

(12) FASCÍCULO DE PATENTE DE INVENÇÃO

| | |
|--|---|
| (22) Data de pedido: 2009.05.19 | (73) Titular(es): SECURECODE LTD KÄRNIGSBERGER STR. 15 91083 BAIERSDORF DE |
| (30) Prioridade(s): 2008.05.20 DE 102008001880 | |
| (43) Data de publicação do pedido: 2011.02.16 | (72) Inventor(es): MARKUS KAULARTZ DE OLIVER REISER DE MICHAEL ZICH DE SIMON BAUER DE DANIEL KOBSDAJ DE |
| (45) Data e BPI da concessão: 2015.01.14 092/2015 | (74) Mandatário: MANUEL BASTOS MONIZ PEREIRA RUA DOS BACALHOEIROS, 4 1100-070 LISBOA PT |

(54) Epígrafe: **MÉTODO E DISPOSITIVO PARA IDENTIFICAR OBJECTOS**

(57) Resumo:

A INVENÇÃO REFERE-SE A UM MÉTODO PARA A IDENTIFICAÇÃO DE UM OBJECTO QUE COMPREENDE PELO MENOS UM IDENTIFICADOR DE OBJECTO COM UM CÓDIGO DE OBJECTO QUE É UTILIZADO PARA VERIFICAR A AUTENTICIDADE DO OBJECTO. O MÉTODO COMPREENDE OS SEGUINTE PASSOS: A CRIAÇÃO DE UM SISTEMA DE CÓDIGO ÚNICO ALEATÓRIO CONSTITUÍDO POR UM PRIMEIRO E UM SEGUNDO CÓDIGO DO SISTEMA, A PRIMEIRA PARTE DO CÓDIGO DO SISTEMA A SER GERADO A PARTIR DE UM PRIMEIRO CONJUNTO DE CARACTERES POR UM PRIMEIRO MÉTODO ALEATÓRIO E A SEGUNDA PARTE DO SISTEMA CÓDIGO A SER GERADO A PARTIR DE UM SEGUNDO CONJUNTO DE CARACTERES POR UM SEGUNDO MÉTODO DE POUPANÇA ALEATÓRIO E O CÓDIGO DO SISTEMA EM CONJUNTO COM PELO MENOS UMA PRIMEIRA INFORMAÇÃO ESPECÍFICA DO OBJECTO NUMA PRIMEIRA MEMÓRIA DE DADOS, A PRIMEIRA PARTE DO CÓDIGO DO SISTEMA QUE ESTÁ SENDO CRIPTOGRAFADA POR UM PRIMEIRO MÉTODO DE CODIFICAÇÃO E A SEGUNDA PARTE DO CÓDIGO DO SISTEMA POR UM SEGUNDO MÉTODO DE CODIFICAÇÃO ANTES DE SER SALVO, A CRIAÇÃO DE UMA CHAVE DE ENCRIPTAÇÃO ALEATÓRIA DE UM TERCEIRO CONJUNTO DE CARACTERES POR UM TERCEIRO MÉTODO ALEATÓRIO, A CRIAÇÃO DE UM IDENTIFICADOR DE ATRIBUIÇÃO ÚNICA POR UM MÉTODO DE ATRIBUIÇÃO E DE POUPANÇA DA CHAVE DE CRIPTOGRAFIA, IDENTIFICADOR DE ATRIBUIÇÃO E PELO MENOS UM SEGUNDO PEDAÇO ESPECÍFICO DO OBJECTO DE INFORMAÇÕES EM UM SEGUNDO MEMÓRIA DE DADOS A CRIAÇÃO DO CÓDIGO OBJECTO, QUE CONSISTE NA PRIMEIRA PARTE DO CÓDIGO DO SISTEMA E A CHAVE DE ATRIBUIÇÃO, A CRIPTOGRAFIA DO IDENTIFICADOR DO OBJECTO POR UM QUARTO MÉTODO DE CRIPTOGRAFIA E SALVAR O CÓDIGO DO SISTEMA CRIPTOGRAFADO JUNTO COM O IDENTIFICADOR DO OBJECTO CODIFICADO EM UMA TERCEIRA MEMÓRIA DE DADOS E A FIXAÇÃO DO CÓDIGO OBJECTO PARA O OBJECTO.

DESCRIÇÃO

MÉTODO E DISPOSITIVO PARA IDENTIFICAR OBJECTOS

A presente invenção refere-se a um método e um dispositivo para a identificação de objectos e para a verificação da autenticidade dos objectos etiquetados e em particular para um sistema de rotulagem à prova de falsificação dos fármacos e / ou medicamentos, bem como para a verificação da identificação por um consumidor.

Vários métodos têm sido desenvolvidos para a rotulagem dos produtos, tais como medicamentos, vestuário, transportadores de som ou semelhantes, a fim de dar aos fabricantes, comerciantes, autoridades aduaneiras, consumidores etc., a possibilidade de verificar a autenticidade das mercadorias. Estes métodos são supostamente para permitir que os consumidores, por exemplo, para verificar a autenticidade dos bens adquiridos, a fim de proteger-se, assim, a partir de produtos de contrafacção, nomeadamente de drogas e / ou medicamentos falsificados, o que, possivelmente, não têm os efeitos desejados ou mesmo ter efeitos prejudiciais.

A DE 43 41 880 A1 descreve um sistema de controlo para objectos com suportes de dados, nos quais os dados podem ser armazenados como um código de identificação, e com equipamentos externos para aquisição de dados e de processamento de dados auxiliada por computador, que pode ser utilizado para protecção de imitação proibida e recreação de artigos. O fabricante garante dados do sistema de controlo -específica, que são armazenados como um código de identificação do suporte de dados, tal como um chip de RFID. O portador de dados é anexado ao artigo a ser protegido. Tais chips RFID conhecidos são, no entanto, não

à prova de falsificação, uma vez que são possíveis uma falsificação ou recriação de suportes de dados similares, bem como uma reprogramação ou a destruição do suporte de dados por métodos conhecidos. A possibilidade de manipular os suportes de dados limita a fiabilidade de um sistema de controlo correspondente consideravelmente. Além disso, um dispositivo especial, com que o suporte de dados é lido, é necessário para a verificação da autenticidade do código de identificação. Este equipamento normalmente não está disponível, especialmente para o consumidor, devido à diversidade dos diferentes portadores de dados ou objectos, de modo que uma verificação simples e precisa de itens não está disponível, especialmente para o consumidor.

A EP 0 889 448 B1 descreve um método no qual os objectos são fornecidos com uma etiqueta, em que um padrão não reproduzível é colocado. O padrão não reproduzível é produzido a partir da descrição do objecto. Neste método, a verificação da etiqueta é realizada através da detecção com um dispositivo especial. No entanto, esses dispositivos não estão disponíveis no local para os consumidores e a verificação das etiquetas não está, portanto, disponível especialmente para os consumidores. Além disso, tais dispositivos especiais para verificação não são fáceis de operar, de modo que existem erros inevitáveis na verificação por pessoas inexperientes, como o consumidor, o que afecta a fiabilidade do método em causa.

O objectivo da invenção, portanto, é o de propor um método e um dispositivo para a identificação de objectos e para a verificação da autenticidade de objectos adequadamente marcados, que são muito precisos e fáceis de usar.

O objecto da invenção é resolvido por um método para a identificação de um objecto, que tem, pelo menos, um identificador de objecto, com um código de objecto, que é utilizado para a verificação da autenticidade do objecto, e que tem as seguintes etapas: um gerador de código de sistema único aleatório, consistindo de uma primeira e uma segunda parte do código do sistema, a primeira parte do código do sistema a ser gerado a partir de um primeiro conjunto de caracteres por um primeiro método aleatório e a segunda parte do código do sistema a partir de um segundo conjunto de caracteres por um segundo método aleatório, e armazenar o código do sistema em conjunto com pelo menos uma primeira informação específica do objecto numa primeira memória de dados, pelo que a primeira parte do código do sistema é codificado através de um método de codificação primeiro e o segundo parte do código do sistema por um segundo método de codificação antes de ser salvo; geração de uma chave de codificação aleatória a partir de um terceiro conjunto de caracteres por um terceiro método aleatório, gerar um identificador de transmissão única por um método de transmissão e armazenamento da chave de codificação, o identificador de tarefa e pelo menos uma segunda informação específica do objecto numa segunda dados memória; geração do código de objecto, que consiste, pelo menos, da primeira parte do código do sistema e o identificador de transmissão, encriptar o código de sistema por um terceiro método de codificação, encriptar o identificador do objecto por um quarto método de codificação e armazenar o código do sistema encriptado juntos com o identificador do objecto codificado em uma terceira memória de dados; e fixação do código de objecto ao objecto.

Um aspecto da presente invenção propõe que o método que inclui a característica pela qual a activação é uma informação armazenada na primeira memória de dados para além do código armazenado do sistema, que indica se o código de sistema está activo ou não activo, em que o código do sistema pode ser verificado somente após a activação. A segurança da identificação do objecto é melhorada com vantagem por isso, uma vez que a identificação do objecto é activada somente antes da venda do objecto para o consumidor e, portanto, uma cadeia de fornecimento inseguro desde o produtor até o consumidor está superada.

Outro aspecto do presente invento propõe que o código objecto seja dividido em um primeiro e um segundo código de objecto. É ainda proposto que a segunda parte do código objecto seja ligada ao objecto, de tal modo que não seja acessível a partir do lado de fora e a primeira parte do código objecto seja ligada com o objecto do lado de fora. Propõe-se ainda que a primeira parte do código objecto seja ligada sob uma protecção visual. Com isso, a segurança e a confiabilidade da identificação do objecto pode ser vantajosamente aumentada ainda mais.

