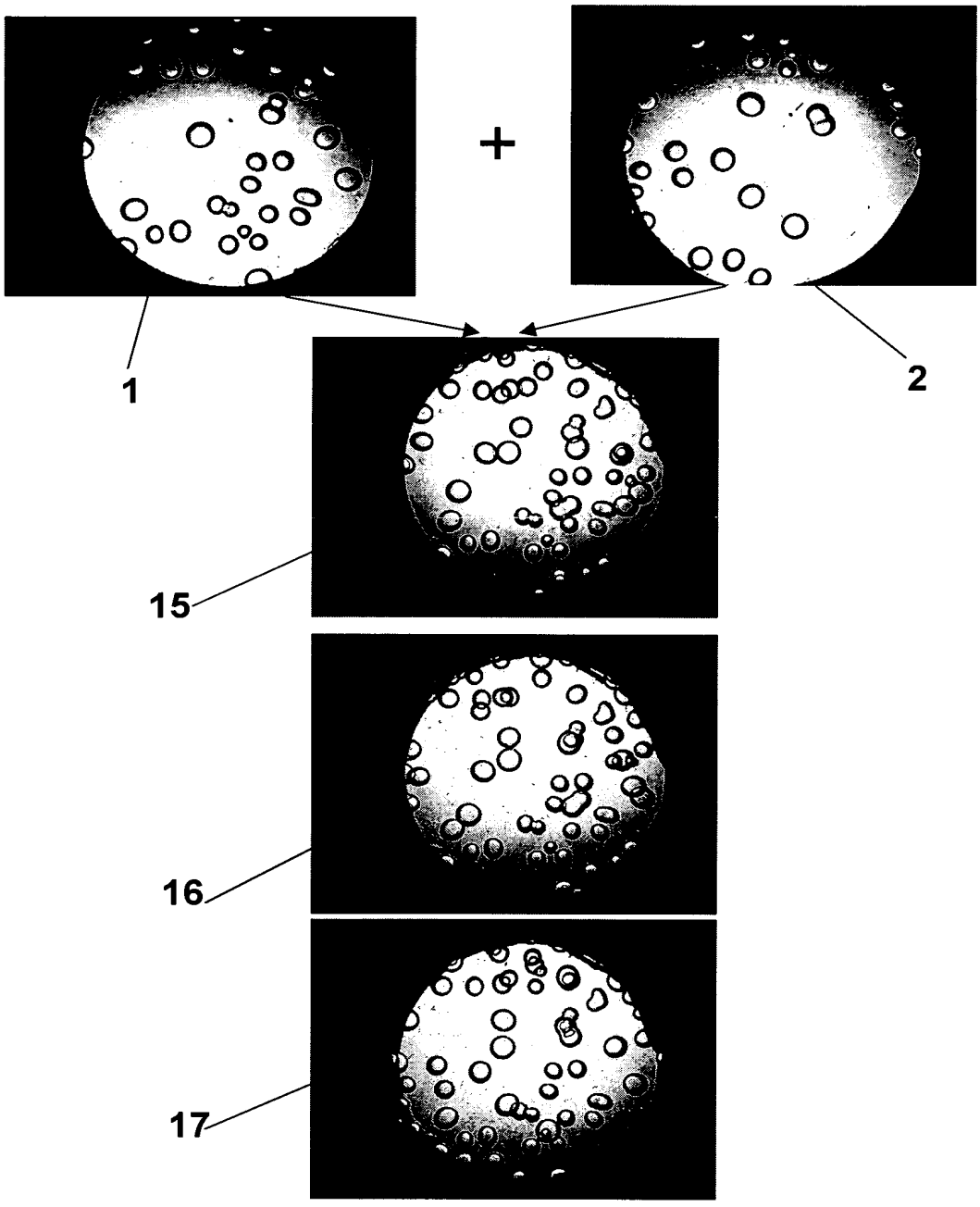


Fig. 3



PI0618427-8

RESUMO

"LACRE DE ALTA SEGURANÇA – REUTILIZÁVEL E A PROVA DE ADULTERAÇÕES", lacre de extrema segurança que pode ser reutilizado indefinidamente porque o elemento de autenticação evolve de maneira caótica cada vez que o lacre é aberto e, assim, o reabilita para o uso. Esse lacre é composto de, pelo menos, dois autenticadores (1) e (2), onde pelo menos um é móvel com relação ao outro, na posição aberto. Esses dois autenticadores ficam fixos e estáveis na posição fechada. Em cada nova posição fixa, os dois autenticadores cooperam para gerar uma nova característica autenticadora que é armazenada em um banco de dados, para que possa ser comparada durante uma verificação. Essa característica será cancelada e substituída por outra quando o lacre for fraudulentamente ou deliberadamente aberto e, assim, oferecerá prova de que foi aberto.