REPÚBLICA FEDERATIVA DO BRASIL

Ministério do Desenvolvimento, Indústria e Comércio Exterior
Instituto Nacional da Propriedade Industrial

CARTA PATENTE N.º PI 9805995-5

Patente de Invenção

O INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL concede a presente PATENTE, que outorga ao seu titular a propriedade da invenção caracterizada neste título, em todo o território nacional, garantindo os direitos dela decorrentes, previstos na legislação em vigor.

(21) Número do Depósito : PI 9805995-5

(22) Data do Depósito : 12/06/1998

(43) Data da Publicação do Pedido : 17/12/1998

(51) Classificação Internacional : G07B 17/00

(30) Prioridade Unionista : 12/06/1997 US 60/049518

(54) Título : Sistema de ministração de franqueamento postal seguro e processo para evidenciar pagamento de franquia postal.

(73) Titular : Pitney Bowes INC.. Endereço: One Elmcroft Road, Stamford, Connecticut 06926, Estados Unidos (US).

(72) Inventor : ROBERT A. CORDERY. Endereço: 11 1/2 Jeanette Street, Danbury-Connecticut, Estados Unidos, CEP: 06811. Cidadania: Norte Americana.; FRANK M. D´IPPOLITO. Endereço: 47 Commodore Commons, Derby, Connecticut 06418, Estados Unidos. Cidadania: Norte Americana.; GARY M. HEINDEN. Endereço: 14 Woodsend Avenue, Shelton, Connecticut 06484, Estados Unidos. Cidadania: Norte Americana.; DAVID K. LEE. Endereço: 12 Alpine Road, Monroe, Connecticut 06468, Estados Unidos. Cidadania: Norte Americana.

Prazo de Validade : 10 (dez) anos contados a partir de 08/04/2014, observadas as condições legais.

Expedida em : 8 de Abril de 2014.

Assinado digitalmente por
Júlio César Castelo Branco Reis Moreira
Diretor de Patentes

"SISTEMA DE MINISTRAÇÃO DE FRANQUEAMENTO POSTAL SEGURO E PROCESSO PARA EVIDENCIAR PAGAMENTO DE FRANQUIA POSTAL".

O presente é uma 'continuação–em–parte' do pedido de patente provisório US SN 60/049.518, depositado em 13 de junho de 1997 e cedido à cessionária da presente invenção.

Campo Técnico

A presente invenção refere-se genericamente a um sistema de franquia postal e processo para evidenciar o pagamento da franquia em um sistema aberto e, mais especificamente, a um sistema e processo de franquia postal para evidenciar o pagamento da franquia em uma configuração de máquina de franquear virtual.

Pedidos Correlatos

O presente pedido está relacionado com os seguintes pedidos de patente internacional (Nºs do Agente E-731, E-733, E-734, E-735 e E-736), todos depositados concorrentemente com o presente, todos os quais são aqui incorporado a título de referência na sua totalidade.

Técnica Anterior

Sistemas de franqueamento postal foram desenvolvidos que empregam informações criptografadas que são impressas sobre um artigo de correio como parte de marcações postais evidenciando o pagamento do porte postal. As informações criptografadas incluem um valor do porte para o artigo de correio combinado com outros dados postais que referem-se ao artigo de correio e à máquina de franquear que imprime as marcações postais. As informações criptografadas, tipicamente designadas como símbolo digital ou assinatura digital, autentica e protege a integridade de informações, inclusive o valor do porte postal, impresso sobre o artigo de correio para verificação posterior do pagamento do porte. Uma vez que o símbolo digital incorpora informações criptografadas relativas à comprovação de pagamento

de porte, a alteração das informações impressas em uma marcação postal é detectável por procedimentos de verificação padronizados. Exemplos de sistemas que geram e imprimem as ditas marcações postais são descritos nas patentes US: 4.725.718, 4.757.537; 4.775.246 e 4.873.645, cada uma cedida à cessionária da presente invenção.

Atualmente, existem dois tipos de máquinas de franqueamento postal: um sistema fechado e um sistema aberto. Em um sistema fechado, a funcionalidade do sistema é exclusivamente dedicada à atividade de medição. Exemplos de máquinas de franqueamento postal em sistema fechado também são designados de máquina de comprovação de franqueamento, incluem máquinas de franquear digital e analógica convencionais (mecânicas e eletrônicas) nas quais uma impressora dedicada é seguramente acoplada com uma função de medição ou contabilização. Em um sistema fechado, tipicamente a impressora é seguramente acoplada e dedicada à máquina de franquear, e a comprovação de impressão não pode se processar sem levar em conta a evidencia de pagamento de porte. Em um sistema aberto, a impressora não é dedicada à atividade de medir, liberando a funcionalidade do sistema para múltiplas e diversas aplicações além da atividade de medição. Entre os exemplos de máquinas de franquear em sistema aberto se incluem dispositivos baseados em computador pessoal (PC) com sistemas operacionais de tarefa única e/ou múltiplas tarefas, aplicações de múltiplos usuários e impressoras digitais. Uma máquina de franquear em sistema aberto é uma máquina comprovadora de pagamento de porte postal com uma impressora não dedicada que não está seguramente acoplada com um módulo contábil seguro. Uma marcação de sistema aberto impressa pela impressora não dedicada é tornada segura incluindo informações do destinatário na evidencia criptografada de franquia impressa sobre o artigo de correio para subseqüente verificação. Ver as patentes US 4.725.718 e 4.831.555, cada uma cedida à cessionária da presente invenção.

O Serviço dos Correios dos USA ("USPS") propôs um Programa de Marcações Postais Baseado sobre Informações ("IBIP"), que é um sistema seguro distribuído para recondicionar e incrementar as máquinas de franquear existentes utilizando nova evidência de pagamento de porte conhecida como marcações baseadas em informações. O programa confia sobre técnicas de assinatura digital para produzir para cada envelope uma marcação cuja origem pode ser autenticada e o teor da qual não pode ser modificado. O IBIP é previsto suportar novos processos de aplicar franquia adicionalmente à abordagem atual, que tipicamente confia sobre uma máquina de franquear para imprimir marcações sobre artigos de correio. O IBIP requer a impressão de um grande código de barras, de alta densidade, bidimensional ("2-D") sobre um artigo de correio. O código de barras 2-D codifica informações e é assinado com uma assinatura digital.

O serviço de correios dos USA publicou rascunhos de propostas para o IBIP. O INFORMATION BASED INDICIA PROGRAM (IBIP) INDICIUM SPECIFICATION, com data de 13 de junho de 1996, e revisto em 23 de julho de 1997, ("IBIP Indicium Specification") define os requisitos propostos para uma nova marcação que será aplicada ao correio sendo criado utilizando IBIP. O INFORMATION BASED INDICIA PROGRAMA POSTAL SECURITY DEVICE SPECIFICATION, com data de 13 de junho de 1996, e revisto em 23 de julho de 1997, ("IBIP PSD SPECIFICATION") define os requisitos propostos para um Dispositivo de Segurança Postal ("PSD"), que é um dispositivo contábil baseado em processador seguro que ministra e contabiliza o valor postal nele armazenado para suportar a criação de uma nova marcação ou indicação de porte "baseado em informação" que será aplicado ao material de correio a ser postado sendo processado utilizando IBIP. O INFORMATION BASED INDICIA PROGRAM HOST SYSTEM SPECIFICATION, com data de 9 de outubro de 1996, define os requisitos propostos para um elemento de sistema

central de IBIP ("IBIP Host Specification"). IBIP inclui a interconexão de usuário, infra-estruturas postal e de vendedor que constituem os elementos de sistema do programa. O INFORMATION BASED INDICIA PROGRAM KEY MANAGEMENT PLAN SPECIFICATION, com data de 25 de abril de 1997, define a geração, distribuição, uso e substituição das chaves criptográficas usadas pelo provedor de produto/serviço USPS e PSDs ("IBIP KMS Specification"). As especificações são coletivamente aqui designadas de "IBIP Specifications".

