



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

(11) PI 0512338-0 B1



(22) Data do Depósito: 21/06/2005

(45) Data de Concessão: 09/04/2019

(54) Título: MÉTODO PARA LIDAR COM NOTIFICAÇÃO DE RECEBIMENTO DE MENSAGEM E MEIO NÃO-TRANSITÓRIO LEGÍVEL POR COMPUTADOR

(51) Int.Cl.: H04W 4/12; H04L 12/58.

(52) CPC: H04W 4/12; H04L 51/30; H04L 51/38.

(30) Prioridade Unionista: 21/06/2004 US 60/581.644.

(73) Titular(es): BLACKBERRY LIMITED.

(72) Inventor(es): NEIL PATRICK ADAMS; HERBERT ANTHONY LITTLE; MICHAEL KENNETH BROWN; MICHAEL STEPHEN BROWN.

(86) Pedido PCT: PCT CA2005000962 de 21/06/2005

(87) Publicação PCT: WO 2005/125115 de 29/12/2005

(85) Data do Início da Fase Nacional: 21/12/2006

(57) Resumo: SISTEMA E MÉTODO PARA LIDAR COM NOTIFICAÇÃO DE RECEBIMENTO DE MENSAGEM. Sistemas e métodos para operação sobre um dispositivo móvel sem fio para lidar com notificações de mensagem. O método pode incluir receber uma mensagem pelo dispositivo móvel sem fio por uma rede de comunicação sem fio. A mensagem recebida é processada de modo que pelo menos uma parcela da mensagem do remetente é exibida para o usuário do dispositivo móvel sem fio antes de um recibo assinado ser fornecido ao remetente.

**MÉTODO PARA LIDAR COM NOTIFICAÇÃO DE RECEBIMENTO DE
MENSAGEM E MEIO NÃO-TRANSITÓRIO LEGÍVEL POR COMPUTADOR
HISTÓRICO**

CAMPO TÉCNICO

5 Este documento relaciona-se genericamente ao campo da comunicação e, em particular, a lidar com mensagens em dispositivos de comunicação sem fio.

DESCRIÇÃO DA TECNOLOGIA RELACIONADA

10 Dispositivos sem fio móveis são configurados para enviar e receber mensagens, como as mensagens de correspondência eletrônica. Tipicamente, um recibo assinado é enviado antes do usuário ter permissão para visualizar a mensagem. Adicionalmente, a mensagem poderá precisar ser verificada antes do recibo assinado ser enviado. Para
15 verificar a mensagem, tipicamente a totalidade da mensagem precisa estar presente. Isto pode ser difícil de executar em um dispositivo restrito, como um dispositivo móvel, pois poderá levar algum tempo para receber suficiente da mensagem no dispositivo para fazer a verificação. Na
20 realidade, o dispositivo poderá nunca receber a mensagem inteira, como quando a mensagem é relativamente longa ou em outras situações (por exemplo, quando a mensagem é recebida e visualizada em parcelas ou pedaços). Adicionalmente, em
25 certas situações, poderá não haver um mecanismo para receber a mensagem total até o usuário iniciar a visualizar a mensagem (por exemplo, quando o usuário tem que solicitar pedaços de mensagem adicionais enquanto visualiza uma mensagem).

SINOPSE

30 De acordo com os ensinamentos aqui revelados, sistemas

e métodos são fornecidos para fornecer notificações de recibo assinado. Um exemplo de um sistema e método inclui um dispositivo móvel que é capaz de enviar uma notificação de recibo assinado embora a mensagem inteira poderá ainda não haver sido recebida.

Como outro exemplo, um sistema e método pode incluir receber uma mensagem pelo dispositivo móvel sem fio por uma rede de comunicação sem fio, em que o remetente compôs a mensagem pretendida para recebimento por pelo menos um receptor. A mensagem recebida é processada de modo que pelo menos uma parcela da mensagem do remetente é exibida para o usuário do dispositivo móvel sem fio antes de um recibo assinado ser fornecido ao remetente.

Como outro exemplo, um sistema e método pode ser configurado para incluir instruções de processamento de notificação que podem processar a mensagem recebida pelo dispositivo móvel sem fio por uma rede de comunicação sem fio, em que o remetente compôs a mensagem pretendida para recebimento por pelo menos um receptor. Instruções de geração de recibo assinado são utilizadas para gerar um recibo assinado com base na mensagem recebida. As instruções de processamento de notificação são configuradas para processar a mensagem recebida de modo que pelo menos uma parcela da mensagem do remetente é exibida para o usuário do dispositivo móvel sem fio antes do recibo assinado gerado ser fornecido ao remetente. O recibo assinado pode ser utilizado pelo menos em parte para confirmar se o receptor específico recebeu a mensagem do remetente.

Como será apreciado, os sistemas e métodos aqui

revelados são capazes de outras e diferentes versões, e seus variados detalhes são capazes de modificações em várias relações, tudo sem desviar do espírito das técnicas aqui reveladas. Assim, os desenhos e a descrição aqui
5 expostos devem ser considerados como de natureza ilustrativa e não restritiva.

BREVE DESCRIÇÃO DOS DESENHOS

A Figura 1 é uma visão geral de um sistema de comunicação exemplar em que um dispositivo de comunicação
10 sem fio poderá ser utilizado.

A Figura 2 é um diagrama de blocos de um outro sistema de comunicação exemplar que inclui múltiplas redes e múltiplos dispositivos de comunicação móvel.

A Figura 3 é um diagrama de blocos que representa um
15 sistema para lidar com mensagens recebidas por uma rede.

A Figura 4 é um diagrama de blocos que representa um sistema para fornecer notificações de recibo assinado.

A Figura 5 é um diagrama de blocos que representa um sistema que interage com o usuário para fornecer
20 notificações de recibo assinadas.

A Figura 6 é um diagrama de blocos que representa a utilização da funcionalidade da geração do recibo assinado para gerar um recibo assinado.

A Figura 7 é uma interface do usuário que fornece um
25 ou mais indicadores a respeito de uma notificação de recibo assinada.

A Figura 8 é um fluxograma que representa um cenário operacional exemplar em que uma mensagem que é recebida pelo dispositivo móvel é processada para gerar um recibo
30 assinado.

A Figura 9 é um fluxograma que representa um cenário operacional exemplar que ilustra a interação com o usuário para fornecer notificações de recibo assinado.

A Figura 10 é um diagrama de blocos de um dispositivo móvel exemplar.

DESCRIÇÃO DETALHADA DOS DESENHOS

A Figura 1 é uma visão geral de um sistema de comunicação exemplar em que um dispositivo de comunicação sem fio poderá ser utilizado. Alguém habilitado na tecnologia apreciará que poderá haver centenas de topologias diferentes, mas o sistema mostrado na Figura 1 ajuda a demonstrar a operação dos sistemas e métodos de processamento de mensagem codificada descritos na presente aplicação. Também poderá haver muitos remetentes e receptores de mensagens. O sistema simples mostrado na Figura 1 é apenas para fins ilustrativos, e mostra talvez o ambiente de correspondência eletrônica pela Internet mais prevalente em que segurança não é geralmente utilizada.

A Figura 1 mostra um remetente de correspondência eletrônica 10, a Internet 20, um sistema servidor de mensagem 40, um portal sem fio 85, infra-estrutura sem fio 90, uma rede sem fio 105 e um dispositivo de comunicação móvel 100.

O sistema remetente de correspondência eletrônica 10, por exemplo, poderá estar conectado a um ISP (Internet Service Provider - Provedor de Serviço de Internet) em que o usuário do sistema 10 tem uma conta, localizado dentro de uma empresa, possivelmente conectado a uma rede de área local (LAN), e conectado à Internet 20, ou conectado à Internet 20 através de um grande ASP (provedor de serviço

de aplicação) como a America Online (AOL). Aqueles habilitados na tecnologia apreciarão que os sistemas mostrados na Figura 1 poderão, em vez disso, estar conectados a uma rede de área ampla (WAN) que não a Internet, embora transferências de correspondência eletrônica sejam comumente realizadas através de disposições conectadas à Internet como é mostrado na Figura 1.