Além disso, a presente invenção propõe um método para verificar a autenticidade de um objecto com um código de objecto, que tem, pelo menos, um identificador de objecto que é marcado por um dos métodos propostos para a identificação de objectos de acordo com a presente invenção. O método tem as seguintes etapas: a transferência do código objecto através de um meio de transmissão e recepção do código objecto transferido pelo dispositivo de verificação, em divisão do código objecto em, pelo menos, uma primeira parte do código do sistema e um identificador

de transmissão, cifrando do primeira parte do código do sistema por um primeiro método de codificação, comparando da primeira parte cifrada do código do sistema com as primeiras partes dos códigos do sistema que estão armazenados na primeira memória de dados e, se a primeira parte do código encriptado é sistema encontrado na primeira memória de dados, descodificar a segunda parte do código do sistema armazenadas na primeira memória de dados por segundo do método de codificação, a combinação da primeira e da segunda parte dos códigos do sistema em conjunto para formar um código de sistema, comparando o identificador de transmissão com identificadores de transmissão que são armazenados na segunda memória de dados e, se um identificador de tarefa correspondente for encontrado, o código de codificação de sistema por um terceiro método de codificação, comparando o código do sistema codificado com códigos encriptados sistema armazenados na terceira memória de dados e, se um código de sistema de correspondência codificado for encontrado, descodificação de um objecto identificador codificado atribuído por um quarto método de codificação e exibição de um identificador de objecto descodificado para comparar o identificador do objecto exibido com o identificador do objecto sobre o objecto. Por conseguinte, o método permite um controlo particularmente simples e de confiança da identificação.

Outro aspecto da aplicação do referido método propõe que o método, em que o código do sistema é armazenado na primeira memória de dados com uma informação de activação adicional, mostra se o código do sistema está activo ou não activo, e tem um passo em que a informação de activação é activado por um dos códigos de sistema. Este aspecto do método é particularmente útil para fechar a cadeia de abastecimento inseguro entre os produtores e consumidores.

De acordo com aspectos adicionais da invenção, o meio de transmissão é a Internet ou uma rede de telefone celular. Para além disso, dados específicos de recuperação, que são gerados durante a verificação do código de objecto, são armazenados numa quarta memória de dados. Propõe-se, para efeitos práticos, que, dependendo do meio de transmissão, os dados específicos de recuperação contenham, na entrada do código através da Internet, pelo menos, o tempo, o endereço IP, o prestador de serviços de Internet eo número de tentativas de entrada e, no momento da entrada do código via SMS, pelo menos, o tempo, o número de telefone celular e o número de selecção SMS. Isto é vantajoso, uma vez que o meio de transmissão proposto é difundido e é, portanto, acessível para quase todos os consumidores. Além disso, o armazenamento de dados específicos de recuperação é vantajoso a fim de verificar, por exemplo, quando, como e por meio do qual se verificou um código de objecto para o primeiro tempo.

A presente invenção propõe ainda um dispositivo para a rotulagem de um objecto com um código de objecto e um dispositivo para a verificação de um código de objecto de um objecto, através do qual os dispositivos têm instalações configuradas para executar os passos do método da presente invenção. Além disso, a presente invenção propõe um programa de computador que, quando executado num computador, faz com que ele execute o método de acordo com a presente invenção, bem como um suporte de dados no qual o programa de computador é armazenado.

Outro aspecto da presente invenção propõe um objecto que é identificado com um código de objecto, o qual foi produzido pelo método de acordo com a invenção.

Formas de execução preferidas da invenção são explicadas a seguir, puramente como um exemplo e sem qualquer restrição, com o auxílio dos desenhos anexos, em que:

A Fig. 1 é um fluxograma de uma forma de implementação do método de acordo com a invenção;

A Fig. 2 é um fluxograma pormenorizado para a geração do código de sistema de um exemplo de implementação da forma de execução conforme a Fig. 1;

A Fig. 3 mostra um fluxograma pormenorizado para a geração de chaves de codificação de acordo com um exemplo de implementação da forma de execução conforme a Fig. 1;

A Fig. 4 mostra um fluxograma pormenorizado para a geração do código de objecto de acordo com um exemplo de implementação da forma de execução conforme a Fig. 1;

A Fig. 5A mostra um objecto com uma primeira parte do código objecto anexado na parte externa sob uma protecção visual e uma segunda parte do código de objecto não é acessível a partir do exterior;

A Fig. 5B mostra o objecto de acordo com a Fig. 5A, no qual a protecção visual foi removida a partir da primeira parte do código de objecto e a segunda parte do código de objecto é acessível através da abertura do objecto;

A Fig. 5C mostra um fluxo esquemático de uma verificação do código de objecto do objecto, conforme a Fig. 5B por um consumidor, utilizando-se o método de acordo com a Fig. 1;

A Fig. 6 mostra uma representação esquemática de uma forma do dispositivo de etiquetagem de objectos de aplicação; e

A Fig. 7 mostra uma representação esquemática de uma forma de o dispositivo para a verificação de um código de objecto aplicação.

Um exemplo de implementação de um dispositivo para a marcação de um objecto é mostrado na Fig. 6. O dispositivo 600 compreende um Sistema de Geração de Código da Instalação 610, que cria um sistema de código aleatório exclusivo e transfere-a para uma Memória de Primeiros Dados de Instalação 620 para armazenamento em uma memória de dados 625; uma Instalação de geração de Chave de Codificação 630, que cria uma chave de codificação aleatória e transfere-a para um Segundo Mecanismo de Memória de Dados 640 para o armazenamento em uma memória de dados 645; uma Instalação de Geração de Código de Objecto 650, que cria um código de objecto e o transfere para um Terceiro Mecanismo de Memória de Dados 660 para armazenamento em uma memória de dados 665; e uma Instalação de Código de Objecto Anexo 670, que atribui o código de objecto criado pela Instalação de Geração de Código de Objecto 650 a um objecto. Além disso, o código do sistema criado pelo Sistema de Geração de Código de Instalação 610 e a chave de codificação criada pela Instalação de Geração de Chave de Codificação 630 são transferidos para o Instalação de Geração de Código de Objecto 650.

As Instalações de Memória de Dados 620, 640 e 660 e as memórias de dados de 625, 645 e 665 são executadas de preferência fisicamente separadas para melhorar a segurança; em um exemplo de implementação simplificada, as memórias de dados de 625, 645 e 665 estão integrados também

nas correspondentes Instalações de Memória de Dados 620, 640 e 660. Além disso, as memórias de dados 625, 645 e 665 são de preferência aplicadas como memórias de dados fisicamente separados, a fim de assegurar uma quantidade máxima de segurança. As memórias de dados 625, 645 e 665 são combinadas numa memória de dados de um exemplo de execução para a simplificação do dispositivo 600. É evidente para o especialista que as duas memórias de dados de cada um também podem ser combinadas em uma memória de dados e uma memória de dados separado adicional para a terceira memória de dados é considerada como parte da invenção.

No exemplo de implementação de um método de acordo com a Fig. 1, o código do sistema é criado no passo 105, as chaves de codificação no passo 110 e o código do objecto no passo 115. Os exemplos de implementação das Figuras. 2, 3 e 4 mostram, respectivamente, a geração de códigos individuais ou chaves em detalhe. Como simplificação, as memórias de dados 625, 645 e 665 são mostrados como uma memória de dados 120 na Fig. 1.

A geração do código do sistema é mostrada em detalhe na Fig. 2. Como um exemplo, a geração de um código de sistema com um comprimento de 128 caracteres é descrita aqui, em que o código do sistema é formado a partir de uma primeira parte do código do sistema 215, que contém os primeiros dez caracteres do código do sistema, e um segunda parte do código do sistema 245, que contém os outros 118 caracteres do código do sistema. É evidente para o perito que outros comprimentos arbitrários de caracteres, tal como 64, 256, 512 caracteres, podem ser utilizados de maneira adequada para o código do sistema e para as respectivas partes de código de sistema 215, 245. A primeira parte do código do

sistema 215 com um comprimento de dez caracteres é criado pelo Sistema de Geração de Código de Instalação 610 a partir de um primeiro conjunto de caracteres 200, utilizando o primeiro método aleatório 205. O primeiro conjunto de caracteres 200 contém, por exemplo, um número de caracteres, que são seleccionados a partir de um conjunto completo de caracteres, que está disponível para o método ou o dispositivo. Sob a forma de implementação descrita aqui, o conjunto de caracteres completa contém as letras maiúsculas de A a Z e os números de 0 a 9, mas sem caracteres especiais. O primeiro conjunto de caracteres 200 é reduzido neste exemplo de implementação por caracteres e números, tais como Z e 2, a fim de assegurar a ambiguidades da primeira parte do código do sistema 215. O primeiro método aleatório 205 é um estado arbitrário do método de arte, em que uma série de caracteres são seleccionados aleatoriamente, ou seja, não previsivelmente, a partir de um conjunto de caracteres predefinido. Como exemplo, o encadeamento "F37E4A1BD8" é gerado aqui como a primeira parte do código do sistema 215 pelo Sistema de Geração de Código de Instalação 610. Esta primeira parte do código do sistema é codificado 215 no passo 220, usando um estado do método de codificação de arte em uma primeira parte criptografada do código do sistema 225. Neste exemplo de implementação de preferência uma função de cardinal de codificação, como o Message Digest Algorithm 5 (em suma: MD5) ou o Secure Hash Algorithm (em suma: SHA) é usada como método de codificação.