As Especificações IBIP definem um sistema de franquia aberto autônomo aqui designado de um Franqueador Postal PC que compreende um PSD acoplado com um computador pessoal ("PC") que opera como um sistema host com uma impressora acoplada com o mesmo ("Host PC"). O PC Host roda o software de aplicação de franquia e bibliotecas associadas (aqui coletivamente designados de "Aplicações Host") e comunica-se com um ou mais PSDs afixados. O Franqueador Postal PC somente pode acessar PSDs acoplados com o PC Host. Inexiste qualquer acesso PSD remoto para o Franqueador Postal PC.

O Franqueador Postal PC processa as transações para fornecer o porte postal, registrar e recarregar o Franqueador Postal PC. O processamento é realizado localmente entre PC Host e o PSD com ele acoplado. As conexões com um Centro de Dados, por exemplo para transações de registro e recarga, são estabelecidas localmente do PC Host através de uma conexão local ou através de uma rede modem/internet. A contabilização para débitos e créditos para o PSD é também efetuada localmente, registrando as transações no PC Host. O PC Host pode acomodar mais de um PSD, por exemplo suportando um PSD por porta serial. Vários programas de aplicação rodando no PC Host, tal como um processador de texto ou impressor de envelope, podem acessar as Aplicações Host.

As especificações IBIP não se dirigem a um sistema de

franqueamento postal aberto IBIP em um ambiente de rede. Todavia, as especificações não interditam um sistema baseado em rede. Genericamente, em um ambiente de rede um Servidor de rede controla a impressão remota solicitada por um PC de Cliente na rede. Naturalmente, o PC de Cliente controla qualquer impressão local.

Um sistema de franquia postal em rede, aqui designado de "franqueador virtual", tem muitos PCs Host sem quaisquer PSDs com ele acoplados. Os PCs Host rodam Aplicações Host, porém todas as funções PSD são desempenhadas sobre Servidores localizados em um Centro de Dados. As funções do SD no Centro de Dados podem ser desempenhadas em um dispositivo seguro afixado a um computador no Centro de Dados, ou podem ser desempenhadas no computador do Centro de Dados propriamente dito. Os PCs Host tem de conectar-se com o Centro de Dados para processar transações tais como ministração de franquias, registro da máquina de franquear ou recarga das máquinas de franquear. As transações são solicitadas pelo PC Host e transmitidas para o Centro de Dados para processamento remoto. As transações são processadas centralmente no Centro de Dados e os resultados são retornados ao PC Host. A contabilização para fundos e processamento de transações são centralizadas no Centro de Dados. Veja-se, por exemplo, as patentes US 5.454.038 e 4.873.645, que são cedidas à cessionária da presente invenção.

A máquina de franquear virtual não satisfaz todos os requisitos atuais das Especificações IBIP. Em particular, as Especificações IBIP não permitem que funções PSD sejam desempenhadas no Centro de Dados. Todavia, é entendido que uma configuração de máquina de franquear virtual com o PSD de cada remetente localizado no Centro de Dados pode proporcionar um nível equivalente de segurança conforme requerido pelas Especificações IBIP.

Nas máquinas de franquear mecânicas e eletrônicas de sistema

fechado convencional um enlace seguro é exigido entre as funções de impressão e as funções contábeis. Para máquinas de franquear configuradas com funções de imprimir e de contabilizar desempenhadas em uma única caixa segura, a integridade da caixa segura é monitorada por inspeções periódicas das máquinas de franquear. Mais recentemente, máquinas de franquear com impressão digital tipicamente incluem uma impressora digital acoplada com um dispositivo contador (com função contábil), que é aqui designado de uma dispositivo de segurança postal (PSD). As máquinas de franquear digitais eliminaram a necessidade por inspeção física criptograficamente protegendo o enlace entre os mecanismos de contabilizar e de imprimir. Essencialmente, as novas máquinas de franquear com impressão digital criam um enlace de comunicação ponto a ponto seguro entre o PSD e a cabeça impressora. Veja-se, por exemplo, a patente US nº 4.802.218, concedida a Christopher B. Wright e ora cedida à cessionária da presente invenção. Um exemplo de uma máquina de franquear com impressão digital com comunicação segura com a cabeça impressora é a Personal Post Office™ fabricada pela Pitney Bowes Inc. de Stamford, Connecticut.

Nas patentes US nºs. 4.873.645 e 5.454.038, um sistema e processo de franquear virtual são expostos nas quais a contabilidade postal e geração de símbolos ocorre em um centro de dados afastado da impressora comprovadora de franquia. Embora o Centro de Dados possa ser uma instalação segura, permanecem determinadas questões de segurança intrínsecas uma vez que as funções contábeis e de geração de símbolos não ocorrem em um dispositivo seguro local para a impressora de franquia. O sistema de franquia postal virtual inclui um computador acoplado com uma impressora não segura e com um sistema contador de dados remoto. A contabilização postal e a geração de símbolos ocorrem no Centro de Dados.

O Centro de Dados é uma instalação centralizada sob o

controle de um fornecedor de máquinas de franquear, tal como a Pitney Bowes ou a repartição dos correios. Como tal, é considerada como segura comparada com o ambiente em que os clientes manuseiam as máquinas de franquear diretamente. Todavia, os dados armazenados no Centro de Dados são acessíveis ao pessoal do Centro de Dados e, por conseguinte, sujeitos no mínimo à modificação inadvertida pelo pessoal em questão. Quaisquer mudanças desautorizadas para o usuário e dados de medidor armazenados no Centro de Dados comprometem a integridade do sinal de máquina de franquear virtual.

Descrição da Invenção

Foi determinado que um sistema de franqueamento postal virtual proporciona benefícios que não são disponíveis sob sistemas de pagamento de porte postal convencionais. Para os Correios, um sistema de franquia postal virtual proporciona gerenciamento central de toda franquia postal sem a necessidade de gerenciar as máquinas de franquiar físicas ou PSDs. Um outro benefício é a oportunidade para associar diretamente um expedidor com cada artigo postal em contraposição a cada restauração. Tampouco os expedidores necessitam manter listas atuais de endereços válidos, tais como com CD-ROMs adquiridos. Os expedidores ou remetentes podem adquirir franquia numa base conforme necessitada. Finalmente, os fornecedores de máquinas de franquear não tem de manter acompanhamento de máquinas de franquear físicas. Um sistema de franquear postal virtual elimina problemas de máquinas de franquear roubadas ou relocadas e simplifica o gerenciamento de máquinas de franquear em geral.

A presente invenção proporciona segurança de dados digitais para um Centro de Dados de um sistema de franqueamento postal virtual que previne modificações inadvertidas e intencionais para os dados de medidor e de usuário armazenados no Centro de Dados. De acordo com a presente invenção caixas de segurança são usadas para proteger contra alteração

desautorizada de máquinas de franquear e de registros de usuários armazenados no centro de dados. A presente invenção também proporciona controle seguro do processo de geração de símbolos digitais e a contabilidade segura associada para transação evidenciadora de franquia que ocorra no Centro de Dados.

As questões de segurança para o sistema de franqueamento postal virtual incluem autenticação de usuário, transações financeiras e de franquia, e registros de medidores. Para a autenticação de usuário e de registros de medidor, as base dados armazena chaves de criptografação em texto cifrado e não em texto normal.. Para cada transação, todos os dados, inclusive um carimbo horário ou número de sequência, usados para completar a transação são digitalmente assinados e a assinatura é armazenada como parte do registro de transação atualizado. Verificou-se que a manutenção de registros de transação desta maneira previne modificação inadvertida dos registros.

Embora a assinatura digital proporcione segurança razoável, não é "a prova de bala". Verificou-se que um registro historicamente assinado poderia ser usado em lugar de um registro atual exigindo um sistema de verificação mais robusto para detectar a dita "violação". De acordo com a presente invenção, outro nível de segurança é adicionado. Verificou-se que uma vez que a assinatura seja verificada, os dados da transação podem ser testados quanto à sua "atualização" para eliminar qualquer possibilidade de violação, inadvertida ou intencional.