O servidor de mensagem 40 poderá, por exemplo, ser implementado em um computador de rede dentro da parede de fogo de uma empresa, um computador dentro de um sistema ISP ou ASP ou assemelhado, e age como a interface principal para o intercâmbio de correspondência eletrônica pela Internet 20. Embora outros sistemas de mensagem podem não exigir um sistema servidor de mensagem 40, o dispositivo móvel 100 configurado para receber e possivelmente enviar correspondência eletrônica normalmente estará associado a uma conta em um servidor de mensagem. Talvez os dois servidores de mensagem mais comuns são Microsoft Exchange™ e Lotus Domino™. Esses produtos são muitas vezes utilizados em conjunto com roteadores de correspondência da Internet que roteiam e entregam a correspondência. Esses componentes intermediários não estão mostrados na Figura 1, pois eles não interpretam diretamente um papel no processamento de mensagem segura descrito abaixo. Servidores de mensagem como o servidor 40 tipicamente se estendem além apenas do envio e do recebimento de correspondência eletrônica; eles também motores de armazenamento de base de dados dinâmicos que possuem formatos de base de dados predefinidos para dados como

calendários, listas de afazeres, listas de tarefas, correspondência eletrônica e documentação.

O portal sem fio 85 e a infra-estrutura 90 fornecem um enlace entre a Internet 20 e a rede sem fio 105. A infra-estrutura sem fio 90 determina a rede mais provável para localizar um dado usuário e acompanha o usuário à medida que eles fazem visitas entre países ou redes. A mensagem é então entregue para o dispositivo móvel 100 através de transmissão sem fio, tipicamente a uma frequência de rádio (RF), de uma estação base na rede sem fio 105 para o dispositivo móvel 100. A rede particular 105 poderá ser virtualmente qualquer rede sem fio pela qual mensagens poderão ser intercambiadas com um dispositivo de comunicação móvel.

Como é mostrado na Figura 1, uma mensagem de correspondência eletrônica composta 15 é enviada pelo remetente de correspondência eletrônica 10, localizado em algum lugar na Internet 20. Esta mensagem 15 é normalmente inteiramente em claro e utiliza o tradicional Simple Mail Transfer Protocol (SMTP), cabeçalhos RFC822 e partes de corpo Multipurpose Internet Mail Extension (MIME) para definir o formato da mensagem de correspondência. Essas técnicas são todas bem conhecidas daqueles habilitados na tecnologia. A mensagem 15 chega no servidor de mensagem 40 e normalmente é armazenada em um armazém de mensagens. A maioria dos sistemas de mensagens conhecidos suporta um assim-chamado esquema de acesso de mensagem "pull", em que o dispositivo móvel 100 precisa solicitar que as mensagens armazenadas sejam encaminhadas pelo servidor de mensagem para o dispositivo móvel 100. Alguns sistemas fornecem o

roteamento automático dessas mensagens que são endereçadas utilizando um endereço de correspondência eletrônica específico associado ao dispositivo móvel 100. Em uma versão preferida descrita em maior detalhe abaixo, 5 mensagens endereçadas a uma conta no servidor de mensagem associado a um sistema principal como o computador residencial ou o computador de escritório que pertence ao usuário do dispositivo móvel 100 são redirecionados do servidor de mensagem 40 para o dispositivo móvel 100 na 10 medida em que são recebidas.

Independentemente do mecanismo específico que controla o encaminhamento das mensagens para o dispositivo móvel 100, a mensagem 15, ou possivelmente uma versão traduzida ou reformatada desta, é enviada para o portal sem fio 85. A 15 infra-estrutura sem fio 90 inclui uma série de conexões com a rede sem fio 105. Essas conexões poderiam ser conexões Integrated Services Digital Network (ISDN), Frame Relay ou T1, utilizando o protocolo TCP/IP utilizado por toda a Internet. Como é aqui utilizado, o termo "rede sem fio" 20 pretende incluir três tipos diferentes de rede, estes sendo (1) redes sem fio centradas em dados, (2) redes sem fio centradas na voz e (3) redes no modo dual que podem suportar tanto a comunicação de dados como de voz pelas mesmas estações base físicas. Redes no modo dual combinadas 25 incluem, sem a elas se limitar, (1) redes Code Division Multiple Access (CDMA - Acesso Múltiplo de Divisão por Código), (2) o Groupe Special Mobile ou o Global System for Mobile Communications (GSM) e as redes General Packet Radio Service (GPRS), e (3) redes futuras de terceira geração 30 (3G) como Enhanced Data-rates for Global Evolution (EDGE) e

Universal Mobile Telecommunications Systems (UMTS). Alguns exemplos mais antigos de rede centrada em dados inclui a Mobitex™ Radio Network e a DataTAC™ Radio Network. Exemplos de redes de dados centrados na voz mais antigos incluem redes Personal Communication Systems (PCS) como GSM, e sistemas TDMA.

A Figura 2 é um diagrama de blocos de um outro sistema de comunicação exemplar que inclui múltiplas redes e múltiplos dispositivos de comunicação. O sistema da Figura 2 é substancialmente similar ao sistema da Figura 1, mas inclui um sistema principal 30, um programa de redirecionamento 45, um berço de dispositivo móvel 65, um roteador de rede privada virtual sem fio (VPN) 75, uma rede sem fio adicional 110, e múltiplos dispositivos de comunicação móvel 100. Como foi descrito acima em conjunto com a Figura 1, a Figura 2 representa uma visão geral de uma topologia de rede exemplar. Embora os sistemas e métodos de processamento de mensagem codificada aqui descritos poderão ser aplicados a redes dotadas de muitas topologias diferentes, a rede da Figura 2 é útil na compreensão de um sistema de redirecionamento de correspondência automático sucintamente mencionado acima.

O sistema principal central 30 será tipicamente uma LAN de escritório central ou outra LAN, mas poderá, em vez disso, ser um computador de escritório residencial ou algum outro sistema privado em que mensagens de correspondência estão sendo intercambiadas. Dentro do sistema principal 30 há o servidor de mensagem 40, que processa em algum computador dentro da parede de fogo do sistema principal, que age como a interface principal para o sistema principal

intercambiar correspondência eletrônica com a Internet 20.
No sistema da Figura 2, o programa de redirecionamento 45
permite o redirecionamento de itens de dados do servidor 40
para o dispositivo de comunicação móvel 100. Embora o
5 programa de redirecionamento 45 seja mostrado como
residente na mesma máquina que o servidor de mensagem 40
para facilidade de apresentação, não há qualquer requisito
de que ele precise residir no servidor de mensagem. O
programa de redirecionamento 45 e o servidor de mensagem 40
10 são projetados para cooperar e interagir para permitir o
"push" (impulso) da informação para os dispositivos móveis
100. Nesta instalação, o programa de redirecionamento 45
toma informação confidencial e não confidencial empresarial
para um usuário específico e a redireciona para fora
15 através da parede de fogo empresarial até os dispositivos
móveis 100. Uma descrição mais detalhada do software de
redirecionamento 45 poderá ser encontrada na Patente dos
Estados Unidos comumente designada 6.219.694 ("a Patente
694"), intitulada "System and Method for Pushing
20 Information From a Host System To a Mobile Data
Communication Device Having a Shared Electronic Address" e
emitido para o designado da aplicação em tela em 17 de
abril de 2001, que é aqui incorporada dentro da presente
aplicação por referência. Esta técnica "push" poderá
25 utilizar uma técnica de codificação amigável para sem fio,
de compressão e de criptografia para entregar toda a
informação para um dispositivo móvel, assim eficazmente
ampliando a parede de fogo de segurança para incluir cada
dispositivo móvel 100 associado ao sistema principal 30.
30 Como é mostrado na Figura 2, poderá haver muitas vias