Além disso, na etapa 240 a Sistema de Geração de Código de Instalação 610 cria uma segunda parte do código do sistema 245 de um segundo conjunto de caracteres 230 por meio de um segundo método aleatório 235. O segundo conjunto de caracteres 230 de preferência contém o conjunto de

caracteres completo descrito acima. O segundo método aleatório 235 é também um método aleatório arbitrário com as mesmas características, como já descrito acima, o segundo método aleatório 235 é de preferência idêntico, com o primeiro método aleatório 205. A segunda parte do código do sistema 245 criado desta maneira, com um comprimento de 118 caracteres é codificado pelo segundo método de codificação na etapa 250. Neste exemplo de implementação de um método de codificação simétrica, como, por exemplo, o Advanced Encryption Standard (em suma: AES) ou o Data Encryption Standard (em suma: DES), é preferencialmente utilizado, que usa a primeira parte do código do sistema 215 como chave para a codificação. O resultado da etapa 250 é uma segunda parte criptografada do código do sistema 255.

A primeira parte encriptada do código do sistema 225 e a segunda parte encriptada do código do sistema 255 em conjunto com uma primeira informação específica do objecto 260 são armazenados no passo 265 pela Instalação dos Primeiros Dados de Memória 620 na memória de dados 625, de tal maneira, que a primeira parte encriptada do código do sistema 225, a segunda parte encriptada do código do sistema 255 e a primeira informação específica do objecto 260 são atribuídos um ao outro. Neste exemplo de implementação, a primeira informação específica do objecto 260 inclui, de preferência um número de unidade de produção, que identifica uma série de objectos de uma produção, bem como a data actual.

A primeira parte do código do sistema 215 e a segunda parte do código do sistema 245 formam o código do sistema quando ambas as partes dos códigos do sistema são combinadas umas com as outras. De acordo com a forma de execução mostrada na Fig. 2, o código do sistema não é formado de tal modo

que esteja disponível para utilização em fases posteriores do método, em vez do código do sistema é formado de novo para o passo individual na qual ele é necessário, por combinação da primeira parte do código do sistema 215 com a segunda parte do código do sistema 245 neste único passo. A combinação é uma concatenação do primeiro e segundo elementos do código do sistema para um sistema de código de comprimento correspondente. É evidente para o perito que o código do sistema pode ser fornecido como tal por um passo adicional correspondente para uso em outros métodos.

Além disso, em um exemplo de implementação de uma informação de activação, não mostrados na Fig. 2, além disso é salvo pela Instalação de Memória de Dados 620 na memória de dados 120, que atribuiu a uma primeira parte criptografada do código do sistema 215 indica se este está bloqueado ou livre. A fim de ser capaz de verificar o código de objecto, esta informação de activação deve ser activado antes da verificação de um código de objecto de um passo de activação, o qual é descrito em mais detalhe abaixo.

Noutro passo 110, o método na Fig. 1 produz uma chave de codificação de 315 e um identificador de transmissão 330. A geração da chave de codificação 315 e o identificador de tarefa 330 é mostrado em pormenor na Fig. 3 de acordo com um exemplo de implementação. A chave de codificação 315 é criada no passo 310 pelo Mecanismo de Geração de Chave de Codificação 630, usando um terceiro método aleatório 305 de um terceiro conjunto de caracteres 300. O terceiro conjunto de caracteres 300 contém, por exemplo, o conjunto de caracteres completo descrito acima e, além disso, também todas as letras minúsculas e caracteres especiais. O terceiro método aleatório 305 é, para fins práticos

idênticos com o primeiro método aleatório 205 e o segundo método aleatório 235, pelo que também podem ser utilizados outros métodos conhecidos aleatórios. A codificação de chave 315 tem de preferência um comprimento de caracteres entre 200 e 500 caracteres e é variável, ou seja, as alterações de comprimento personagem em intervalos predeterminados. A codificação de chave tem um comprimento de 256 caracteres no exemplo de implementação preferido aqui.

Além disso, no passo 325 um identificador de tarefa 330 é criado por meio de um método de transmissão fixa 320. Um método preferido de transmissão 320 calcula, por exemplo, o número de dias entre a data de referência e o dia de codificação, e dá isso como o identificador de transmissão 330. Além disso, uma codificação do identificador de tarefa 330 é possível pelo método de transmissão 320. No exemplo implementação preferida aqui, o identificador de transmissão 330 é criptografada usando um método de codificação simples, em que cada carácter individual está codificado. Por exemplo, se há 121 dias entre a data de referência e o dia de codificação, o número de dias é primeiro dividido pelo método de transmissão 320 em duas partes, tal como 1 como a primeira parte 21 e numa segunda parte. Depois que a primeira e a segunda parte são convertidos por meio de uma fórmula de transformação, tais como 1 = A, 2 = B, C 3 =, ..., L = 21, ..., 26 = Z, 27 = A, ..., 52 = Z, 53 = A etc., para dar as letras "A" para a primeira parte e "U" para a segunda parte, em que concatenando a primeira e segunda parte da combinação de letras resultados de "au" como identificador de transmissão 330.

No passo 340, a chave de codificação 315 e o identificador de tarefa 330 em conjunto com uma segunda informação específica do objecto 335 são armazenados pela Segunda Instalação de Memória de Dados 640 na memória de dados 120. As segundas informações específicas do objecto 335 compreendem, de preferência o número da unidade de produção e a data actual.

A geração do código de objecto 405 é realizada no passo 115 na Fig. 1, que é mostrado em pormenor um exemplo de acordo com a aplicação na Fig. 4. Um código de objecto 405, que consiste em, pelo menos, a primeira parte do código do sistema 215 e o identificador de transmissão 330, é criado no passo 400, pela Instalação de Geração de Código de Objecto 650. A primeira parte do código do sistema 215 e o identificador de tarefa 330 são de preferência combinados em conjunto, através do qual, no exemplo descrito aqui o objecto de código 405 "F37E4A1BD8AU" com 12 caracteres resulta a partir da primeira parte do código do sistema 215 com dez caracteres e a transmissão identificador 330 com dois personagens, descritos acima.

Além disso, o código do sistema, que consiste na primeira parte do código do sistema 215 e a segunda parte do código do sistema 245, é codificado pela Instalação de Geração de Código de Objecto 650 no passo 410 por um terceiro método de codificação para dar um sistema de código encriptado 415. O terceiro método de codificação é um estado do método de codificação da arte, de preferência um método de codificação assimétrica, tal como o algoritmo RSA, o qual utiliza a chave 315 como chave de codificação. Na forma de realização aqui descrita, o método de codificação assimétrica não é utilizado como um método de chave pública clássico, mas como uma codificação unidireccional, uma vez

que o método utiliza a chave 315 como uma chave de cifração pública, sem fornecer outra chave como chave privada para descodificação.

Além disso, a Instalação de Geração de Código de Objecto 650 criptografa um identificador de objecto 420 no passo 425 por um quarto método de codificação. O quarto método de codificação é um método de codificação conhecido arbitrário; por exemplo, um método simétrico codificação, como o Advanced Encryption Standard (em suma: AES) ou o Data Encryption Standard (em suma: DES), é usado aqui, que usa o código do sistema que consiste na primeira parte do código do sistema 215 e a segunda parte do código do sistema 245, como chave. O identificador de objecto 420 contém neste exemplo de implementação de preferência o nome do produto, a unidade de produção e / ou a especificação do produto ou informações de o conteúdo exacto do produto, que tem de ser fornecido com o código de objecto. O resultado da etapa 425 é um objecto identificador codificado 430.

No passo 440, o código do sistema encriptado 415 a partir do passo 410 e o objecto identificador codificado 430 a partir do passo 425 são armazenados pela Terceira Instalação de Memória de Dados 660 na memória de dados 120.

No passo 125 mostrado na Fig. 1, o código objecto 405 está ligado ao objecto, para o qual o código objecto 405 foi criado, pelo Instalação de Fixação de Código de Objecto 670. O objecto foi assim fabricado pela produção com o número da unidade de produção correspondente e desde que com o identificador do objecto correspondente 420. O código de objecto 405 é ligado ao objecto de tal maneira que é, por exemplo, pode ser lido por um consumidor e, portanto, verificável posteriormente.

Em um outro exemplo de execução, o código de objecto é dividido numa primeira e numa segunda parte do código de objecto. A divisão, assim como os comprimentos de caracteres da primeira e da segunda parte do código de objecto pode ser seleccionado arbitrariamente. No exemplo de implementação aqui preferido, a primeira parte do código de objecto representa dois terços e a segunda parte do código de objecto de um terço do código de objecto 405. Ao dividir o código de objecto 405, como descrito no exemplo acima, a primeira parte do código objecto é "F37E4A1B" e a segunda parte do código de objecto é "D8AU".É evidente para o perito que outras divisões, como um quarto e três quartos para as respectivas partes do código de objecto, também são possíveis.

É, pois, evidente para o perito que a segurança do método é conseguido através da descodificação do identificador do objecto 420 a partir da memória de dados 645, e a transmissão de um código de objecto a outro identificador só é possível se o método de codificação usado, bem como as teclas usadas para isso sejam conhecidos, no entanto, existem apenas como dados encriptados nas memórias de dados 625 e 645. Informações sem codificação, que consistem na chave de codificação 315, a transmissão de um identificador 330 e os segundos dados específicos do objecto 335, está disponível apenas na memória de dados 635, que, no entanto por si só não é suficiente para descodificar as informações criptografadas na memória de dados de 625 ou 645 ou para a produção de uma transmissão de código de objecto a um objecto identificador. Portanto, mesmo com o conhecimento das informações de uma das memórias de dados de 625, 635 ou 645, não é possível restaurar todas as informações criptografadas, em particular o identificador do objecto e

a transmissão de código de um objecto a outro identificador.