De acordo com a presente invenção, um sistema e processo de comprovação de pagamento de franquia proporciona uma caixa segura que é usada para assinar os dados da transação e autenticar registros de medidor e de usuário. O sistema e processo inclui um centro de dados com uma base de dados contendo uma pluralidade de registros de medição armazenados. Cada registro de medição inclui informações de franquia correspondentes a uma

conta de franquia postal alocada a cada um de uma pluralidade de dispositivos de usuário remotos que estão autorizados a solicitar comprovação de pagamento de porte ou franquia postal. Quando uma solicitação por franquia postal é recebida no centro de dados, um dispositivo coprocessador seguro no centro de dados obtém o registro de medidor apropriado e verifica a autenticidade do registro de medidor verificando uma assinatura no registro do medidor e comparar dados atuais no registro de medidor com dados de atualização no dispositivo seguro. Se verificado, o dispositivo seguro então justifica um valor de franquia postal a ser comprovado, gerando evidência do pagamento do porte ou franquia postal e atualiza as informações do registro, inclusive a condição atualizada dos dados, no registro do medidor. O dispositivo seguro então assina as informações de medidor atualizadas e armazena a assinatura no registro de medidor. O dispositivo seguro então retorna o registro de medidor atualizado à base de dados.

Descrição Sucinta dos Desenhos

Os acima e demais objetivos e vantagens da presente invenção se evidenciarão do exame da descrição detalhada que se segue, tomada em conjunção com os desenhos apensos, nos quais caracteres de referência idênticos se reportam a partes idênticas através da sua totalidade, e nos quais:

A fig. 1 é um diagrama em blocos de um sistema de franquia postal virtual para ministrar franquias incorporando os princípios da presente invenção;

A fig. 2 é um diagrama em blocos do servidor de base de dados do Centro de Dados e caixa segura para o sistema de franquia postal virtual da fig. 1;

A fig. 3 é um fluxograma do processo para comprovar pagamento de franquia postal pelo sistema de franquia postal virtual da fig. 1; e

A fig. 4 é um fluxograma do processo realizado dentro da caixa de medidor segura do sistema de franquia postal virtual da fig. 1.

Modalidade Ideal de Realização da Invenção

Na descrição da presente invenção, referência é feita aos desenhos nos quais é visto na fig. 1, u m sistema de franquia postal virtual, genericamente designado 10. O sistema de franquia postal virtual 10 inclui uma pluralidade (somente um é mostrado) de sistemas de computador pessoal (PC), genericamente designados 20, cada um tendo acesso a uma impressora 22 para imprimir evidência de pagamento de franquia ou porte sobre um envelope ou etiqueta. O PC 20 é conectado com um Centro de Dados 30 de processamento de transação que efetuar a contabilidade postal e a comprovação do pagamento de franquia. O sistema de franquia postal virtual 10 permite que cada expedidor ou remetente utilize um PC convencional para remotamente obter evidência de pagamento de franquia numa base conforme necessário. Distintamente dos sistemas de franquia postal convencional, o sistema de franquia postal virtual 10 não inclui qualquer hardware medidor localizado no local do expedidor ou remetente. Tampouco são armazenados quaisquer fundos postais no local do expedidor. Toda medição e contabilização de fundos ocorre no Centro de Dados 30 utilizando software funcional e registros de base de dados representando cada "máquina de franquear" de remetente, aqui designado de "conta da máquina de franquear".

O processo de contabilização para o sistema de franquia postal virtual 10 pode ser um sistema de pré-pagamento convencional ou sistema de pós-pagamento. O processo preferencial um processo de pagamento prévio no qual cada máquina de franquiar é exigida a depositar uma quantia mínima de dinheiro na conta da máquina de franquiar virtual do expedidor ou remetente.

A medida que os fundos da conta decrescem abaixo de um nível específico uma recarga é debitada à conta corrente do expedidor. Um

processo contábil alternativo que é conveniente para um sistema de franquia postal virtual é um processo de pagamento em tempo real no qual a quantia de uma transação é debitada em uma conta de cartão de crédito do expedidor quando a transação ocorre. Este processo é aqui designado de um pagamento de franquia "carregador gotejador", porque o remetente ou expedidor não paga pela franquia postal por um artigo de correio até o expedidor estar pronto para imprimir a franquia sobre o artigo de correio.

No sistema de franqueamento postal virtual, um vendedor de "franquia postal" tal como a Pitney Bowes Inc. fornece ao expedidor software de cliente que roda no PC 20, p.ex. o software de cliente pode ser transferido do servidor de Internet do vendedor. Alternativamente, o software de cliente pode ser "home pages" do navegador de Internet que proporciona interações do usuário com o Centro de Dados. O vendedor de medidor (franqueador) também gerencia o Centro de Dados 30. O software de cliente inicia comunicações com o Centro de Dados 30 que realiza transações de medição para evidenciar a franquia para artigos postais individuais ou lotes de artigos postais. Na concretização preferencial, o software de cliente estabelece uma conexão com o Centro de Dados, e solicita franquia fornecendo informações postais relativas às transações solicitadas, tal como o valor da franquia ou porte postal, informações de destinatário e (opcionalmente) a origem do depósito para cada artigo postal. O centro de Dados 30 recebe as informações postais, determina o código de endereçamento (CEP) de origem para o artigo postal, desempenha funções contábeis e gera uma evidência criptografada de pagamento do porte postal (franquia), tal como um símbolo ou assinatura digital, e transmite informações das marcações postais inclusive o símbolo, para o PC 20. O PC 20 recebe as informações de marcações postais, cria um mapa de bits das marcações postais, que podem ser exibidas visualmente sobre um monitor de PC (não mostrado) e impressas sobre o artigo postal pela impressora 22. O

PC 20 então desconecta-se do Centro de Dados 30 ou solicita outra transação. A conexão entre o PC 20 e o Centro de Dados 30 pode ser através de um Provedor de Serviços de Rede, tal como sobre a Internet, ou por discagem direta utilizando o modem do PC.

O sistema de franqueamento postal virtual 10 elimina a necessidade de manter e contabilizar máquinas de franquear tradicionais no local de cada expedidor e proporciona flexibilidade para processar solicitações de múltiplas origens de depósito por cada expedidor. O sistema de franqueamento postal virtual 10 também presta serviços de valor agregado que não são disponíveis com as máquinas de franquear convencionais, tais como higiene de endereço em tempo real, serviços de marketing direto e pagamento de porte postal por "gotejamento". O sistema de franqueamento postal virtual 10 proporciona autenticação do usuário pelo Centro de Dados 30 para identificar expedidores com contas válidas. Quando um expedidor tiver sido autenticado para cada solicitação, por exemplo, pelo nome de um usuário, senha, ou outros métodos convencionais, o Centro de Dados 30 atende à solicitação, e retorna informações de marcações postais para o PC 20 onde a marcação postal é criada e impressa sobre um artigo de correio.

Reportando-se mais uma vez à fig. 1, o expedidor inicia uma transação evidenciadora de franqueamento postal rodando software de cliente no PC 20, que contacta o Centro de Dados 30. No Centro de Dados 30, um Servidor de Comunicação 32 suporta a conectividade de várias tecnologias e protocolos de comunicação. O Servidor de Comunicação efetua a fusão de todo o tráfego entrante e o encaminha para um Servidor de Função 34, que inclui software de aplicação que suporta a conexão do expedidor, a ministração de franquia e reporte postal. Todas as informações de expedidor e de franquia postal são acessadas a partir de um Servidor de Base de Dados 36 onde as informações são seguramente armazenadas utilizando processos e protocolos criptográficos seguros como descrito abaixo. O Centro de Dados

30 mantém chaves criptográficas para cada conta de medidor no Servidor de Base de Dados 36. As chaves criptográficas são usadas para comprovação e verificação de franquias assim como para segurança dos registros armazenados no Servidor de Base de Dados 36. Um sistema de gerenciamento de chaves 38 administra todas chaves criptográficas usadas no sistema de franqueamento postal virtual 10. As chaves criptográficas podem ser distribuídas para verificadores em locações remotas. O pedido de patente US SN 08/553812, depositado em 23 de outubro de 1995, e cedido à cessionária da presente invenção, descreve o dito sistema de gerenciamento de chaves.

Um expedidor pode abrir uma conta de franquia postal através de um processo de conexão em linha com o Centro de Dados 30. Durante a conexão, o expedidor introduz, no PC 20, informações de conta, tal como nome de usuário, senha e processo de pagamento. Quaisquer taxas de registro podem ser debitadas nessa ocasião. O Centro de Dados 30, de preferência administrado por um fornecedor ou vendedor de máquinas de franquear, tal como a Pitney Bowes Inc., formula todas as licenças de franquia e contratos entre seus expedidores e a repartição dos Correios.