alternativas para fazer chegar informação até o dispositivo móvel 100. Um método para carregar informação no dispositivo móvel 100 é através de um portal designado 50, utilizando um berço para dispositivo 65. Este método tende a ser útil para atualizações de informação a granel muitas vezes efetuada na inicialização de um dispositivo móvel 100 com o sistema principal 30 ou um computador 35 dentro do sistema 30. O outro método principal para o intercâmbio de dados é pelo ar utilizando redes sem fio para entregar a informação. Como é mostrado na Figura 2, isto poderá ser efetuado através de um roteador VPN sem fio 75 ou através de uma conexão Internet tradicional 95 até um portal sem fio 85 e uma infra-estrutura sem fio 90, como foi descrito acima. O conceito de um roteador VPN sem fio 75 é novo na indústria sem fio e implica que a conexão VPN poderia ser estabelecida diretamente através de uma rede sem fio específica 110 até o dispositivo móvel 100. A possibilidade de utilizar o roteador VPN sem fio 75 apenas recentemente tornou-se disponível e poderia ser utilizada quando o novo Internet Protocol (IP Version 6 (IPV6) chegar nas redes sem fio com base em IP. Este novo protocolo fornecerá endereços IP suficientes para dedicar um endereço IP a cada dispositivo móvel 100 e assim tornar possível empurrar a informação até o dispositivo móvel 100 em qualquer ocasião. A vantagem principal de utilizar este roteador VPN sem fio 75 é que ele poderia ser um componente VPN tirado da prateleira, assim ele não exigiria a utilização de um portal sem fio separado 85 e de infra-estrutura sem fio 90. A conexão VPN preferivelmente seria uma conexão Transmission Control Protocol (TCP)/IP ou User Datagram

Protocol (UDP)/IP para entregar as mensagens diretamente ao dispositivo móvel 100. Se um VPN sem fio 75 não está disponível então um enlace 95 para a Internet 20 é o mecanismo de conexão mais comum disponível e já foi descrito acima.

No sistema de redirecionamento automático da Figura 2, uma mensagem de correspondência eletrônica composta 15 que deixa o remetente da correspondência eletrônica 10 chega no servidor de mensagem 40 e é redirecionado pelo programa de redirecionamento 45 para o dispositivo móvel 100. Na medida que este redirecionamento ocorre, a mensagem 15 é re-envelopada, conforme indicado em 80, e um algoritmo possivelmente proprietário de compressão e de criptografia pode então ser aplicado à mensagem original 15. Desta forma, mensagens que estão sendo lidas no dispositivo móvel 100 não são menos seguras do que se elas estivessem sendo lidas em uma estação de trabalho de mesa como a 35 dentro da parede de fogo. Todas as mensagens intercambiadas entre o programa de redirecionamento 45 e o dispositivo móvel 100 utilizam preferivelmente esta técnica de re-embalagem da mensagem. Outra meta deste envelope externo é manter a informação de endereçamento da mensagem original exceto o endereço do remetente e do receptor. Isto permite que mensagens de resposta alcancem o seu destino apropriado, e também permite que o campo "from" reflita o endereço de mesa do usuário móvel. Utilizar o endereço de correspondência eletrônica do usuário do dispositivo móvel 100 permite que a mensagem recebida pareça como se a mensagem originasse do sistema de mesa do usuário 35 e não do dispositivo móvel 100.

Com referência de volta à conectividade de portal 50 e de berço 65 ao dispositivo móvel 100, esta via de conexão oferece muitas vantagens para permitir o intercambio de dados de uma só vez de itens grandes. Para aqueles

5 habilitados na tecnologia de assistentes digitais pessoais (PDAs) e de sincronização, o dado mais comum intercambiado por este enlace são dados PIM (Personal Information Management - Gerenciamento de Informação Pessoal) 55. Quando intercambiado pela primeira vez esses dados tendem a

10 ser de grande quantidade, de natureza de atacado e requer uma grande largura de banda para ser carregado no dispositivo móvel 100 onde ele pode ser utilizado em viagem. Este enlace serial também poderá ser utilizado para outros fins, incluindo o estabelecimento de uma chave de

15 segurança privada 111 como uma chave privada específica S/MIME ou PGP, o Certificado (Cert) do usuário, e suas Certificate Revocation Lists (CRLs - Listas de Revogação de Certificado) 60. A chave privada é preferivelmente intercambiada de modo que o sistema de mesa e o dispositivo

20 móvel 100 partilham uma personalidade e um método para acessar toda a correspondência. O Cert e CRLs são normalmente intercambiados por esse enlace pois eles representam uma grande quantidade dos dados que são necessitados pelo dispositivo para S/MIME, PGP e outros

25 métodos de segurança com chave pública.

A Figura 3 representa um dispositivo móvel 230 (por exemplo, um dispositivo de comunicação móvel sem fio) que recebe uma ou mais mensagens 210 de um remetente 200 por uma rede 220. As mensagens 210 podem ser mensagens de

30 correio eletrônico ou outro tipo de comunicação do

remetente 200. No exemplo da Figura 3, o remetente 200 solicitou que um recibo assinado seja enviado de volta do dispositivo móvel 230.

Para lidar com o processamento da mensagem recebida 210 e o recibo assinado solicitado, o dispositivo móvel 230 inclui instruções de processamento de notificação 232. As instruções de processamento de notificação 232 processam a mensagem recebida 210 de modo que pelo menos uma parcela 240 da mensagem do remetente é exibida na interface de dispositivo 234 para o usuário 250.

A Figura 4 mostra mais especificamente que as instruções de processamento de notificação 232 permitem que uma mensagem recebida (ou a parte da mensagem que foi recebida até agora) seja exibida na interface de dispositivo 234 para o usuário 250 antes de uma notificação 260 (por exemplo, o recibo assinado) seja fornecido para o remetente. Assim, isto permite que a notificação 260 seja enviada enquanto também permite ao usuário 250 visualizar a mensagem exibida 240 no dispositivo móvel 230.

A Figura 5 ilustra que o dispositivo 230 no qual o usuário 250 está visualizando a mensagem recebida pode enviar a notificação 260 de muitas formas diferentes, como manual ou automaticamente. Por exemplo, o usuário 250 pode ser orientado através da orientação 310 a enviar um recibo assinado 300 quando o usuário 250 sair da mensagem exibida 234 independentemente de se a mensagem inteira do remetente foi enviada para o dispositivo 230. O usuário 250 pode fornecer qualquer informação necessária para lidar com a visualização e o envio do recibo assinado 300 ao fornecer entrada 320 para o dispositivo 230. O usuário 250 também

pode ser orientado também quanto a qualquer informação adicional, como a sua senha, para utilização na geração de um recibo assinado digitalmente 300.

A Figura 6 representa que a instrução de processamento de notificação 232 pode ter acesso à funcionalidade ou às instruções 350 para lidar com a geração de um recibo assinado. As instruções de geração de recibo assinado 350 podem ser configuradas tal que o processo de notificação ocorre de maneira automática. Por exemplo, se a chave privada do usuário fosse criptografada com uma senha de baixa segurança que não exigiria a solicitação ao usuário, o recibo assinado pode ser automaticamente enviado sem a intervenção do usuário.

Outras abordagens também poderão ser utilizadas, como o dispositivo 230 orientar em 310 o usuário 250 quanto a senha para descriptografar a chave privada para assinar a mensagem, em cujo ponto o usuário poderia cancelar e o recibo assinado não seria enviado. O usuário também poderá não precisar fornecer sua senha antes de sair da mensagem pois o usuário já foi mostrado a mensagem.