Com referência à fig. 5A e a Fig. 5B, que vai agora ser descrito como o código de objecto 405 é ligado ao objecto 500. A primeira parte do código de objecto e a segunda parte do código de objecto, que de acordo com o exemplo de implementação descrito acima, foram criados pela divisão do código de objecto 405, estão ligados em um exemplo de implementação preferido em diferentes posições em relação ao objecto 500. A primeira parte do código de objecto 520 é, assim, ligado sem ser visível, acessível a partir do exterior, para o objecto 500 em si ou na embalagem do objecto, na Fig. 5A. A segunda parte do código de objecto 530 é ligado, não é acessível do exterior, sobre o objecto 500, por exemplo no interior da embalagem de objecto ou sobre o produto embalado. No exemplo de implementação mostrado na Fig. 5A a primeira parte do código de objecto 520 é ligado sob uma protecção visual 510, como por exemplo, um campo de zero, pelo que a protecção visual 510 deve ser destruída, a fim de ver a primeira parte do código de objecto 520. Além disso, de acordo com a Fig. 5B, a segunda parte do código de objecto 530 é acessível se, por exemplo, a embalagem do objecto for aberta.

Um dispositivo para a verificação de um código de objecto de um objecto é mostrado em um exemplo de implementação na Fig. 7. O dispositivo 700 contém uma Unidade de Recepção 720, que recebe o código de objecto do objecto, que é transmitido através de um meio de transmissão 710, e transfere-a para um Mecanismo de Verificação 740, pelo qual este código de objecto é verificado. O resultado da verificação é exibido por um Mecanismo de Exibição 790. O Mecanismo de Verificação 740 compreende um Instalação de

divisão de Código de Objecto 750, que divide o código de objecto e passa-o por uma Primeira Instalação de Comparação 760 e por uma Segunda Instalação de Comparação 770 para processamento posterior. A Primeira Instalação de Comparação 760 processa a parte transferida do código de objecto e compara o resultado deste tratamento com dados de uma memória de dados 765, em que a Primeira Instalação de Comparação 760, na busca de uma entrada na memória de dados de 765 correspondentes a uma parte processada do código de objecto, lê os dados da memória de dados 765, que é atribuído à entrada correspondente. A leitura dos dados é mantida disponível pela Primeira Instalação de Comparação 760 da Instalação de Verificação 740 para processamento posterior. A Segunda Instalação de Comparação 770 compara a outra parte transferida do código de objecto com dados em uma memória de dados 775 e, ao encontrar uma entrada correspondente na memória de dados 775, lê os dados atribuídos a esta entrada a partir da memória de dados 775. A leitura dos dados é ainda processada pela segunda Instalação de Comparação 770 e mantida à disposição na Instalação de Verificação 740. Uma Terceira Instalação de Comparação 780 leva sobre os dados, que são mantidos à disponibilidade da Instalação de Verificação 740, e processa estes dados, pelo que os dados processados são comparados com os dados que são armazenados em uma memória de dados 785. Ao encontrar uma entrada correspondente na memória de dados 785, a Terceira Instalação de Comparação 780 lê dados atribuídos a esta entrada e transfere-os para o Instalação de Exibição 790 como o resultado da verificação do código de objecto.

Num exemplo de implementação, a memória de dados / memórias 765, 775 e 785 é / são idênticas com a correspondente memória de dados / memórias 625, 645 e 665 na Fig. 6. Em

outro exemplo de implementação, em que as memórias de dados na Fig. 7 e as memórias de dados na Fig. 6 não são idênticos, pelo menos, os dados armazenados nas memórias de dados 765, 775, 785 da Fig. 7 são idênticos com os dados armazenados nas correspondentes memórias de dados 625, 645 e 665 na Fig. 6. Além disso, num exemplo de implementação, o dispositivo 700 inclui uma Instalação de Activação 730, que armazena informação de activação na memória de dados 765.

A seguir abaixo, a forma do método de implementação para a verificação de um código de objecto é descrito com referência à fig. 1. Na Fig. 1 as memórias de dados 765, 775 e 785 são mostradas como memórias de dados de 120 como uma simplificação. O código de objecto, o qual foi criado com o método descrito acima e que está ligado a um objecto, é transferido no passo 130 para o meio de transmissão 710 para a verificação. O meio de transmissão 710 transmite o código de objecto para a Unidade Receptora 720. A Unidade Receptora 720, em seguida, transfere o código de objecto recebido para a Instalação de Verificação 740. O meio de transmissão 710 é a Internet ou uma rede de telefonia celular. Tanto a Internet e a rede de telefonia celular são alternativas utilizáveis como um meio de transmissão de 710 em um exemplo de implementação particularmente preferido para a transferência do código de objecto para a Instalação de Verificação 740. Se o meio de transmissão 710 é a Internet, a unidade receptora 720 é de preferência uma página da web 560 e, se o meio de transmissão 710 é a rede de telefone celular, é uma mensagem 550, tais como o estado da técnica conhecida Short Message Service (SMS). O código de objecto recebido pela Unidade Receptora 720 é então transferido no passo 135 para a Instalação de Verificação 740 para verificação.

No passo 135 o código de objecto é dividido pela Instalação de Divisão de Código de Objecto 750 em pelo menos uma primeira parte do código de sistema e um identificador de transmissão. No exemplo aqui descrito, em que o código de objecto é constituído por 12 caracteres, em que os primeiros dez caracteres correspondem à primeira parte do código de sistema e

os dois últimos caracteres do identificador de transmissão, o código de objecto é dividido em uma primeira parte do código do sistema com dez caracteres e um identificador de transmissão com dois caracteres. Como descrito acima, a primeira parte do código de sistema é então encriptada na Primeira Instalação de Comparação 760 pelo método de codificação primeiramente seleccionado. Em seguida, esta primeira parte encriptada do código de sistema é comparada com as primeiras partes dos códigos de sistema encriptados, os quais são armazenados na memória de dados 120. Se uma primeira parte encriptada armazenada do código de sistema se encontra na memória de dados 120, que coincide com a primeira parte encriptada do código de sistema do código de objecto a ser verificado, a Primeira Instalação de Comparação 760 lê os dados designados armazenados na memória de dados 120. No exemplo de implementação aqui preferido, esses dados armazenados compreendem uma segunda parte encriptada do código de sistema e uma primeira informação específica do objecto. A segunda parte encriptada do código de sistema é descodificada para uma segunda parte do código de sistema pela Primeira Instalação de Comparação 760 usando o segundo método de codificação, o qual é idêntico ao método de codificação simétrica seleccionado acima, e com a primeira parte do sistema como código de chave. Num exemplo de implementação, a primeira

parte do código de sistema e a segunda parte do código decodificado do sistema são então aglutinados dando origem a um código de sistema. A primeira e segunda parte do código de sistema, a primeira informação específica do objecto e, na medida do computado, os códigos de sistema são mantidos à disposição da Instalação de Verificação 740 para posterior utilização em outras instalações da Instalação de Verificação 740. Além disso, num exemplo de implementação, os dados de leitura e / ou a mensagem indicadora de que uma correspondência foi encontrada na memória de dados 120 é transferidos para a Instalação de Exibição 790 para exibição. Se a Primeira Instalação de Comparação 760 não encontrar uma correspondência encriptada primeira parte do código de sistema na memória de dados 120, em seguida, uma mensagem de erro 145 é transferido para a Instalação de Exibição 790, o que indica que nenhuma correspondência terá sido encontrada. Neste caso, o método é finalizado e da Instalação de Exibição 790 exibe a mensagem de erro 145.

Se a Primeira Instalação de Comparação 760 encontrar uma correspondência encriptada primeira parte do código do sistema na memória de dados 120, o método prossegue com a transferência do identificador de transmissão, obtido pela divisão do objecto Divisão de Código de Acesso 750, para a Segunda Instalação de Comparação 770. A Segunda Instalação de Comparação 770 compara o identificador atribuído com a transferência de identificadores de transmissão armazenados na memória de dados 120. Se um identificador de transmissão correspondente for encontrado na memória de dados de 120, a Segunda Instalação de Comparação 770 lê os dados atribuídos a este identificador de transmissão, como por exemplo, uma chave de codificação e uma segunda informação específica do objecto, que é mantida à disposição para posterior

processamento em Instalação de Verificação 740. Os dados de leitura e / ou uma mensagem adequada, que diz que foram encontrados dados na memória de dados 120 e está disponível para processamento adicional na Instalação de Verificação 740, é / são transferidas para a Instalação de Exibição 790 para exibição. Se nenhum identificador de transmissão de harmonização puder ser encontrado na memória de dados 120, uma mensagem de erro apropriada 145 é enviado para a Instalação de Exibição 790, o que indica que o identificador de transmissão não foi encontrado na memória de dados 120 pela Segunda Instalação de Comparação 770. Neste caso, o método é finalizado e a Instalação de Exibição 790 exibe a mensagem de erro 145.

Se o mecanismo de segunda comparação 770 encontrou uma correspondência na memória de dados de 120, o método continua com a Terceira Instalação de comparação 780. A Terceira Instalação de Comparação 780, utilizando o terceiro método de codificação, encripta o código de sistema que é mantido à disponibilidade na Instalação de Verificação 740, a qual é formada a partir da primeira e da segunda parte do código de sistema, com a chave de codificação. O terceiro método de codificação é idêntico ao terceiro método de codificação acima descrito. O código de sistema, assim encriptado é comparado com os códigos de sistema encriptados na memória de dados 120. Se um código de sistema de correspondência encriptada é encontrado na memória de dados de 120, então os dados atribuídos a este código sistema encriptado, aqui, por exemplo, um objecto identificador encriptado aqui, é lido pela Terceira Instalação de Comparação 780. O identificador de objecto encriptado é descodificado usando o quarto método de codificação acima descrito pela Terceira Instalação de Comparação 780 com o código de sistema acessível nas

Instalações de Verificação 740 como chave. O identificador de objecto descodificado e / ou uma mensagem adequada que um sistema de código encriptado combinado foi encontrado na memória de dados 120 é / são transferido(os) para a Instalação de Exibição 790 a ser exibidos pela Instalação de Exibição 790. Se nenhuma correspondência for encontrada na memória de dados 120, uma mensagem de erro é enviada 145 para a Instalação de Exibição 790, o que indica que o código do sistema não foi encontrado na memória de dados 120. Neste caso, o método é finalizado e a Instalação de Exibição 790 exibe a mensagem de erro 145.