Na presente invenção, o PSD é inexistente, isto é, inexiste qualquer máquina de franquear acoplada com o PC do qual o pagamento de franquia seja solicitado. O sistema de franqueamento postal virtual 10 substitui as funções contábeis e medidoras do PSD com software de medição no PC 20 e informações de conta do expedidor executadas e atualizadas no Centro de Dados 30. O sistema de franqueamento postal virtual 10 provê cada expedidor com um sistema de medição que tem a faculdade de originar transações provenientes de múltiplas origens de depósito. Ver, por exemplo, o Pedido de Patente Internacional SN **[Nº do Agente E-735]**.

Vários métodos podem ser usados para determinar a origem de depósito para uma transação solicitada. Por exemplo, um método para

determinar o código de endereçamento postal de origem utilizando uma ID de chamador de uma chamada telefônica é exposto no pedido de patente US SN 08/775.818, depositado em 31 de dezembro de 1996, e cedido à cessionária da presente invenção, que é aqui incorporado na sua totalidade a título de referência.

De acordo com a presente invenção, um ou mais módulos criptográficos, aqui designados de "caixas seguras", são localizados dentro do Centro de Dados 30 e são usados para executar processos criptográficos. Cada caixa segura é um dispositivo seguro, evidenciador de violação e que reage à violação, incluindo um processador e memória, que armazena chaves de criptografação e executa operações criptográficas utilizando as chaves dentro dos limites seguros do dispositivo. O Centro de Dados 30 inclui vários tipos de caixas seguras que são descritos abaixo. Na concretização preferencial, o Centro de Dados 30 inclui múltiplas caixas de cada tipo para redundância e desempenho.

O Sistema de Gerenciamento de Chaves 38 inclui uma caixa de manufatura (não mostrada) que proporciona chaves de nível mais alto usadas para gerar números randômicos para semear cada uma das outras caixas seguras. Compartilhando uma chave criptográfica comum, as caixas seguras se comunicam com segurança dentro do Centro de Dados 30. O Sistema de Gerenciamento de Chave 38 também inclui uma caixa de "aço" (não mostrada) que partilha uma chave comum com a caixa de medidor 44 (descrita abaixo) para criptografar/descriptografar chaves símbolo de autorização para evidenciar transações de franquia para a conta de cada medidor. A caixa de aço efetua a fusão de uma chave de vendedor e de chave postal em um registro no texto cifrado. Para cada conta de medidor, o Centro de Dados 30 cria um medidor lógico, isto é, um registro de medidor, no Servidor de Base de Dados 36 gerando uma chave símbolo utilizando as chaves de vendedor e postal, inicializando registros de medidor (ascendentes

e descendentes), dados de atualização de medidor (descritos abaixo) e outras informações postais como parte do registro de medidor, e a seguir armazenando o registro de medidor no Servidor de Base de Dados 36.

O Centro de Dados 30 também inclui uma caixa de medidor 44 que compartilha uma chave secreta com a caixa de aço para descriptografar a chave símbolo criptografada no registro de medidor. A caixa de medidor 44 também armazena a chave usada para a assinatura digital de registros de transação. A única outra informação armazenada na caixa medidor 44 são os dados de atualização para registro de medidor processado pela caixa de medidor 44. Para cada transação de franquia, a caixa de medidor 44 gera pelo menos um símbolo digital ou assina a transação de franquia, e atualiza o registro de medidor correspondente à transação. Cada registro de medidor no Servidor de Base de Dados 36 inclui fundos postais assim como as chaves símbolo em texto cifrado. A caixa de medidor 44 utiliza as chaves símbolo para gerar símbolos, atualizar os fundos postais no registro do medidor, e assina o registro de medidor atualizado. Desta maneira, a caixa de medidor 44 efetua e controla a contabilidade segura para cada transação. A caixa de medidor 44 também pode ser usada para verificar o símbolo ou a assinatura de transação para verificação da franquia evidenciadora para a transação.

O Centro de Dados 30 também inclui uma caixa de autenticação 40 que compartilha uma chave secreta diferente com a caixa de aço para descriptografar uma chave de autenticação de usuário armazenada em texto cifrado no Servidor de Base de Dados 36. A caixa de autenticação 40 também executa os algoritmos de autenticação utilizando a chave de autenticação descriptografada para autenticar um expedidor. Esta função pode ser adicionada à caixa de aço do Sistema de Gerenciamento de Chave 38 para eliminar a necessidade por uma caixa separada no Centro de Dados 30.

Finalmente, o Centro de Dados 30 inclui uma caixa de transação 42 que compartilha outra chave secreta com a caixa de aço para assinar outros registros de transação de usuário diferentes dos registros de medidor assinados pela caixa de medidor 44, tais como conexões e registros de histórico de conexão. A caixa de transação 42 posteriormente verifica a assinatura de registro de transação quando a transação seguinte é solicitada.

Reportando-se a seguir à fig. 2, é mostrada uma configuração de Servidor de Base de Dados 36, incluindo uma base de dados de medidor 60, uma base de dados de expedidor 62 e uma base de dados de registros de medidor 64. A base de dados de medidor 60 compreende informações de medidor associadas para cada conta de medidor, tais como, número serial de medidor, contador de atualização de registro, registro ascendente, registro descendente e outros valores postais. A base de dados de expedidor 62 compreende informações de expedidor e informações que associam um expedidor com uma conta de medidor.

Em operação, o Servidor de Comunicação 32 recebe uma solicitação por uma transação de medidor do PC 20 do expedidor. O software de aplicação no Servidor de Função 34 controla o processamento da solicitação de transação. O Servidor de Função 34 acessa a base de dados do expedidor 62 e a base de dados do medidor 60 para obter registros, inclusive o registro do medidor apropriado 64, correspondente à conta de medidor do expedidor iniciador da solicitação. O Servidor de Função 34 comunica registros de expedidor da base de dados de expedidor 62 à caixa de autenticação 40, que a seguir autentica o expedidor solicitador da transação. Uma vez que o expedidor tenha sido autenticado, o Servidor de Função 34 comunica o registro de registro apropriado 64 à caixa de medidor 44, que verifica uma assinatura e dados de atualização para o registro. A caixa de medidor 44 decifra a chave ou chaves criptografadas que são armazenadas dentro do registro de medidor 64, desempenha funções contábeis sobre os

registros ascendentes e descendentes no registro de medidor 64, e utiliza as chaves para gerar um símbolo para a transação solicitada. A caixa de medidor 44 então gera dados para uma marcação postal, e re-assina o registro de medidor 64. O registro atualizado e assinado é então transmitido de retorno para o Servidor de Base de Dados 36 onde é armazenada como parte da base de dados do medidor 60.

No Centro de Dados 30, as chaves de autenticação não são disponíveis em texto normal, porém tem de ser distribuídas para o expedidor. Os processos convencionais de distribuição e atualização da chave de autenticação para cada expedidor pode ser usada. Ver, por exemplo, o pedido de patente previamente indicado US SN 08/553.812, que descreve um sistema de gerenciamento de chaves para distribuir e atualizar chaves criptográficas para as caixas seguras e o PC do expedidor.

Uma das tarefas importantes para o sistema de gerenciamento de chaves 38 é obter uma chave postal e associar a mesma com a chave de um vendedor. No sistema de gerenciamento de chaves 38, a caixa de aço cria um número serial de medidor, número de fabricação, chaves de vendedor e postal em um registro de medidor 64 para cada conta de medidor.

Para os algoritmos de criptografar/decriptografar, uma série de chaves DES tripla é usada para codificar as chaves de criptografação para gerar símbolos ou assinaturas para marcações postais (indicia). Outra série de chaves DES tripla é usada para assinar os registros de medidor. A caixa de medidor 44 armazena com segurança ambas as séries de chaves DES triplas. De maneira a evitar a utilização de somente uma chave para cifrar a inteira série de chaves de medidor para gerar símbolos ou assinaturas para marcações postais (indicia), uma chave derivada é adotada. A primeira série de chaves DES triplas deriva chaves DES triplas criptografando o número serial (conta) de medidor em cada registro de medidor. As chaves DES triplas derivadas então cifram as chaves de criptografação para as marcações postais

que devem ser armazenadas no Servidor de Base de Dados 36 A segunda série de chaves DES triplas para assinatura utiliza um esquema similar para derivar as chaves de assinatura de uma maneira similar, isto é, utilizando o número serial de medidor como dados para derivar chaves. Será entendido que uma série de chaves DES triplas pode ser usada para ambas as finalidades. Todavia, há conveniência que cada série de chaves seja usada somente para uma finalidade.