Uma interface pode fornecer um ou mais indicadores sobre a situação do processo de notificação da mensagem. Por exemplo, o dispositivo pode exibir um ícone que indica se a notificação foi enviada. Isto pode ser útil pois o recibo assinado poderá ou não ter sido enviado para uma mensagem particular. Um item de menu também pode ser fornecido para forçar o recibo a ser enviado antes de sair da mensagem se isso é desejado. Uma indicação também pode ser mostrada dentro de uma mensagem enviada de que o recibo assinado foi solicitado. (É observado que em uma

implementação de mesa típica, essa indicação não é necessária pois é suposto que o recibo assinado foi enviado antes do usuário visualizar a mensagem, pois o computador de mesa tem a mensagem inteira.) A Figura 7 mostra uma
5 ilustração de uma indicação 410 sendo fornecida através da interface 400 de que um recibo assinado é solicitado.

A Figura 8 representa um cenário operacional exemplar em que uma mensagem é recebida pelo dispositivo móvel na etapa 500 pela rede. A mensagem inteira ou uma parcela da
10 mensagem enviada poderá ter sido recebida pelo dispositivo móvel. Na etapa 502, a mensagem é visualizada pelo usuário. Quando a notificação pode ser gerada, a notificação é enviada para o remetente na etapa 504.

Os sistemas e métodos aqui revelados são apresentados apenas por meio de exemplo e não pretendem limitar o escopo da invenção. Outras variações dos sistemas e métodos descritos acima serão aparentes para aqueles habilitados na tecnologia e, como tal, são considerados como estando dentro do escopo da invenção. Por exemplo, a Figura 9
20 ilustra que após a mensagem ser exibida na etapa 502 para o usuário, o usuário pode optar por sair da mensagem 550, quando o usuário pode ser orientado através da orientação 554 sobre se envia o recibo assinado e/ou, se necessário, fornecer uma senha através da orientação 556. Se o usuário
25 indicou que o recibo assinado é para ser enviado e a informação necessária para gerar o recibo assinado foi fornecida, então o recibo assinado é gerado e enviado ao remetente na etapa 558. O remetente recebe a mensagem e valida que ela contém um recibo assinado para a mensagem
30 original.

Neste cenário operacional, o recibo assinado pode ser gerado de formas diferentes, como através de instruções de software (por exemplo, instruções de geração de recibo assinado 350 da Figura 6) que foram configurados para
5 assinar digitalmente o recibo para utilização na confirmação de que a mensagem foi entregue e verificada com sucesso.

Como outro exemplo do amplo escopo dos sistemas e métodos aqui revelados, um sistema e método poderia ser
10 configurado para lidar com o envio de um recibo assinado quando do recebimento da mensagem em pedaços ou partes de cada vez. Em um dispositivo de recursos restritos, o dispositivo pode solicitar o recebimento de pedaços da mensagem quando da solicitação do usuário para visualizar
15 mais da mensagem. O dispositivo pode enviar um recibo assinado quando o último pedaço da mensagem chega o que permite ao dispositivo móvel verificar a mensagem e assim enviar o recibo assinado (ou o recibo pode ser enviado conforme de outra forma aqui revelado).

20 Os sistemas e métodos poderão ser fornecidos em muitos tipos diferentes de mídia lida por computador incluindo mecanismos de armazenamento por computador (por exemplo, CD-ROM, disquete, RAM, memória flash, unidade de disco rígido do computador, etc.) que contém instruções
25 para utilização em execução por um processador para efetuar as operações dos métodos e implementar os sistemas aqui descritos. Ilustrações dos sistemas e métodos incluem, sem a eles se limitar, um dispositivo móvel capaz de enviar uma notificação de recibo assinado embora a mensagem inteira
30 poderá ainda não ter sido recebida. Como outra ilustração,

um sistema e método pode incluir receber a mensagem pelo dispositivo móvel sem fio por uma rede de comunicação sem fio, em que o remetente compôs a mensagem pretendida para recebimento por pelo menos um receptor. A mensagem recebida
5 é processada de modo que pelo menos uma parte da mensagem do remetente é exibida para o usuário do dispositivo móvel sem fio antes de um recibo assinado ser fornecido ao remetente. Como outra ilustração, um sistema e método pode ser configurado para incluir instruções de processamento de
10 notificação que podem processar a mensagem recebida pelo dispositivo móvel sem fio por uma rede de comunicação sem fio, em que o remetente compôs a mensagem dirigida para recebimento por um receptor específico. Instruções de geração de recibo assinado são utilizadas para gerar um
15 recibo assinado com base na mensagem recebida. As instruções de processamento de notificação são configuradas para processar a mensagem recebida de modo que pelo menos uma parte da mensagem do remetente é exibida ao usuário do dispositivo móvel sem fio antes do recibo assinado gerado
20 ser fornecido ao remetente. O recibo assinado pode ser utilizado pelo menos em parte para confirmar se o receptor específico recebeu a mensagem do remetente.

Como outro exemplo do amplo escopo dos sistemas e métodos aqui revelados, os sistemas e métodos poderão ser
25 utilizados com muitos computadores e dispositivos diferentes, como o dispositivo de comunicação móvel sem fio mostrado na Figura 10. Com referência à Figura 10, o dispositivo móvel 100 é um dispositivo móvel de modo dual e inclui um transceptor 611, um microprocessador 638, uma
30 tela 622, memória não volátil 624, memória de acesso

aleatório (RAM) 626, um ou mais dispositivos de entrada/saída (I/O) auxiliares 628, uma porta serial 630, um teclado 632, um alto-falante 634, um microfone 636, um subsistema de comunicação sem fio de curto alcance 640, e
5 outros subsistemas do dispositivo 642.

O transceptor 611 inclui um receptor 612, um transmissor 614, antenas 616 e 618, um ou mais osciladores locais 613, e um processador de sinal digital (DSP) 620. As antenas 616 e 618 poderão ser elementos de antena de uma
10 antena de múltiplos elementos, e são preferivelmente antenas embutidas. Contudo, os sistemas e métodos aqui descritos de modo algum são limitados a um tipo particular de antena, ou mesmo a dispositivos de comunicação sem fio.

O dispositivo móvel 100 é preferivelmente um
15 dispositivo de comunicação bilateral dotado de capacidade de comunicação de voz e de dados. Assim, por exemplo, o dispositivo móvel 100 poderá comunicar por uma rede de voz, como qualquer uma das redes celulares analógica ou digital, e também poderá comunicar por uma rede de dados. As redes
20 de voz e de dados são representadas na Figura 10 pela torre de comunicação 619. Essas redes de voz e de dados poderão ser redes de comunicação separadas que utilizam infraestrutura separada, como estações base, controladoras de rede, etc., ou elas poderão ser integradas dentro de uma
25 única rede sem fio.

O transceptor 611 é utilizado para comunicar com a rede 619, e inclui o receptor 612, o transmissor 614, o um ou mais osciladores locais 613 e o DSP 620. O DSP 620 é utilizado para enviar e receber sinais de e para os
30 transceptores 616 e 618, e também fornece informação de

controle para o receptor 612 e o transmissor 614. Se a comunicação de voz e de dados ocorrem em uma única frequência, ou conjuntos intimamente espaçados de frequências, então um único oscilador local 613 poderá ser
5 utilizado em conjunto com o receptor 612 e o transmissor 614. Alternativamente, se frequências diferentes são utilizadas para a comunicação por voz verso a comunicação por dados, por exemplo, então uma pluralidade de osciladores locais 613 podem ser utilizados para gerar uma
10 pluralidade de frequências correspondentes às redes de voz e de dados 619. A informação, que inclui tanto a informação de voz como a de dados, é comunicada de e para o transceptor 611 através de um enlace entre o DSP 620 e o microprocessador 638.