A Instalação de Visualização de 790 exibe os dados e / ou mensagens recebidas a partir do primeiro, segundo e terceiro instalações de comparação. Por exemplo, em um exemplo de implementação preferido a mensagem de erro 145 é exibida, que diz que o código de objecto transferido não existe, o que implica que não havia uma entrada errada do código de objecto ou uma falsificação do objecto. Se o código de objecto for encontrado, ou seja, o primeiro código de sistema for encontrado na memória de dados 120, o identificador de transmissão será encontrado na memória de dados 120 e os dados correspondentes também serão encontrados na memória de dados 120, em seguida, o identificador de objecto descodificado 180 será apresentado pela Instalação de Exibição 790.

A seguir abaixo, a verificação de um código de objecto por um consumidor, utilizando o método descrito acima é descrita com a fig. 5A, 5B e 5C. O consumidor adquire, por exemplo a partir de um comerciante, um objecto 500, que tem um código de objecto criado usando o método para a identificação de um objecto de acordo com a presente invenção. A primeira parte do código objecto 520 "F37E4A1B"

torna-se visível, destruindo a protecção visual 510. A segunda parte do código objecto 530 "D8AU" torna-se visível ao abrir a embalagem do objecto 500. O consumidor agora une as duas partes dos códigos de objecto uma à outra para obter o código de objecto "F37E4A1BD8AU". Este código de objecto é transmitido pelo consumidor para a Instalação de Verificação 740 p meio de transmissão 710. Na Fig. 5C uma página web 540 é mostrada, a qual funciona como uma Unidade de Recepção 720, se o meio de transmissão 710 é a Internet. Há um campo de entrada de 541 na página web 540, em que o consumidor faz a inserção do código de objecto. A transferência do código de objecto inserido, para a Instalação de Verificação 740 é realizada através do funcionamento do interruptor de função 542 fornecido na página web 540. Como descrito acima, a Instalação de Verificação 740 agora verifica o código de objecto transmitido no passo 135. O resultado da etapa 135 é transferido para a Instalação de Exibição 790. Se o meio de transmissão 710 é a Internet, a Instalação de Exibição 790 exibe o resultado de preferência como uma página web 560, em que o identificador de objecto 561 para o código de objecto verificado é exibido. Além disso, a Instalação de Exibição 790 também pode exibir o código de objecto inserido, por exemplo, para fins de controlo. Se o passo 135 não for executado com sucesso, então a Instalação de Visualização de 790 exibe a mensagem de erro 145 na página web 560, que diz que o código de objecto não foi encontrado. O consumidor agora compara em uma etapa de 580 se o identificador de objecto transmitido 561 corresponde ao identificador de objecto no objecto 500. Se estes dois identificadores de objectos são os mesmos, então o objecto é autêntico de acordo com o método. De acordo com um outro exemplo de implementação que é agora descrito em referência à Fig. 5C, o consumidor introduz o código de objecto do

objecto 500 em uma mensagem de SMS 550, se a rede de telefone celular é utilizada como um meio de transmissão 710. A mensagem SMS 550 contém o número 551 da Instalação de Verificação, bem como o código de objecto a ser {2 visto como texto da mensagem 552. A mensagem SMS 550 é transmitida para a Instalação de Verificação 740 quando o consumidor prime o botão "enviar" 553 no seu dispositivo, como um telefone móvel que utiliza a rede de telefonia celular. A Instalação de Verificação 740 verifica o código de objecto, executando o passo 135. O resultado da verificação é enviado em formato de uma resposta de SMS 570 para o dispositivo do consumidor através da rede de telefone celular. No caso de uma verificação bem sucedida a resposta SMS contém como texto de resposta 572, por exemplo, o código de objecto para fins de controlo e o identificador de objecto. No caso de uma verificação com resultado negativo o texto de resposta 572 contém a mensagem 145. O consumidor agora compara num passo 580 o identificador de objecto transmitido no texto de resposta 572 com o identificador de objecto no objecto 500. Se estes dois identificadores de objecto são os mesmos, o objecto é autêntico de acordo com o método. De acordo com um exemplo de realização preferida, como mostrado na Fig. 5C, a Instalação de Exibição 790 exhibe o identificador de objecto como uma página web 580, se o meio de transmissão é a Internet e, se o meio de transmissão é uma rede de telefonia celular, como uma mensagem de resposta 570. O identificador de objecto pode ser exibido agora, em comparação com o identificador de objecto preso no objecto, a fim de determinar a autenticidade do objecto. O objecto é autenticado se o identificador do objecto exibido e o identificador do objecto anexado são idênticos.

Em um exemplo preferencial de implementação do método de acordo com a Fig. 1, o código de sistema é proporcionado com informação de activação na memória de dados 120, que indica se o código objecto é activado ou não. Após a verificação do código de objecto no passo 135 é adicionalmente verificado na etapa 160 se o código de objecto verificado também é libertado para verificação. A consulta de um código de objecto desactivado leva a uma mensagem correspondente 165 na Instalação de Exibição 790. Se for encontrado na verificação no passo 160 que o código de objecto é liberado para a verificação, então este é transferido para a Instalação de Exibição 790 para exibição 150.

O código de objecto é, de preferência definido como "desactivado" por defeito durante a geração da primeira parte do código do sistema no passo 110, e assim também o código de sistema, bem como o código de objecto. O código de sistema é activado por uma etapa 155, o qual tem de ser executado no passo 135 antes de uma verificação. O código de objecto é activado, digitando a primeira parte do código de sistema na Instalação de Activação 730 somente se uma primeira parte que combina com o código de sistema, o que ainda não está activada, é encontrada na memória de dados 765. Se a primeira parte compatível não activada do código do sistema é encontrada, em seguida, as informações de activação para a primeira parte do código de sistema são activadas e o código de objecto é assim libertado para verificação. Além disso, uma mensagem adequada, indicando que o código de objecto foi activado, é enviada para a Instalação de Exibição 790. Caso contrário, uma mensagem correspondente é apresentada pela Instalação de Exibição 790, o que indica que a primeira parte do código introduzido sistema não está disponível na memória de dados

765 ou que, embora a primeira parte inserida do código de sistema foi encontrada na memória de dados 765, que já se encontra activada.

Em outros exemplos de implementação do processo de acordo com a Fig. 1, dados específicos de consulta são armazenados na memória de dados do outro que não é mostrado. Estes dados específicos de consulta compreendem, no caso de transmissão do código de objecto através da Internet, de preferência o momento em que o código de objecto foi transmitido, o endereço IP que dá a origem da transmissão, o prestador de serviços de Internet e do número de tentativas de entrada. Se a rede de telefonia celular é usada como um dispositivo de transmissão de 710, os dados específicos de consulta compreendem, de preferência a hora, o número de telefone celular da pessoa a consultar e o número para envio de mensagens SMS. O número de envio de mensagens SMS é, por exemplo, o chamado SMS número de marcação abreviado. No entanto, o número de marcação SMS também pode ser um correspondente SMS número de longa marcação no caso de algumas redes de telefonia celular. Outros formatos de número de marcação SMS são possíveis, dependendo da rede de telefonia celular. É evidente para o perito que outros dados específicos de consulta podem ser armazenados e que a memória de dados adicional mencionada também é idêntica com as memórias de dados descritas acima.

Outros exemplos de Implementação preferidos da presente invenção incluem, durante a verificação de um código de objecto transferido, uma consulta de dados específicos de consulta, a fim de determinar se o código de objecto já foi interrogado ou não. Nestes exemplos de implementação, um identificador de consulta e uma palavra-chave de consulta são gerados além disso durante a primeira consulta do

código de objecto, e armazenados como dados específicos de consulta em uma memória de dados de consulta que não é mostrada. O identificador de consulta e a palavra-chave de consulta são mostrados, por exemplo, através da Instalação de Exibição 790 para o consumidor, que verifica um certo código de objecto pela primeira vez, ou seja, o código de objecto não tinha sido consultado nem verificado ainda. Em outras tentativas de consulta deste código de objecto, que foi já foi consultado uma vez, o identificador de consulta e a palavra-chave de consulta são transmitidos em adição pelo consumidor, a fim de assegurar que só o consumidor que tenha consultado o código de objecto pela primeira vez pode realizar consultas mais bem sucedidas para este código de objecto. Outros consumidores, que não têm o identificador de consulta correspondente e a palavra-chave de consulta para este código de objecto ira acontecer que ou não podem consultar o código de objecto com sucesso ou recebem uma mensagem a dizer que o código de objecto já foi verificado pela primeira vez.

O método de acordo com a invenção é executado de preferência em modo de programa de computador sendo executado em um computador e controlar o computador. O computador inclui várias instalações de processamento de dados, incluindo PCs de usuários simples, estruturas cliente-servidor ou outros sistemas de computadores em rede, na medida em que eles são criados em conformidade e são adequados para a aplicação dos métodos, aparelhos e sistemas aqui descritos.