Na concretização preferencial da presente invenção, uma chave comum é usada para assinar todas as transações e registros que requeiram uma assinatura digital, tais como, registros de medidor, transações de franquia postal, registros de transferência de fundos, registros de conta mestre, etc. Múltiplas caixas de cada caixa são usadas para redundância e partilhar a carga de trabalho com o crescimento do número de transações. A caixa de assinatura, tal como a caixa de medidor 44 ou caixa de autenticação 40, também verificará a assinatura de um registro.

Com relação ao algoritmo de assinatura para o registro de medidor 64, um código de autenticação de mensagem (MAC) é empregado para assegurar a integridade de mensagem para os registros de medidor virtual sensíveis.

Este MAC envolve múltiplas aplicações do Padrão de Criptografação de Dados (DES). As chaves de assinatura serão atualizadas utilizando o mês e ano corrente. Durante a fabricação, duas chaves mestre iniciais serão introduzidas na memória não-volátil (NVM) da caixa de medidor 44. A NVM é usada tanto para armazenamento permanente como para a prevenção de acesso externo às informações chave. As chaves para as marcações postais e as chaves para assinatura são derivadas de uma maneira convencional, tal como descrita acima. O algoritmo de verificação de assinatura de registro de medidor virtual simplesmente recalcula a assinatura do registro de medidor 64 utilizando o algoritmo de assinatura e dados dentro

do registro de medidor 64 e compara a assinatura calculada com a assinatura no registro de medidor 64.

Reportando-se a seguir à fig. 3, o processo para realizar com segurança uma transação evidenciadora de franquia em um sistema de franqueamento postal virtual é descrito. Na etapa 100, o Servidor de Comunicação 32 recebe uma solicitação por mostra de franquia do PC 20 do expedidor. Na etapa 105, o Servidor de Função 34 solicita acesso às informações de conta de expedidores armazenadas no Servidor de Base de Dados 36. Na etapa 110, o Servidor de Base de Dados 36 emite informações do expedidor, informações do medidor, inclusive um registro de medidor associado com o expedidor que iniciou a solicitação. Na etapa 115, o Servidor de Função 34 transmite as informações de expedidor para a Caixa de Autenticação 40. Quando o expedidor é autenticado na etapa 120, então, na etapa 125, o Servidor de Função 34 emite as informações de medidor, inclusive o registro do medidor para a caixa de medidor 44. Na etapa 130, a caixa de medidor 44 autentica o registro do medidor, decifra a chave símbolo criptografada que é parte do registro, verifica a atualização do registro, efetua a contabilização, gera um símbolo, atualiza os dados e assina o registro do medidor, que é retornado ao Servidor de Função 34. Na etapa 135, o Servidor de Função 34 envia o registro atualizado e assinado para o Servidor de Base de Dados 36 e transmite para o Servidor de Comunicação 32 o símbolo e informações postais associadas necessárias para criar uma marcação postal. Na etapa 140, o Servidor de Base de Dados 36 armazena o registro de medidor atualizado e assinado. Na etapa 145, o Servidor de Comunicação 32 emite as informações de símbolo e postais para o PC 20 de expedidor.

Reportando-se a seguir à fig. 4, o processo realizado dentro da caixa de medidor segura do sistema de franqueamento postal virtual é descrito. Na etapa 200, a caixa de medidor 44 recebe um registro de medidor assinado. Na etapa 205, a assinatura do registro de medidor é verificada. Se

não verificada na etapa 210, então, na etapa 215, a caixa de medidor termina a transação e alerta o Servidor de Função 34 para possível violação. Se a assinatura foi verificada, então, na etapa 220, a caixa de medidor compara os dados de atualização que são armazenados na caixa de medidor para cada conta de medidor com dados de atualização armazenados como parte do registro do medidor. Os dados de atualização selecionados para esta comparação tem de ser dados que são singulares para cada transação. Na concretização preferencial, o contador de atualização de registro é usado, todavia, um número randômico, carimbo horário ou outro termo usado para a ocasião ode ser usado. A comparação na etapa 220 previne substituição inadvertida ou intencional do registro de medidor atual por um registro de medidor antigo durante a transação de franqueamento postal virtual.

Na etapa 225, se os dados de atualização comparados não são idênticos, então, na etapa 230, a caixa de medidor termina a transação e alerta o Servidor de Função 34 para possível violação. Se os dados de atualização armazenados no registro do medidor são idênticos aos dados de atualização associados com o registro de medidor que é armazenado na caixa de medidor, então, na etapa 235, a caixa de medidor decifra a chave símbolo que foi recebida na forma criptografada como parte do registro de medidor. Na etapa 240, a caixa de medidor desempenha funções contábeis para a transação, tal como incrementar o registro ascendente, decrementar o registro descendente e incrementar o contador de atualização de registro. Na etapa 245, os dados de atualização no registro de medidor são atualizados. Na etapa 250, os dados de atualização armazenados na caixa de medidor são atualizados. Na etapa 255, a caixa de medidor gera o símbolo utilizando a chave símbolo descriptografada. Na etapa 260, a caixa de medidor atualiza o registro do medidor armazenando os novos valores de registro e contador de atualização de registro no registro de medidor, e então assina o registro atualizado utilizando uma chave armazenada na caixa de medidor. Na etapa 265, a caixa

de medidor transmite o registro de medidor atualizado e assinado para o Servidor de Base de Dados 36 para armazenamento até a transação seguinte para a conta de medidor alocada ao registro de medidor.

Será entendido que, embora as concretizações da presente invenção sejam descritas como sistemas de franqueamento postal, a presente invenção é aplicável a qualquer sistema de medição ou contagem de valores que inclua comprovação de transação, tais como transações monetárias, transações de artigos e transações de informações.

Embora a presente invenção tenha sido exposta e descrita com referência à concretizações da mesma, será evidente, como indicado acima, que variações e modificações, tais como a utilização de chaves públicas em vez de chaves privadas, podem ser introduzidas. É assim proposto nas reivindicações que se seguem abranger cada variação e modificação que se enquadre dentro do fiel espírito e âmbito da presente invenção.

REIVINDICAÇÕES

1. Sistema de ministração de franqueamento postal seguro, o qual compreende:

um centro de dados para ministrar franquia postal em resposta a solicitações por franquia postal a partir de uma pluralidade de dispositivos de usuário remotos, o centro de dados incluindo:

dispositivos de base de dados para armazenar registros de dados, os registros de dados incluindo informações de usuário e informações de medidor para contas de medição individuais, cada uma das contas de medidor sendo alocadas a cada um da pluralidade de dispositivos de usuário remotos;

dispositivos para receber solicitações por evidência de franquia postal a partir da pluralidade de dispositivos de usuário remotos;

dispositivos para autenticar cada solicitação por evidência de franquia postal utilizando ambas as informações de usuário e informações de medidor correspondentes à conta de medição para o dispositivo de usuário remoto que inicia a solicitação por evidência de franquia postal; e

dispositivos para ministrar a evidência de franquia postal solicitada, ditos dispositivos ministradores incluindo pelo menos um primeiro dispositivo seguro, o qual inclui processador e memória, no qual dito primeiro dispositivo seguro obtém as informações de medidor dos dispositivos de base de dados, verifica a autenticidade das informações de medidor, gera a evidência de franquia postal solicitada, atualiza as informações de medidor, sendo que é caracterizado pelo fato de que assina digitalmente as informações de medidor atualizadas e retorna as informações de medidor atualizadas e assinadas aos dispositivos de base de dados.

2. Sistema de acordo com a reivindicação 1, caracterizado pelo fato de que ditos dispositivos de base de dados incluem uma base de dados de registros de medidor, cada um dos registros de medidor incluindo as informações de medidor correspondentes a uma das contas de medição para a pluralidade de

dispositivos de usuário remotos e uma assinatura das informações de medidor.

3. Sistema de acordo com a reivindicação 2, caracterizado pelo fato de que as ditas informações de medidor incluem registros ascendentes e descendentes, uma chave símbolo criptografada e dados de atualização.