15 O projeto detalhado do transceptor 611, como a banda de frequência, seleção de componentes, nível de energia, etc., será dependente da rede de comunicação 619 em que o dispositivo móvel 100 pretende operar. Por exemplo, o dispositivo móvel 100 que pretende operar no mercado da
20 América do Norte poderá incluir um transceptor 611 projetado para operar com qualquer uma de uma variedade de redes de comunicação de voz, como as redes de comunicação de dados Mobitex ou DataTAC, AMPS, TDMA, CDMA, PCS, etc., enquanto o dispositivo móvel 100 que pretende ser utilizado
25 na Europa poderá ser configurado para operar com a rede de comunicação de dados GPRS e a rede de comunicação de voz GSM. Outros tipos de redes de dados e de voz, tanto separadas como integradas, também poderão ser utilizadas com o dispositivo móvel 100.

30 Dependendo do tipo de rede ou de redes 619, os

requisitos de acesso para o dispositivo móvel 100 também poderão variar. Por exemplo, nas redes de dados Mobitex e DataTAC, os dispositivos móveis são registrados na rede utilizando um número de identificação singular associado a cada dispositivo móvel. Contudo, nas redes de dados GPRS, o acesso à rede é associado a um assinante ou usuário do dispositivo móvel. O dispositivo GPRS tipicamente requer um módulo de identidade do assinante ("SIM"), que é obrigatório para operar o dispositivo móvel em uma rede GPRS. Funções de comunicação locais ou não de rede (se houver) poderão ser operadas sem o dispositivo SIM, mas o dispositivo móvel ser incapaz de realizar quaisquer funções que envolvam a comunicação pela rede de dados 619, exceto as operações legalmente obrigatórias, como a chamada de emergência '911'.

Após qualquer procedimento de registro ou de ativação da rede necessário ter sido completado, o dispositivo móvel 100 poderá então enviar e receber sinais de comunicação, incluindo sinais tanto de voz como de dados, pelas redes 619. Os sinais recebidos pela antena 616 da rede de comunicação 619 são roteados para o receptor 612, que fornece amplificação de sinal, conversão descendente da frequência, filtragem, seleção de canal, etc., e também poderá fornecer conversão analógico para digital. A conversão analógico para digital do sinal recebido permite que funções de comunicação mais complexas, como a demodulação digital e a decodificação, sejam efetuadas utilizando o DSP 620. De maneira similar, os sinais a serem transmitidos para a rede 619 são processados, incluindo a modulação e codificação, por

exemplo, pelo DSP 620 e são então fornecidas ao transmissor 614 para a conversão digital a analógica, conversão ascendente da frequência, filtragem, amplificação e transmissão para a rede de comunicação 610 através da
5 antena 618.

Além de processar os sinais de comunicação, o DSP 620 também fornece controle do transceptor. Por exemplo, os níveis de ganho aplicado aos sinais de comunicação no receptor 612 e no transmissor 614 poderão ser
10 adaptativamente controlados através de algoritmos de controle de ganho automáticos implementados no DSP 620. Outros algoritmos de controle do transceptor também poderiam ser implementados no DSP 620 para fornecer o controle mais sofisticado do transceptor 611.

15 O microprocessador 638 preferivelmente gerencia e controla a operação geral do dispositivo móvel 100. Muitos tipos de microprocessadores ou de microcontroladoras poderiam ser aqui utilizadas ou, alternativamente, um único DSP 620 poderia ser utilizado para efetuar as funções do
20 microprocessador 638. Funções de comunicação de baixo nível, incluindo pelo menos as comunicações de dados e de voz, são efetuadas através do DSP 620 no transceptor 611. Outras aplicações de comunicação de alto nível, como a aplicação de comunicação de voz 624A, e uma aplicação de
25 comunicação de dados 624B poderão ser armazenadas na memória não volátil 624 para execução pelo microprocessador 638. Por exemplo, o módulo de comunicação de voz 624A poderá fornecer uma interface de usuário de alto nível operada para transmitir e receber chamadas de voz entre o
30 dispositivo móvel 100 e uma pluralidade de outros

dispositivos de voz ou de modo dual através da rede 619. De modo similar, o módulo de comunicação de dados 624B poderá fornecer uma interface de usuário de alto nível operada para enviar e receber dados, como as mensagens de correspondência eletrônica, arquivos, informação do organizador, mensagens de texto curto, etc., entre o dispositivo móvel 100 e uma pluralidade de outros dispositivos de dados através das redes 619.

O microprocessador 638 também interage com outros subsistemas de dispositivos, como a tela 622, a RAM 626, os subsistemas de entrada/saída (I/O) auxiliares 628, a porta serial 630, o teclado 632, o alto-falante 634, o microfone 636, o subsistema de comunicação de curto alcance 640 e qualquer outro subsistema de dispositivo geralmente designado como 642.

Alguns dos subsistemas mostrados na Figura 10 efetuam funções relacionadas com a comunicação, enquanto outros subsistemas poderão fornecer funções "residentes" ou no dispositivo. Notadamente, alguns subsistemas, como o teclado 632 e a tela 622 poderão ser utilizados tanto para funções relacionadas com a comunicação, como entrar com mensagem de texto para transmissão por uma rede de comunicação de dados, como funções residentes no dispositivo como a calculadora ou lista de tarefas ou outras funções do tipo PDA.

O software do sistema operacional utilizado pelo microprocessador 648 é preferivelmente armazenado em um armazém persistente como a memória não volátil 624. A memória não volátil 624 poderá, por exemplo, ser implementada como um componente de memória Flash, ou uma

RAM suportada por bateria. Além do sistema operacional, que controla funções de baixo nível do dispositivo móvel 610, a memória não volátil 624 inclui uma pluralidade de módulos de software 624A-624N que podem ser executados pelo

5 microprocessador 638 (e/ou o DSP 620), incluindo um módulo de comunicação de voz 624A, um módulo de comunicação de dados 624B, e uma pluralidade de outros módulos operacionais 624N para efetuar uma pluralidade de outras

10 funções. Estes módulos são executados pelo microprocessador 638 e fornecem uma interface de alto nível entre o usuário e o dispositivo móvel 100. Este interface tipicamente inclui um componente gráfico fornecido através da tela 622, e um componente de entrada/saída fornecido através do I/O auxiliar 628, teclado 632, alto-falante 634, e microfone

15 636. O sistema operacional, aplicações ou módulos específicos do dispositivo, ou partes destes, poderão ser temporariamente carregados dentro de um armazém volátil, como a RAM 626 para operação mais rápida. Ademais, os sinais de comunicação recebidos também poderão ser

20 temporariamente armazenados em RAM 626, antes de gravá-los permanentemente em um sistema de arquivos localizados em um armazém persistente como a memória Flash 624.

Um módulo de aplicação exemplar 624N que poderá ser carregado no dispositivo móvel 100 é uma aplicação de

25 gerente de informação pessoal (PIM) que fornece funcionalidade de PDA, como eventos de calendário, compromissos, e itens de tarefas. Este módulo 624N também poderá interagir com o módulo de comunicação de voz 624A para gerenciar chamadas telefônicas, correspondência por

30 voz, etc., e também poderá interagir com o módulo de

comunicação de dados para gerenciar comunicações de correspondência eletrônica e outras transmissões de dados. Alternativamente, toda a funcionalidade do módulo de comunicação de voz 624A e do módulo de comunicação de dados 5 624B poderá ser integrada dentro do módulo PIM.

A memória não volátil 624 preferivelmente também fornece um sistema de arquivos para facilitar o armazenamento de itens de dados PIM no dispositivo. A aplicação PIM preferivelmente inclui a capacidade de enviar 10 e receber itens de dados, quer por ela própria, ou em conjunto com os módulos de comunicação de voz e de dados 624A e 624B, através das redes sem fio 619. Os itens de dados PIM são preferivelmente integrados com precisão, sincronizados e atualizados, através das redes sem fio 619, 15 com um conjunto correspondente de itens de dados armazenados ou associados a um sistema de computador principal, assim criando um sistema espelhado para os itens de dados associados a um usuário particular.