REIVINDICAÇÕES

1. Um método para a identificação de um objecto, que compreende pelo menos um identificador de objecto, com um código de objecto que é utilizado para verificar a autenticidade do objecto, que compreende os passos de:

a) geração de um código de sistema único aleatório, que consiste de uma primeira e uma segunda parte do código do sistema, em que a primeira parte do código do sistema é criada a partir de um primeiro conjunto de caracteres por um primeiro método aleatório e a segunda parte de o código do sistema a partir de um segundo conjunto de caracteres por um segundo método aleatório, e armazenando o código do sistema em conjunto com pelo menos uma primeira informação específica do objecto numa primeira memória de dados, em que a primeira parte do código do sistema é criptografada por um primeiro método de codificação e a segunda parte do código do sistema por um segundo método de codificação, o qual utiliza a primeira parte do código do sistema como a chave, antes de as armazenar;

b) geração de uma chave de codificação aleatória a partir de um terceiro conjunto de caracteres por um terceiro método aleatório; um identificador de transmissão única por um método de transmissão e o armazenamento da chave de codificação, do identificador de transmissão e, pelo menos, uma segunda informação específica do objecto numa segunda memória de dados;

c) geração de um código de objecto, que é constituído por, pelo menos, a primeira parte do código do sistema e o identificador de transmissão; codificação do código de sistema por um terceiro método de codificação, o qual utiliza a chave de codificação como chave; codificação do identificador do objecto por um quarto método de codificação que utiliza o código do sistema como chave; e armazenar o

código do sistema de codificação juntamente com o identificador de objecto codificado em uma terceira memória de dados;

d) fixar o código de objecto ao objecto;

em que o método proporciona uma quarta memória de dados, em que os dados específicos de consulta criados durante a verificação da autenticidade do objecto são armazenados.

2. O método de acordo com a reivindicação 1, em que, para além do sistema de código armazenado no passo a) uma informação de activação, que indica se o código do sistema está activa ou não activa, é armazenado na primeira memória de dados, em que o código do sistema é verificável apenas após a activação.

3. O método de acordo com a reivindicação 1, em que o código de objecto é dividido numa primeira e numa segunda parte do código de objecto.

4. O método de acordo com a reivindicação 3, em que a segunda parte do código de objecto é ligada ao objecto, de tal modo que não é acessível do exterior, e a primeira parte do código de objecto é ligada com o objecto no lado de fora.

5. O método de acordo com a reivindicação 4, em que a primeira parte do código de objecto é ligado sob uma protecção visual.

6. Um método para a verificação da autenticidade de um objecto com um código de objecto que compreende pelo menos um identificador, em que o código de objecto é criado de acordo com uma das reivindicações anteriores, contendo os passos:

e) de transmissão do código de objecto através de um meio de transmissão, recebendo o código de objecto transmitido por

uma Instalação de Verificação e armazenando os dados específicos de consulta, que são gerados durante a verificação da autenticidade do código de objecto, em uma quarta memória de dados;

f) dividindo o código de objecto em, pelo menos, uma primeira parte do código do sistema e um identificador de transmissão;

g) codificação da primeira parte do código do sistema com um primeiro método de codificação; comparação da primeira parte codificada do código do sistema com as primeiras partes dos códigos de sistema armazenadas na primeira memória de dados e, se a primeira parte cifrada do código do sistema se encontra na primeira memória de dados, a descodificação de uma segunda parte do código do sistema armazenado na primeira memória de dados por um segundo método de codificação, o qual usa a primeira parte do código de sistema como chave; concatenação do primeiro e segundo elementos do código de sistema para formar um código de sistema;

h) comparando o identificador de transmissão com os identificadores com os quais são armazenados na segunda memória de dados e, se um identificador de tarefa correspondente for encontrado, encriptar o código do sistema por um terceiro método de codificação, que utiliza uma chave de cifra, que é armazenado em conjunto com o identificador de transmissão na segunda memória de dados, como a chave;

i) comparação do código do sistema codificado com códigos encriptados do sistema que estão armazenados na terceira memória de dados e, se o código de sistema de correspondência encriptado for encontrado, a descodificação de um identificador de objecto encriptado atribuído por um quarto método de codificação, que utiliza o sistema como o código chave; e

j) apresentação de um identificador de objecto descodificado para comparar o identificador do objecto apresentado com o identificador de objecto sobre o objecto.

7. O método de acordo com a reivindicação 6, em que o código do sistema é armazenado na primeira memória de dados com informação de activação adicional, que mostra se o código do sistema está activo ou não activo, pelo que o método tem um passo adicional que é executado antes do passo e), em que a informação de activação é activada por um dos códigos de sistema.

8. O método de acordo com a reivindicação 6, em que o meio de transmissão é a Internet ou uma rede de telefone móvel.

9. O método de acordo com a reivindicação 6, em que os dados específicos de consulta, ao entrar o código através da Internet, compreendem, pelo menos, o tempo, o endereço IP, o fornecedor de serviços da Internet e o número de tentativas de entrada.

10. O método de acordo com a reivindicação 6, em que os dados específicos de consulta, ao entrar no código via SMS, compreendem, pelo menos, o tempo, o número de telefone móvel e o número de marcação de SMS.

11. Um dispositivo para a identificação de um objecto com um código de objecto, que compreende pelo menos um identificador de objecto, que é utilizado para a verificação da autenticidade do objecto, que compreende:

uma Instalação de Criação de um Código de Sistema, que é configurado para criar um código de sistema único aleatório, que consiste de uma primeira e de uma segunda parte do código do sistema, em que a primeira parte do código do sistema é criada a partir de um primeiro conjunto de caracteres por um primeiro método aleatório e a segunda parte do código do

sistema é criado a partir de um segundo conjunto de caracteres por um segundo método aleatório;

uma Primeira Instalação de Memória de Dados, que é configurada para armazenar o código do sistema criado pela Instalação de Criação de Código de Sistema juntamente com pelo menos uma primeira informação específica do objecto, em que, antes de guardar, a primeira parte do código do sistema é criptografada por um primeiro método de codificação e a segunda parte do código do sistema é criptografada por um segundo método de codificação, o qual utiliza a primeira parte do código do sistema de chave;

uma Instalação de Criação de Chave de Codificação, que é configurada para criar uma chave de codificação aleatória de um terceiro conjunto de caracteres por um terceiro método aleatório e um identificador de transmissão único por um método de transmissão;

uma Instalação de Segundos Dados de Memória, que é configurada para armazenar a chave de codificação criada, o identificador de transmissão e, pelo menos, uma segunda informação específica do objecto;

uma Instalação de Criação de Código de Objecto, que é configurada para criar um código de objecto, que é constituído por, pelo menos, a primeira parte do código do sistema e o identificador de transmissão;

uma Terceira Instalação de Memória de Dados, a qual é configurada para armazenar o código do sistema codificado por um terceiro método de codificação, o qual utiliza a chave de codificação como chave, juntamente com o identificador de objecto, que é codificado por um quarto método de codificação que utiliza o código de sistema como chave ;

uma Instalação de Fixação de Código de Objecto, que é configurada para anexar o código de objecto ao objecto; e

uma quarta Instalação de Memória de Dados, a qual é configurada para armazenar dados específicos de consulta, que

são gerados durante a verificação da autenticidade do objecto.

12. O dispositivo de acordo com a reivindicação 11, que compreende ainda: uma Instalação de Divisão, a qual está configurada para dividir o código de objecto em uma primeira e uma segunda parte do código de objecto.

13. Um dispositivo para a verificação da autenticidade de um objecto com um código de objecto que compreende pelo menos um identificador de objecto, em que o código de objecto foi criado por um dispositivo de acordo com a reivindicação 11, que compreende:

uma Unidade Receptora, a qual está configurada para receber o código de objecto, que é transferido através de, pelo menos, um meio de transmissão;

uma Instalação de Verificação, que é configurada para descodificar o código de objecto entrado na instalação de entrada e activar a descodificação do código de objecto inserido, compreendendo:

uma Instalação de Divisão de Código de Objecto, que é configurada para dividir o código de objecto inserido em pelo menos uma primeira parte do código do sistema e um identificador de transmissão;

uma Primeira Instalação de Comparação, a qual está configurada para encriptar a primeira parte do código do sistema por um primeiro método de codificação e para comparar a primeira parte encriptada do código do sistema com as primeiras partes dos códigos de sistema armazenadas na Primeira Instalação de Memória de Dados, e, se a primeira parte cifrada do código do sistema se encontra-se na Primeira Instalação de Memória de Dados, para descodificar uma segunda parte do código do sistema armazenada na Primeira Instalação de Memória de Dados por um segundo método de codificação, o

qual utiliza a primeira parte do código do sistema como chave, e para combinar as primeira e a segunda partes do código do sistema em conjunto para formar um sistema de código;

uma Segunda Instalação de Comparação, que é configurada para comparar o identificador de transmissão com os identificadores de transmissão que são armazenados na Segunda Instalação de Memória de Dados e, se um identificador de tarefa correspondente for encontrado, para encriptar o código do sistema por um terceiro método de codificação, o qual utiliza uma chave de codificação armazenada junto com o identificador de transmissão na segunda memória de dados como chave;

uma Terceira Instalação de Comparação, que é configurado para comparar o código do sistema codificado com códigos codificados do sistema armazenados na Terceira Instalação de Memória de Dados e, se um código de sistema de correspondência codificado for encontrado, para decodificar, um identificador de objecto codificado atribuído por um quarto método de codificação que usa a primeira parte do código do sistema como chave; uma Instalação de Visualização que exhibe o identificador do objecto descodificado pela Instalação de Verificação; e

uma quarta Instalação de Memória de Dados, que é configurada para armazenar dados específicos de consulta de que são gerados durante a verificação da autenticidade do código de objecto.

14. Um dispositivo de acordo com a reivindicação 13, que compreende ainda uma Instalação de Activação, que é configurada para activar um código de sistema armazenado na Primeira Instalação de Memória de Dados como não activo.

15. Um dispositivo de acordo com a reivindicação 13, em que o meio de transmissão é a Internet ou uma rede de telefone móvel.

16. Um dispositivo de acordo com a reivindicação 15, em que, ao entrar o código de objecto através da Internet, a quarta Instalação de Memória de Dados armazena pelo menos o tempo, o endereço IP, o prestador de serviços de Internet e o número de tentativas de entrada.

17. Um dispositivo de acordo com a reivindicação 15, em que, ao entrar no código de objecto via SMS, quarta Instalação de Memória de Dados armazena, pelo menos, o tempo, o número de telefone móvel e um número de marcação de SMS.