4. Sistema de acordo com a reivindicação 3, caracterizado pelo fato de que os dados de atualização compreendem um contador de atualização de registro correspondente ao número de transações evidenciadoras de franquia postal processadas pelo dito dispositivo seguro.

5. Sistema de acordo com a reivindicação 2, caracterizado pelo fato de que dito primeiro dispositivo seguro inclui dispositivos para armazenar primeira e segunda chaves criptográficas, dita primeira chave sendo usada para verificar a assinatura em cada registro de medidor e para assinar as informações de medidor atualizadas antes de retornar cada registro de medidor para os ditos dispositivos de base de dados, dita segunda chave sendo usada para realizar a descriptografia da chave símbolo criptografada no registro de medidor, o dito dispositivo seguro utilizando a chave símbolo para a geração da evidência de franquia postal solicitada.

6. Sistema de acordo com a reivindicação 5, caracterizado pelo fato de que um servidor de função processa cada solicitação recebida pelo dito servidor de comunicação e obtém as informações de usuário e as informações de medidor apropriadas a partir do dito servidor de base de dados e emite ditas informações de usuário e ditas informações de medidor para os dispositivos de autenticação e para os dispositivos ministradores.

7. Sistema de acordo com a reivindicação 1, caracterizado pelo fato de que os dispositivos para autenticação compreendem uma segunda caixa segura, a qual inclui processador, memória e dispositivos para armazenar uma terceira chave criptográfica, dita terceira chave sendo usada para verificar uma assinatura associada com as ditas informações de usuário da conta de medição sendo processada.

8. Sistema de acordo com a reivindicação 7, caracterizado pelo fato de compreender adicionalmente um servidor de sistema de gerenciamento de chave para gerar e manter chaves criptográficas usadas pelos dispositivos de autenticação e pelos dispositivos ministradores.

9. Sistema de acordo com a reivindicação 1, caracterizado pelo fato de que os ditos dispositivos para recepção compreendem um servidor de comunicação e ditos dispositivos de base de dados compreendem um servidor de base de dados, cada um sendo localizado no centro de dados.

10. Processo para evidenciar pagamento de franquia postal, o qual compreende as etapas de:

proporcionar uma pluralidade de registros de medidor, cada registro de medidor incluindo uma informação de medidor correspondente a uma conta de medidor alocada a cada um de uma pluralidade de dispositivos de usuário remotos que são autorizados a solicitar evidência de pagamento de franquia postal;

armazenar a pluralidade de registros de medidor numa base de dados em um centro de dados;

obter um primeiro registro de medidor quando uma solicitação por evidência de pagamento de franquia postal é recebida pelo centro de dados;

verificar a autenticidade do dito primeiro registro de medidor, verificando-se uma assinatura no primeiro registro de medidor;

contabilizar um valor de franquia postal evidenciado;

gerar um símbolo digital como uma evidência de pagamento de franquia postal;

atualizar as informações de medidor no dito primeiro registro de medidor;

caracterizado por, adicionalmente, compreender as etapas de:

assinar as informações de medidor atualizadas para atualizar a assinatura do primeiro registro de medidor; e

retornar o primeiro registro de medidor atualizado à base de dados.

11. Processo de acordo com a reivindicação 10, caracterizado pelo fato de que ditas etapas de obter, verificar, contabilizar, gerar, atualizar, assinar e retornar são executadas em um dispositivo seguro.

12. Processo de acordo com a reivindicação 11, caracterizado pelo fato de que a etapa de verificar a autenticidade daquele primeiro registro de medidor compreende a etapa de:

comparar dados de atualização no primeiro registro de medidor com dados de atualização armazenados no dispositivo seguro.

13. Processo de acordo com a reivindicação 11, caracterizado pelo fato de que a etapa de atualizar as informações de medidor compreende a etapa de:

atualizar os dados de atualização armazenados no dispositivo seguro e no primeiro registro de medidor.

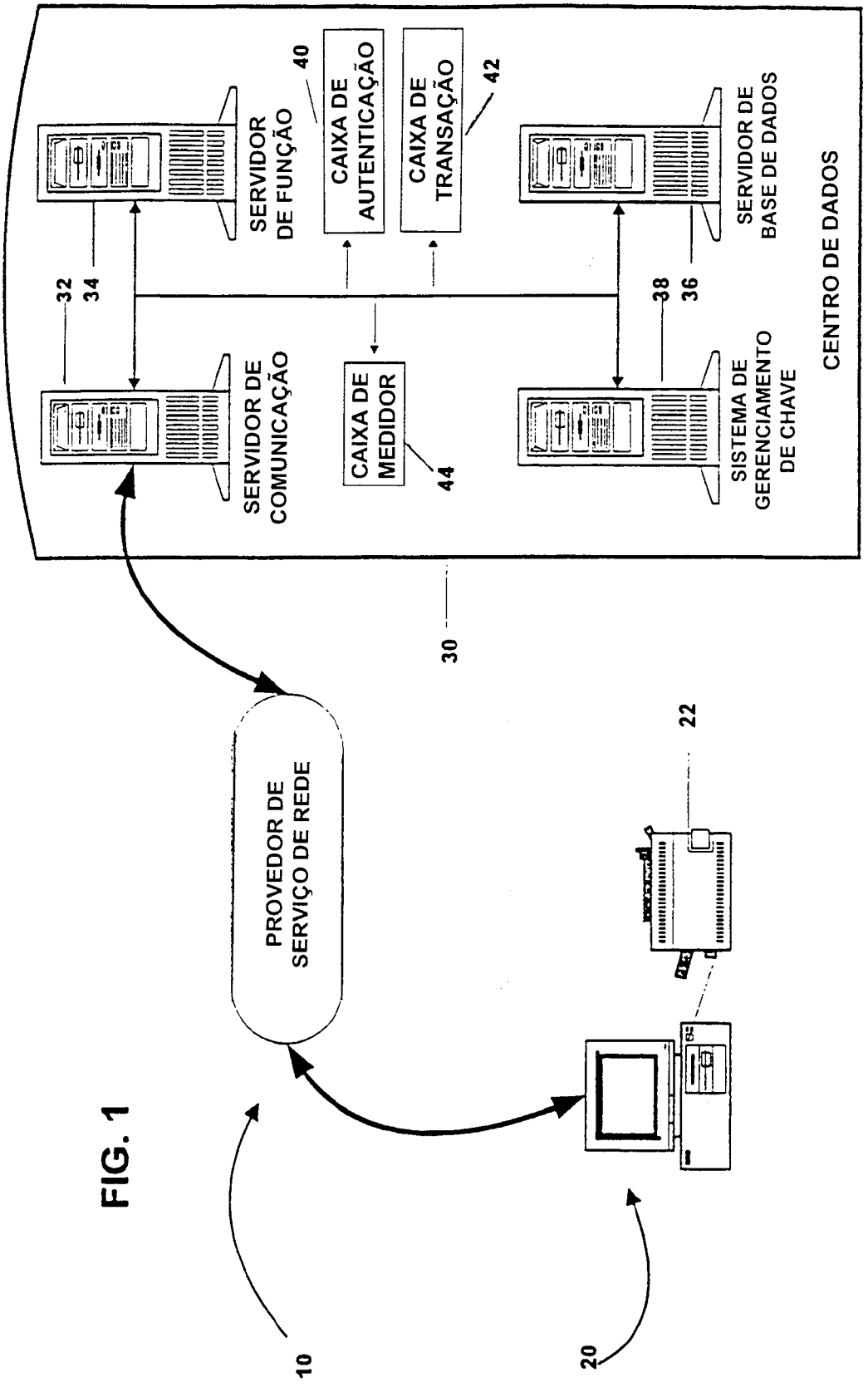
CENTRO DE DADOS
SERVIDOR DE FUNÇÃO
CAIXA DE AUTENTICAÇÃO
CAIXA DE TRANSAÇÃO
SERVIDOR DE BASE DE DADOS
SERVIDOR DE COMUNICAÇÃO
CAIXA DE MEDIDOR
SISTEMA DE GERENCIAMENTO DE CHAVE
PROVEDOR DE SERVIÇO DE REDE
10
20
22
30
32
34
36
38
40
42
44