Objetos de contexto que representam pelo menos itens 20 de dados parcialmente decodificados, bem como itens de dados inteiramente decodificados, são preferivelmente armazenados no dispositivo móvel 100 em um armazém volátil e não persistente como a RAM 626. Essa informação poderá, em vez disso, ser armazenada na memória não volátil 624, 25 por exemplo, quando os intervalos de armazenamento são relativamente curtos, tal que a informação é removida da memória logo após ela ser armazenada. Contudo, armazenamento desta informação na RAM 626 ou em outro armazém volátil e não persistente é preferido, para 30 assegurar que a informação seja apagada da memória quando o

dispositivo móvel 100 perder energia. Isto impede, por exemplo, que uma parte não autorizada obtenha qualquer informação armazenada decodificada ou parcialmente decodificada ao remover um chip de memória do dispositivo móvel 100.

O dispositivo móvel 100 poderá ser manualmente sincronizado com o sistema principal ao colocar o dispositivo 100 em um berço de interface, que acopla a porta serial 630 do dispositivo móvel 100 à porta serial do sistema de computador ou do dispositivo. A porta serial 630 também poderá ser utilizada para permitir que o usuário estabeleça preferências através de um dispositivo externo ou de aplicação de software, ou baixar outros módulos de aplicação 624N para instalação. Este via de baixa por fiação poderá ser utilizada para carregar uma chave de criptografia no dispositivo, que é um método mais seguro do que intercambiar informação de criptografia através da rede sem fio 619. Interfaces para outras vias de baixa por fiação poderão ser fornecidas no dispositivo móvel 100, além ou em vez da porta serial 630. Por exemplo, uma porta USB poderia fornecer uma interface para um computador pessoal equipado de modo similar.

Módulos de aplicação adicionais 624N poderão ser carregados no dispositivo móvel 100 através da rede 610, através de um subsistema de I/O auxiliar 628, através da porta serial 630, através do subsistema de comunicação de curto alcance 640, ou através de qualquer outro subsistema adequado 642, e instalado pelo usuário na memória não volátil 624 ou na RAM 626. Essa flexibilidade na instalação da aplicação aumenta a funcionalidade do dispositivo móvel

100 e poderá fornecer funções aprimoradas no dispositivo, funções relacionadas com a comunicação, ou as duas. Por exemplo, aplicações de comunicação seguras poderão permitir que sejam efetuadas funções de comércio eletrônico e outras
5 transações financeiras dessas utilizando o dispositivo móvel 100.

Quando o dispositivo móvel 100 está operando no modo de comunicação de dados, um sinal recebido, como uma mensagem de texto ou uma baixa de página da web, é
10 processada pelo módulo transceptor 611 e fornecida para o microprocessador 538, que preferivelmente ainda processa o sinal recebido em múltiplos estágios conforme descrito acima, para a eventual saída para a tela 622, ou alternativamente para um dispositivo de I/O auxiliar 628. O
15 usuário do dispositivo móvel 100 também poderá compor itens de dados, como mensagens de correspondência eletrônica, utilizando o teclado 632, que é preferivelmente um teclado alfanumérico completo disposto no estilo QWERTY, embora outros estilos de teclados alfanuméricos completos como o
20 estilo DVORAK conhecido também poderão ser utilizados. A entrada do usuário para o dispositivo móvel 100 é ainda aprimorada com uma pluralidade de dispositivos de I/O auxiliares 628, que poderão incluir um dispositivo de entrada por esfera acionada por polegar, uma almofada de
25 toque, uma variedade de comutadores, um comutador de entrada rocker, etc. Os itens de dados compostos entrados pelo usuário poderão então ser transmitidos pelas redes de comunicação 619 através do módulo transceptor 611.

Quando o dispositivo móvel 100 está operando no modo
30 de comunicação de voz, a operação geral do dispositivo

móvel é substancialmente similar a do modo de dados, exceto que os sinais recebidos são preferivelmente emitidos para o alto-falante 634 e os sinais de voz para transmissão são gerados por um microfone 636. Subsistemas de I/O de voz ou
5 de áudio alternativos como o subsistema de gravação de mensagem de voz, também poderão ser implementados no dispositivo móvel 100. Embora a saída de sinal de voz ou de áudio é preferivelmente efetuada essencialmente através do alto-falante 634, a tela 622 também poderá ser utilizada
10 para fornecer uma indicação da identidade da parte que chama, a duração da chamada de voz, ou outra informação relacionada a uma chamada de voz. Por exemplo, o microprocessador 639, em conjunto com o módulo de comunicação de voz e o software do sistema operacional,
15 poderá detectar a informação de identificação de quem chama de uma chamada de voz de entrada e exibi-la na tela 622.

Um subsistema de comunicação de curto alcance 640 também é incluído no dispositivo móvel 100. O subsistema 640 poderá incluir um dispositivo infravermelho e circuitos
20 e componentes associados, ou um módulo de comunicação RF de curto alcance como o módulo Bluetooth™ ou um módulo 802.11, por exemplo, para fornecer comunicação com sistemas e dispositivos ativados de modo similar. Aqueles habilitados na tecnologia apreciarão que "Bluetooth" e
25 "802.11" referem-se a conjuntos de especificações, disponíveis do Institute of Electrical and Electronics Engineers, relacionados a redes de área pessoal sem fio e redes de área local sem fio, respectivamente.

É ainda observado que os sistemas e métodos poderão
30 ser implementados em vários tipos de arquiteturas de

computador e os sinais de dados de/para um dispositivo poderão ser transportados através de meio de fibra óptica, ondas portadoras, redes sem fio, etc. para comunicação entre múltiplos dispositivos. Os dados dos sistemas e métodos poderão ser armazenados em um ou mais armazéns de dados. Os armazéns de dados podem ser de muitos tipos diferentes de dispositivos de armazenamento e constructos de programação, como RAM, ROM, memória Flash, estruturas de dados de programação, variáveis de programação, etc. É observado que as estruturas de dados descrevem formatos para utilização na organização e no armazenamento de dados em bases de dados, em programas, na memória, ou em outra mídia lida por computador para utilização por um programa de computador.

Os componentes do computador, os módulos de software, funções e estruturas de dados aqui descritos poderão ser conectados direta ou indiretamente um ao outro para permitir o fluxo dos dados necessários para sua operação. Também é observado que um módulo ou processador inclui, mas não é a eles limitado, a uma unidade de código que efetua uma operação de software, e pode ser implementado, por exemplo, como um unidade de subrotina de código, ou uma unidade de função de software de código, ou como um objeto (como em um paradigma orientado ao objeto), ou um applet, ou em uma linguagem de script de computador, ou como outro tipo de código de computador, como Java.

REIVINDICAÇÕES

1. Método para operação sobre um dispositivo móvel sem fio para lidar com uma notificação de mensagem para uma mensagem, caracterizado por compreender:

5 receber uma parte da mensagem pelo dispositivo móvel sem fio através de uma rede de comunicação sem fio;

 em que a mensagem é enviada a partir de um remetente e é pretendida a ser recebida por pelo menos um receptor;

 processar a parte de mensagem recebida de modo que
10 pelo menos a parte da mensagem do remetente é exibida para um usuário do dispositivo móvel sem fio antes de um recibo assinado ser fornecido para o remetente;

 em que o recibo assinado é utilizado pelo menos em parte para confirmar se o receptor pretendido havia
15 recebido a mensagem do remetente;

 em que a parte recebida da mensagem do remetente é exibida para o usuário, embora a mensagem inteira não tenha sido recebida pelo dispositivo móvel sem fio;

 em que a notificação de recibo assinado é fornecida ao
20 remetente, embora a mensagem inteira não tenha sido recebida pelo dispositivo móvel sem fio.