18. Um objecto que é identificado com um código de objecto que foi criado utilizando o método de acordo com a reivindicação 1.

19. Um programa de computador que, quando executado num computador, executa o método de acordo com a reivindicação 1.

20. Um suporte de dados no qual um programa de computador de acordo com a reivindicação 19 é armazenado numa forma legível por máquina.

RESUMO

MÉTODO E DISPOSITIVO PARA IDENTIFICAR OBJECTOS

A invenção refere-se a um método para a identificação de um objecto que compreende pelo menos um identificador de objecto com um código de objecto que é utilizado para verificar a autenticidade do objecto. O método compreende os seguintes passos: a criação de um sistema de código único aleatório constituído por um primeiro e um segundo código do sistema, a primeira parte do código do sistema a ser gerado a partir de um primeiro conjunto de caracteres por um primeiro método aleatório e a segunda parte do sistema código a ser gerado a partir de um segundo conjunto de caracteres por um segundo método de poupança aleatório e o código do sistema em conjunto com pelo menos uma primeira informação específica do objecto numa primeira memória de dados, a primeira parte do código do sistema que está sendo criptografada por um primeiro método de codificação e a segunda parte do código do sistema por um segundo método de codificação antes de ser salvo, a criação de uma chave de encriptação aleatória de um terceiro conjunto de caracteres por um terceiro método aleatório, a criação de um identificador de atribuição única por um método de atribuição e de poupança da chave de criptografia, identificador de atribuição e pelo menos um segundo pedaço específico do objecto de informações em um segundo memória de dados a criação do código objecto, que consiste na primeira parte do código do sistema e a chave de atribuição, a criptografia do identificador do objecto por um quarto método de criptografia e salvar o código do sistema criptografado junto com o identificador do objecto codificado em uma terceira memória de dados e a fixação do código objecto para o objecto..