FIG. 1

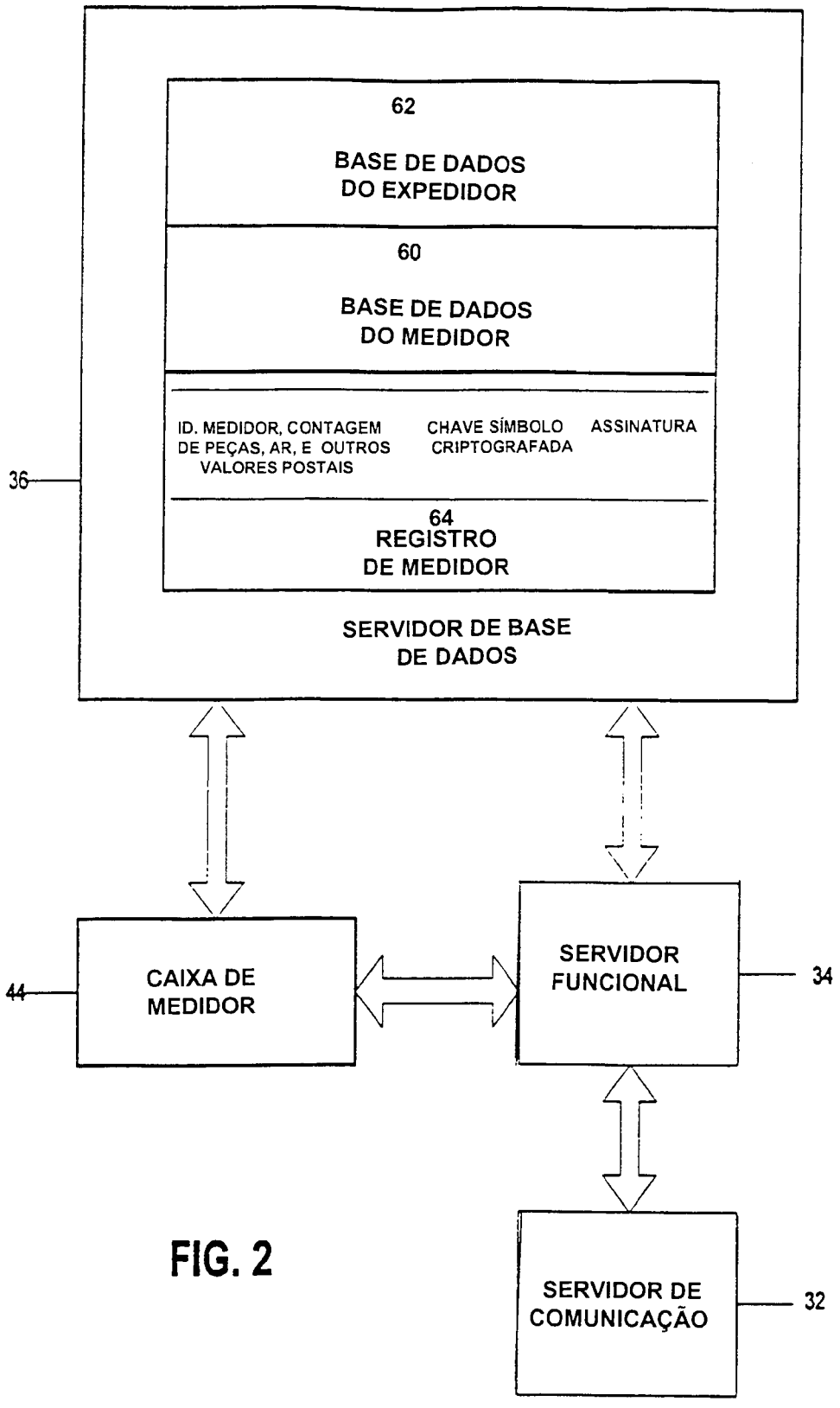
62
BASE DE DADOS
DO EXPEDIDOR
60
BASE DE DADOS
DO MEDIDOR
ID. MEDIDOR, CONTAGEM
DE PEÇAS, AR, E OUTROS
VALORES POSTAIS
CHAVE SÍMBOLO
CRIPTOGRAFADA
ASSINATURA
64
REGISTRO
DE MEDIDOR
SERVIDOR DE BASE
DE DADOS
36
CAIXA DE
MEDIDOR
44
SERVIDOR
FUNCIONAL
34
SERVIDOR DE
COMUNICAÇÃO
32

FIG. 2

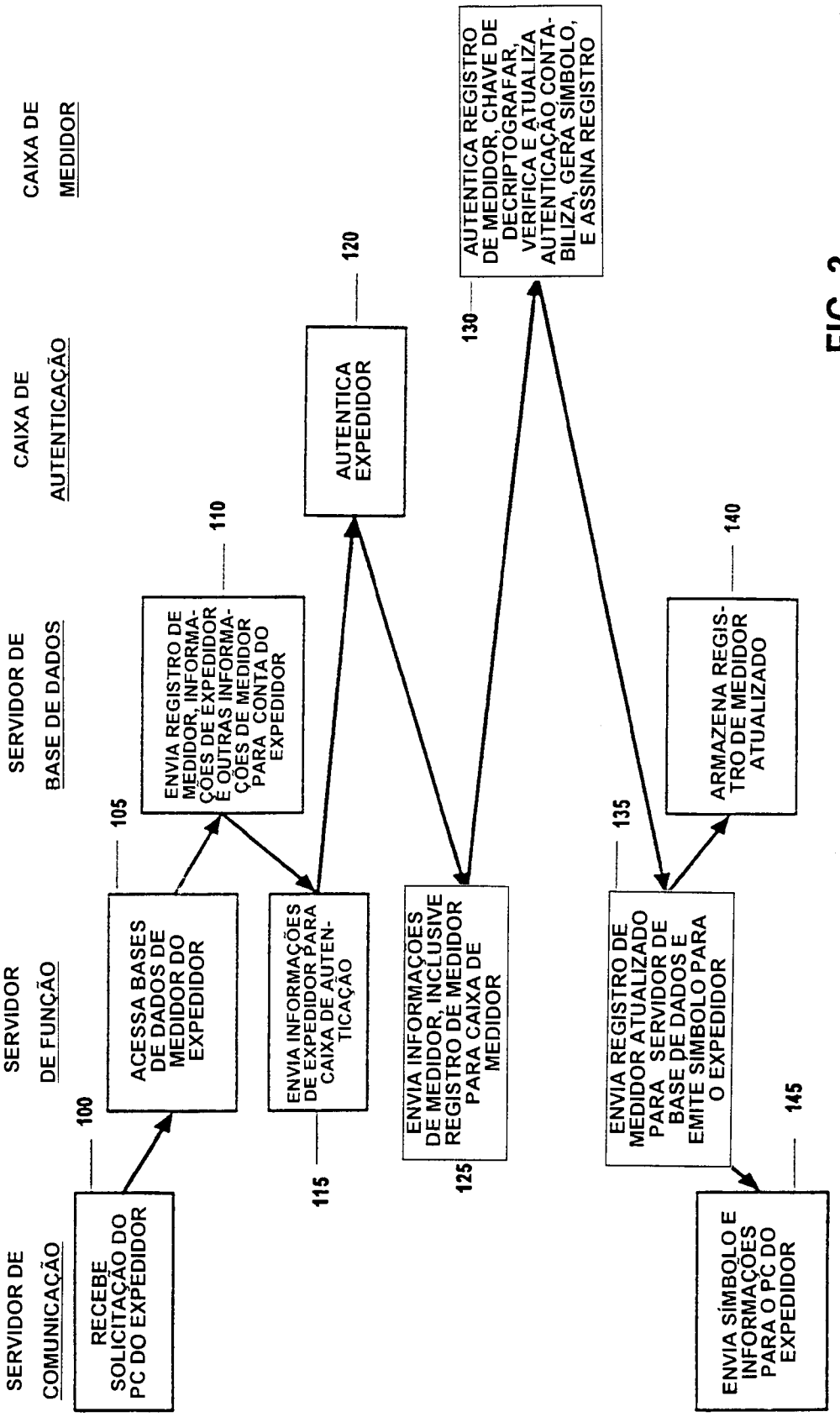
SERVIDOR DE COMUNICAÇÃO
SERVIDOR DE FUNÇÃO
SERVIDOR DE BASE DE DADOS
CAIXA DE AUTENTICAÇÃO
CAIXA DE MEDIDOR
RECEBE SOLICITAÇÃO DO PC DO EXPEDIDOR
100
ACESSA BASES DE DADOS DE MEDIDOR DO EXPEDIDOR
105
ENVIA REGISTRO DE MEDIDOR, INFORMAÇÕES DE EXPEDIDOR E OUTRAS INFORMAÇÕES DE MEDIDOR PARA CONTA DO EXPEDIDOR
110
ENVIA INFORMAÇÕES DE EXPEDIDOR PARA CAIXA DE AUTENTICAÇÃO
115
AUTENTICA EXPEDIDOR
120
ENVIA INFORMAÇÕES DE MEDIDOR, INCLUSIVE REGISTRO DE MEDIDOR PARA CAIXA DE MEDIDOR
125
AUTENTICA REGISTRO DE MEDIDOR, CHAVE DE DECRIPTOGRAFAR, VERIFICA E ATUALIZA AUTENTICAÇÃO CONTABILIZA, GERA SÍMBOLO, E ASSINA REGISTRO
130
ENVIA REGISTRO DE MEDIDOR ATUALIZADO PARA SERVIDOR DE BASE DE DADOS E EMITE SÍMBOLO PARA O EXPEDIDOR
135
ARMAZENA REGISTRO DE MEDIDOR ATUALIZADO
140
ENVIA SÍMBOLO E INFORMAÇÕES PARA O PC DO EXPEDIDOR
145