2. Método, de acordo com a reivindicação 1, caracterizado pelo fato do recibo assinado fornecer uma indicação para o remetente de que a mensagem foi verificada
25 pelo receptor pretendido da mensagem.

3. Método, de acordo com a reivindicação 1, caracterizado pelo fato da geração do recibo assinado incluir verificar a mensagem;

 em que após a mensagem ser verificada, o recibo
30 assinado é fornecido ao remetente.

4. Método, de acordo com a reivindicação 3, caracterizado pelo fato de pelo menos uma parte substancial da mensagem inteira ser necessária antes da mensagem poder ser verificada.

5 5. Método, de acordo com a reivindicação 4, caracterizado pelo fato do dispositivo ser um dispositivo restrito.

6. Método, de acordo com a reivindicação 5, caracterizado pelo fato da mensagem ser fornecida para o
10 dispositivo móvel sem fio em partes.

7. Método, de acordo com a reivindicação 6, caracterizado pelo fato do usuário do dispositivo móvel sem fio fornecer uma solicitação para uma parte adicional da mensagem a ser fornecida ao dispositivo móvel sem fio.

15 8. Método, de acordo com a reivindicação 7, caracterizado pelo fato do usuário fornecer a solicitação enquanto visualiza pelo menos uma parte da mensagem.

9. Método, de acordo com a reivindicação 1, caracterizado pelo fato do recibo assinado ser assinado
20 digitalmente pelo receptor através da utilização de uma chave privada do receptor.

10. Método, de acordo com a reivindicação 1, caracterizado pelo fato da mensagem ser uma mensagem de correio eletrônico.

25 11. Método, de acordo com a reivindicação 1, caracterizado pelo fato de, sem o referido processamento da mensagem recebida, o recibo assinado dever ser enviado antes da mensagem ser exibida.

12. Método, de acordo com a reivindicação 1,
30 caracterizado pelo fato do usuário ser orientado a enviar o

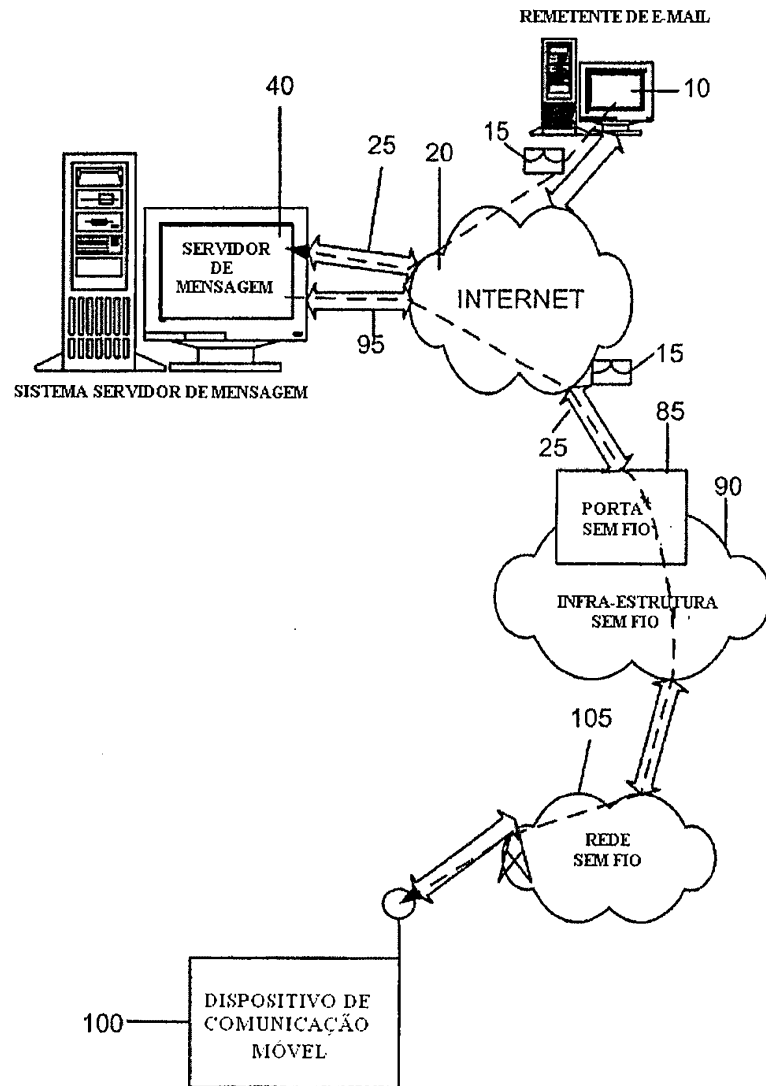
recibo assinado quando o usuário sair da mensagem exibida independentemente se a mensagem inteira do remetente foi enviada para o dispositivo; em que a senha do usuário é solicitada ao usuário para utilização na geração de um
5 recibo digitalmente assinado.

13. Método, de acordo com a reivindicação 1, caracterizado pelo fato de indicadores de interface serem fornecidos para indicar a situação com relação a um recibo assinado.

10 14. Método, de acordo com a reivindicação 1, caracterizado pelo fato do dispositivo móvel sem fio ser um dispositivo de comunicação móvel sem fio.

15 15. Método, de acordo com a reivindicação 1, caracterizado pelo fato do dispositivo móvel sem fio ser um assistente digital pessoal (PDA).

16. Meio não-transitório legível por computador caracterizado por ter nele gravadas instruções para executar o método conforme definido na reivindicação 1.