Fig. 1

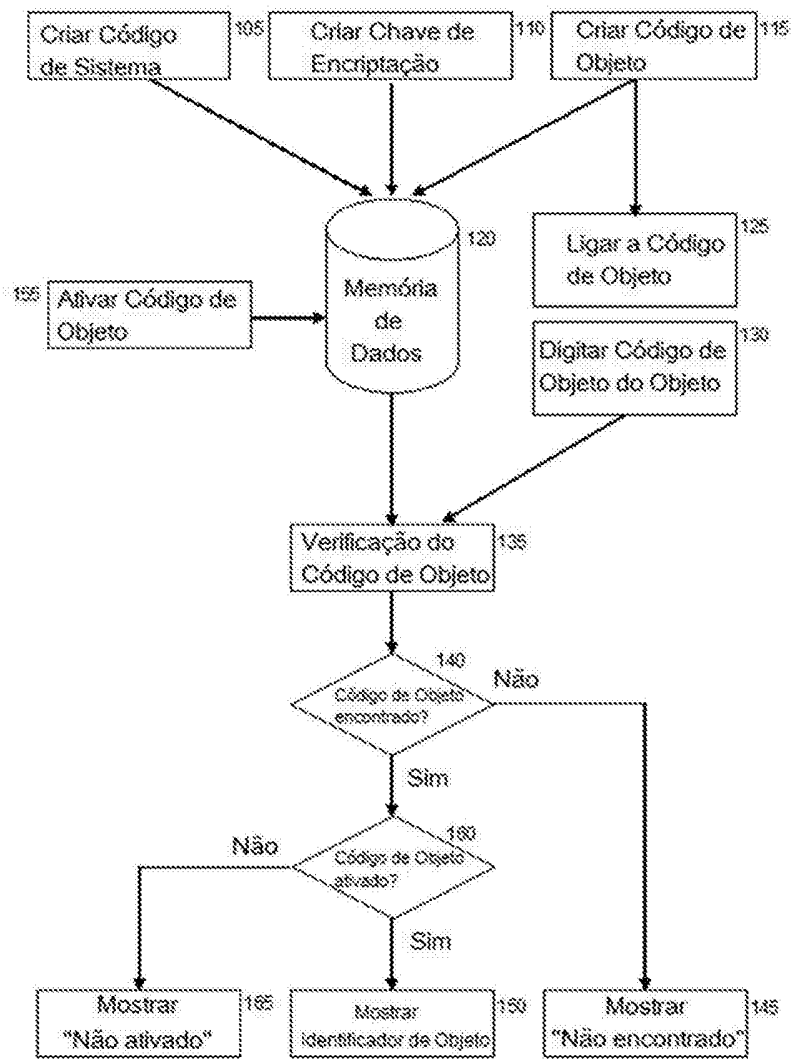


Fig. 2

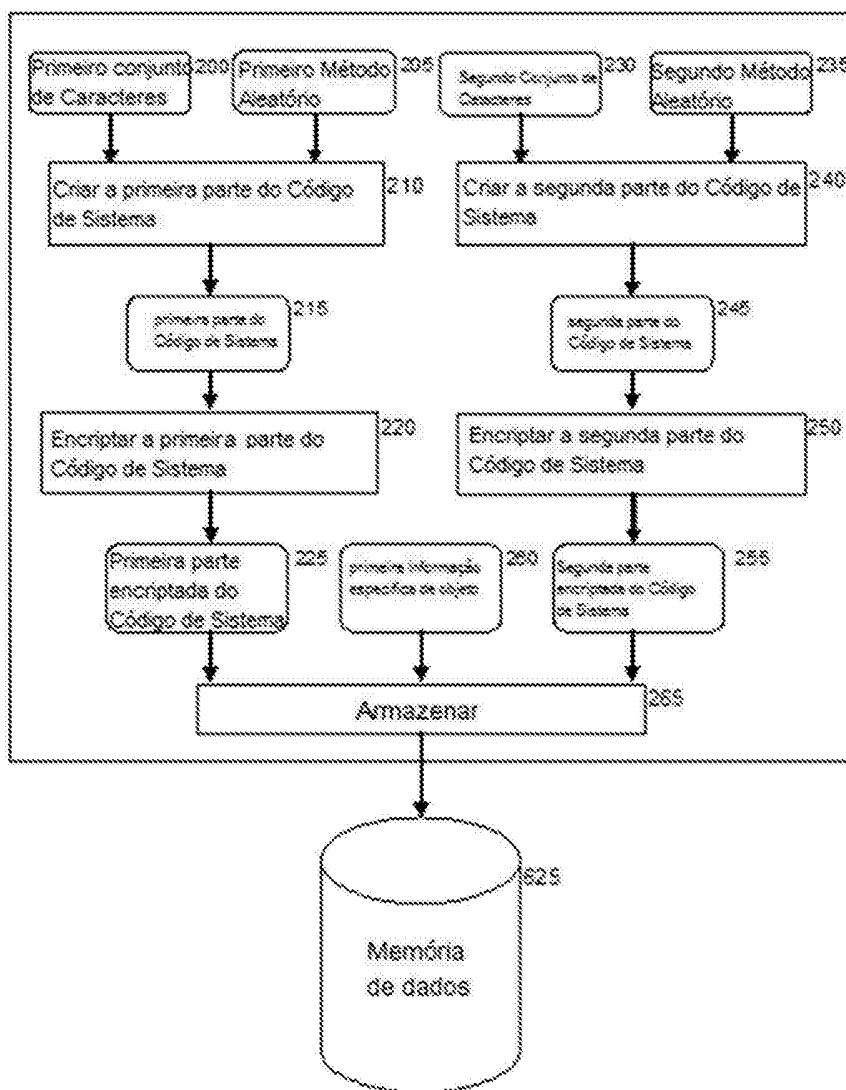


Fig. 3

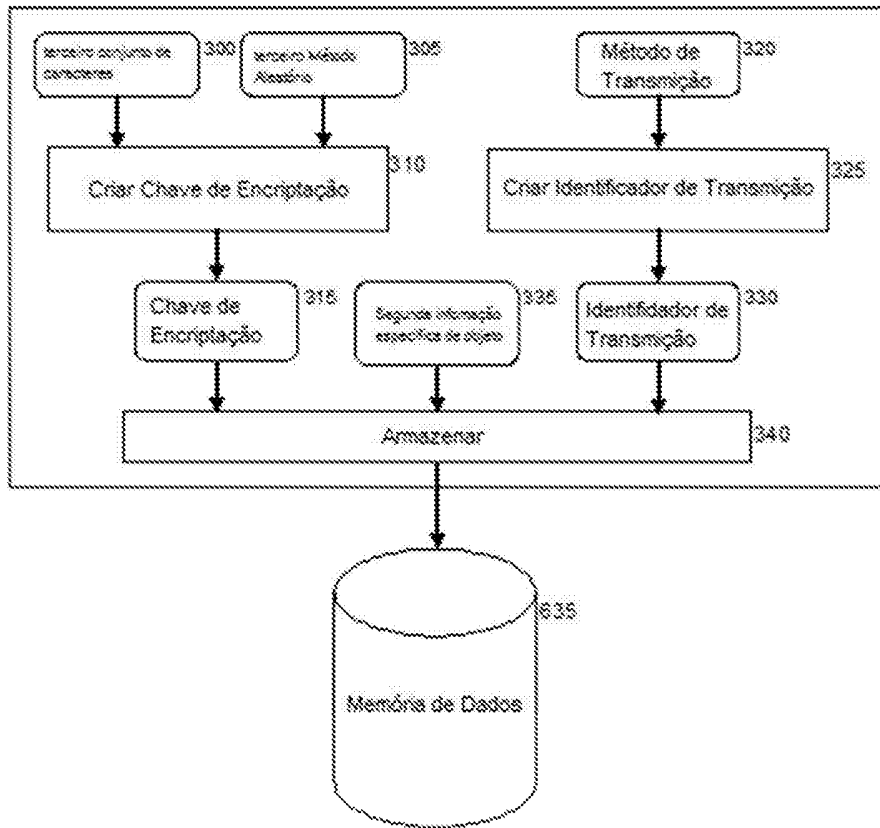


Fig. 4

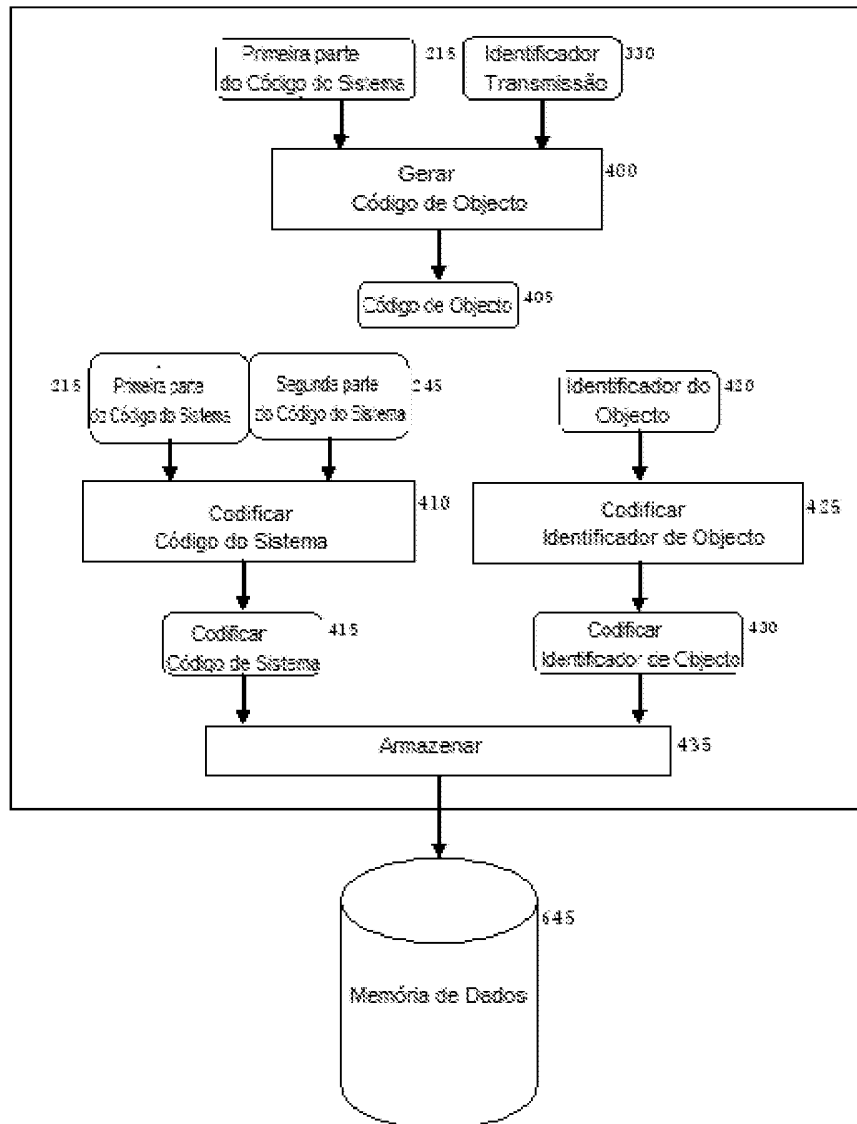


Fig. 5A

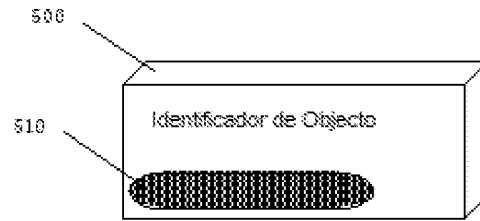
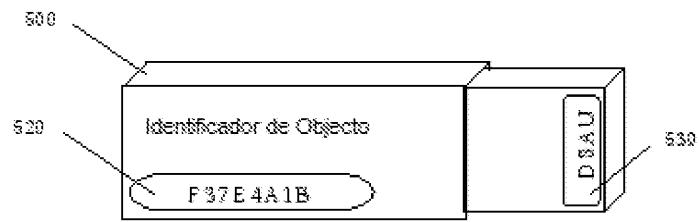


Fig. 5B



Código de Objeto = F 37 E 4 A 1 B D 8 A U

Fig. 5C

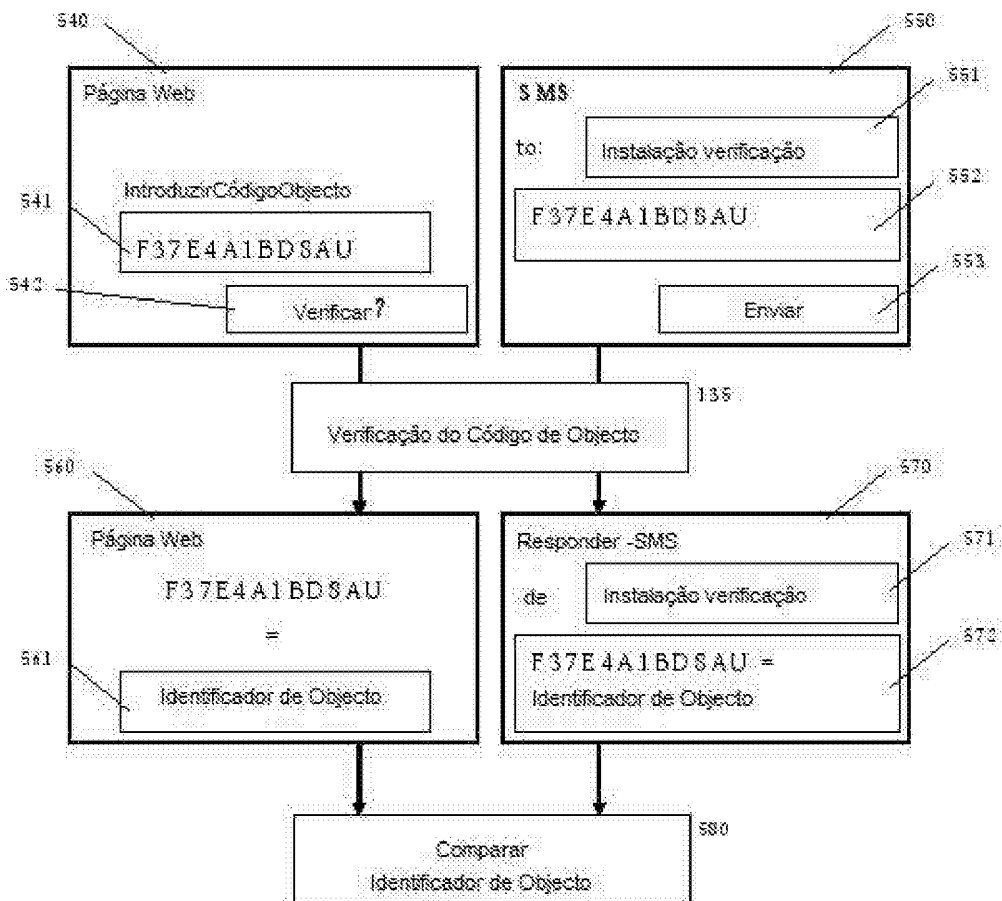


Fig. 6

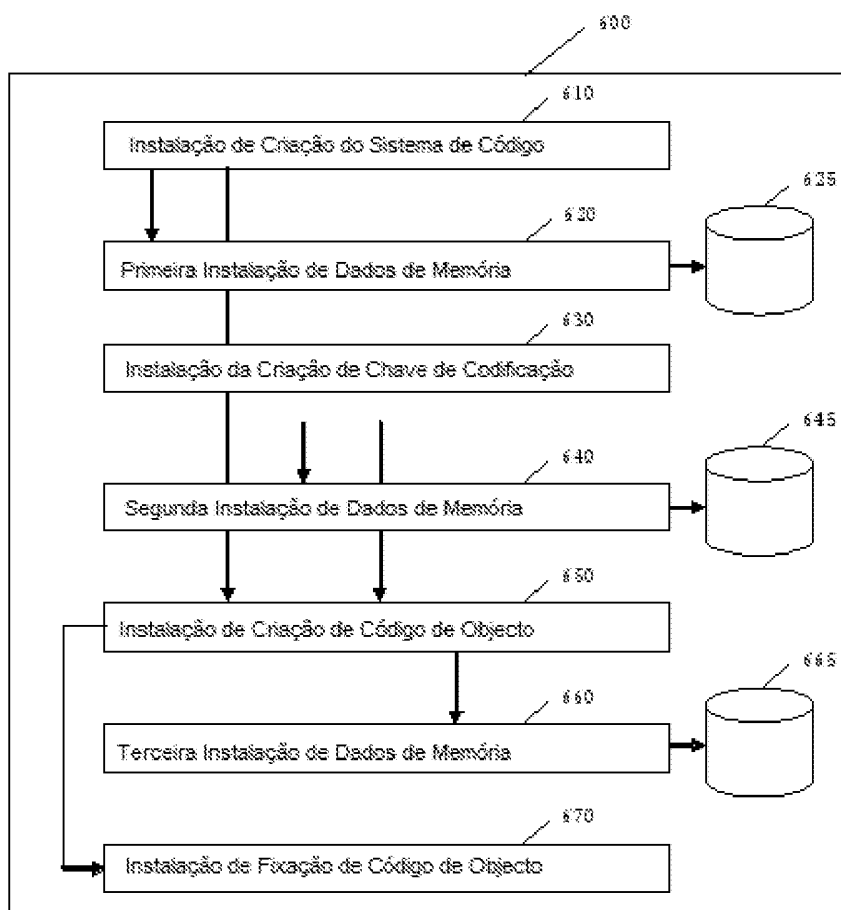


Fig. 7