FIG. 3

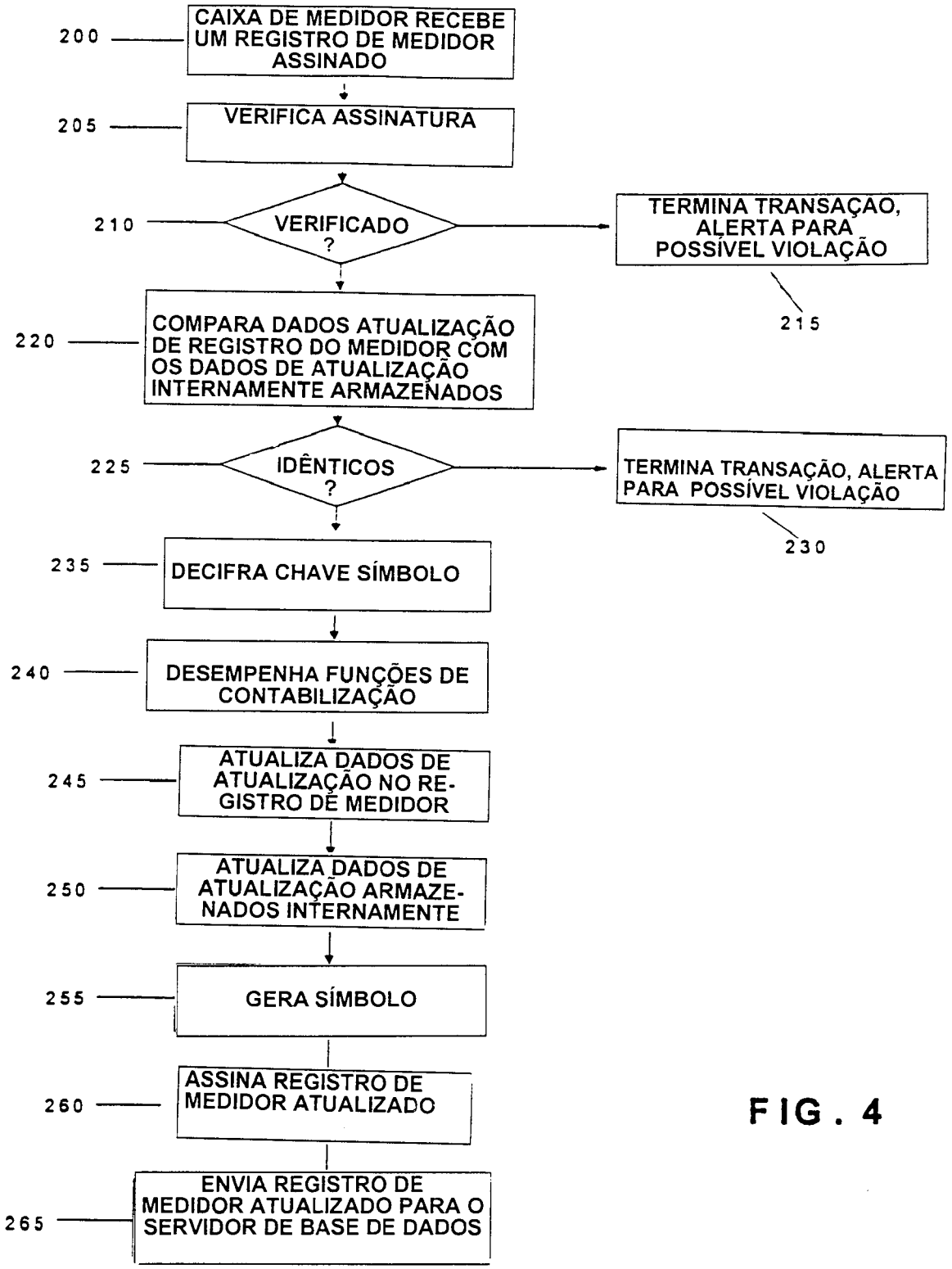
200
CAIXA DE MEDIDOR RECEBE UM REGISTRO DE MEDIDOR ASSINADO
205
VERIFICA ASSINATURA
210
VERIFICADO ?
TERMINA TRANSAÇAO, ALERTA PARA POSSÍVEL VIOLAÇÃO
215
220
COMPARA DADOS ATUALIZAÇÃO DE REGISTRO DO MEDIDOR COM OS DADOS DE ATUALIZAÇÃO INTERNAMENTE ARMAZENADOS
225
IDÊNTICOS ?
TERMINA TRANSAÇÃO, ALERTA PARA POSSÍVEL VIOLAÇÃO
230
235
DECIFRA CHAVE SÍMBOLO
240
DESEMPENHA FUNÇÕES DE CONTABILIZAÇÃO
245
ATUALIZA DADOS DE ATUALIZAÇÃO NO REGISTRO DE MEDIDOR
250
ATUALIZA DADOS DE ATUALIZAÇÃO ARMAZENADOS INTERNAMENTE
255
GERA SÍMBOLO
260
ASSINA REGISTRO DE MEDIDOR ATUALIZADO
265
ENVIA REGISTRO DE MEDIDOR ATUALIZADO PARA O SERVIDOR DE BASE DE DADOS

FIG. 4

RESUMO

"SISTEMA DE MINISTRAÇÃO DE FRANQUEAMENTO POSTAL SEGURO E PROCESSO PARA EVIDENCIAR PAGAMENTO DE FRANQUIA POSTAL".

Um sistema (10) e processo para evidenciar o pagamento de franquia postal compreendem um centro de dados (3) com uma base de dados (36) tendo uma pluralidade de registros de medidor (64) armazenados na mesma. Cada registro de medidor (64) inclui informações de medidor correspondentes a um a conta de medição alocada a cada um de uma pluralidade de dispositivos de usuário remotos (20, 22) que estão autorizados a solicitar evidencia de pagamento de franquia. Quando uma solicitação por franquia (100) é recebida no centro de dados (30), um dispositivo coprocessador seguro (44) no centro de dados (3) obtém o registro de medidor apropriado (64) e verifica a autenticidade do registro de medidor (64) verificando uma assinatura (205, 210) no registro de medidor (64) e comparar dados de atualização (220, 225) no registro de medidor (64) com dados de atualização no dispositivo seguro (44). Se verificado, o dispositivo seguro (44) então justifica um valor de franquia a ser evidenciado (130) gera evidência de pagamento de franquia (130) e atualiza as informações de medidor, inclusive os dados de atualização (130), no registro de medidor (64). O dispositivo seguro (44) então assim as informações de medidor atualizados e armazena a assinatura no registro de medidor (64, 135, 140). O dispositivo seguro (44) então retorna o registro de medidor atualizado (64) à base de dados (36, 135, 140).