**FIG. 1**

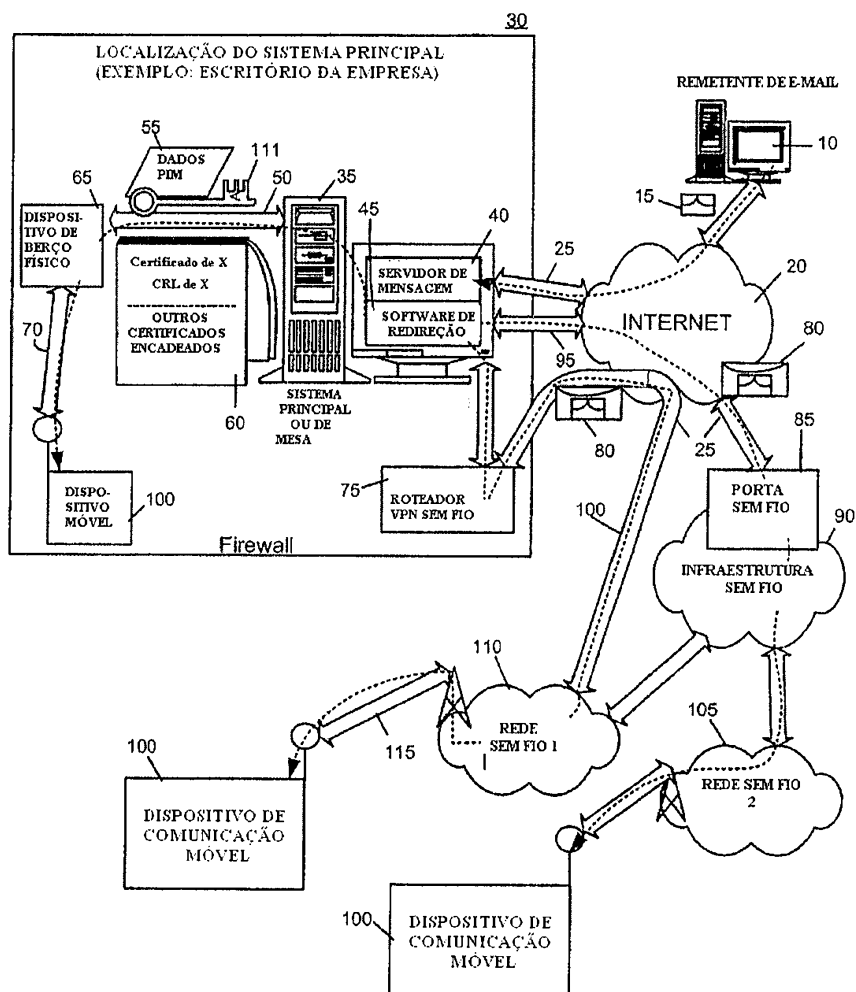
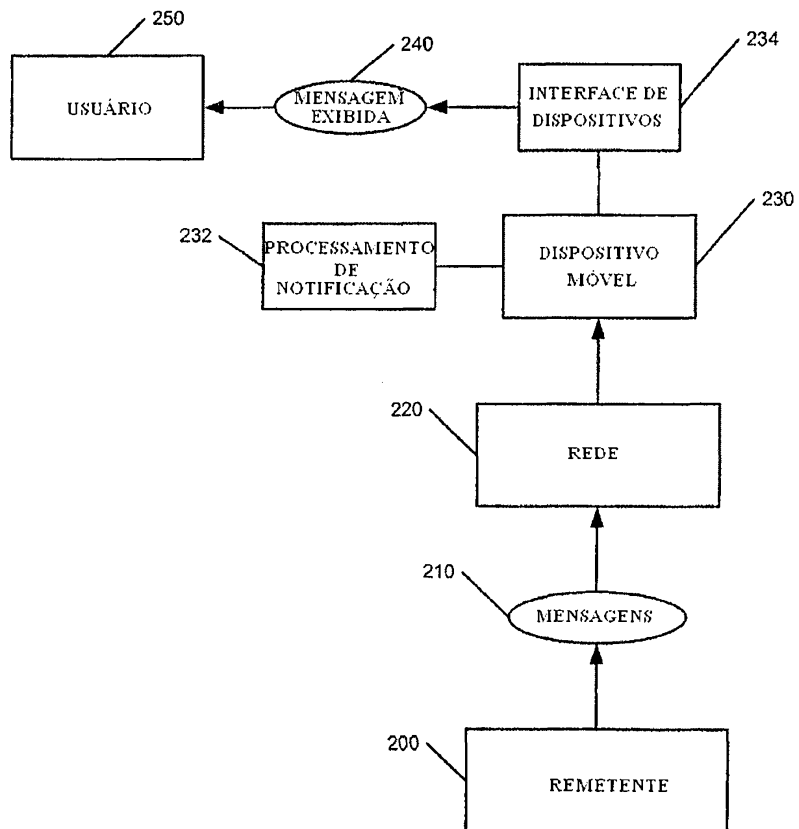
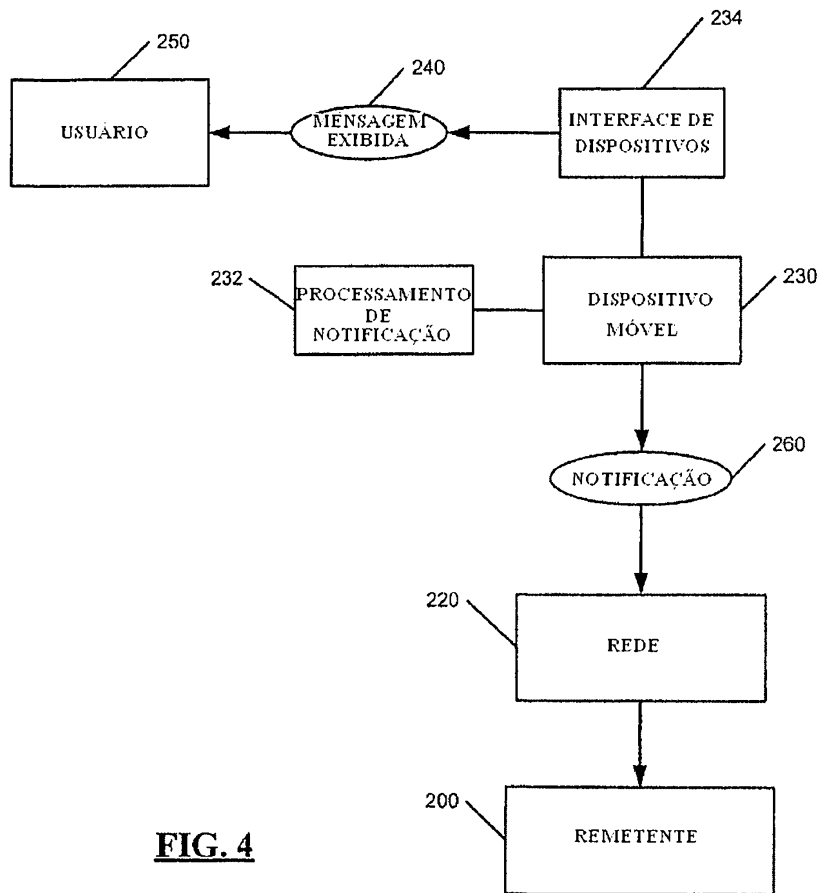
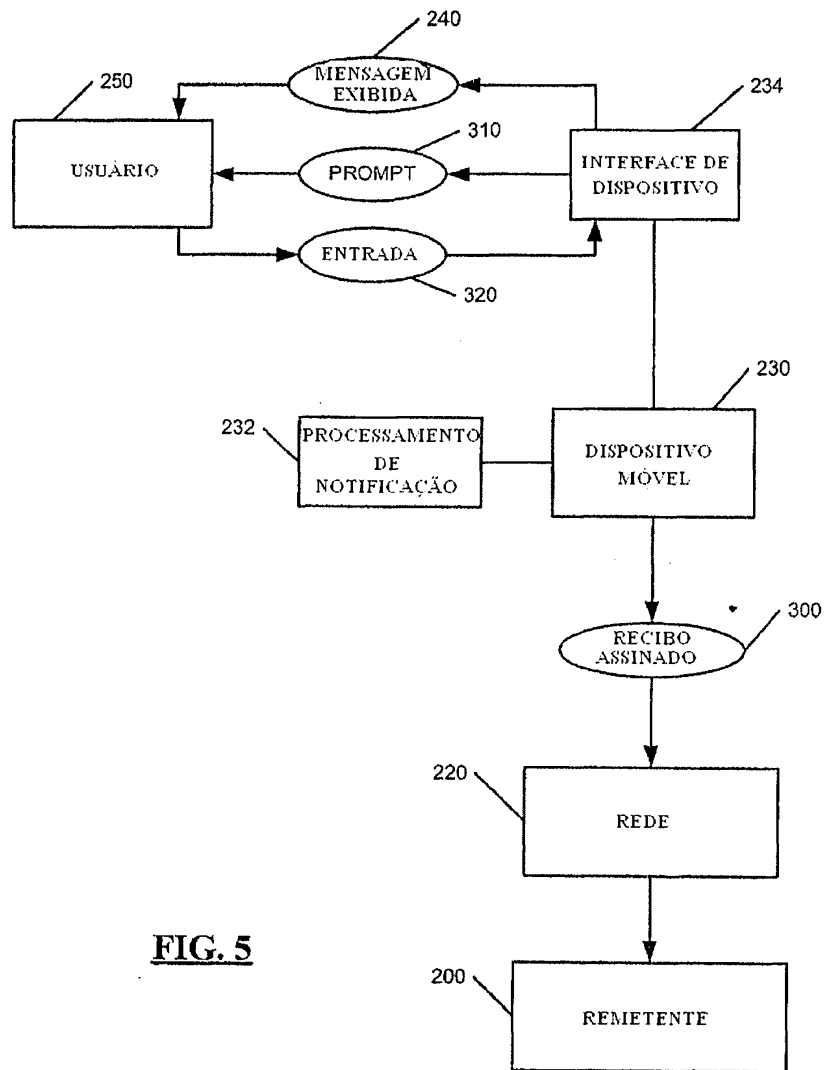
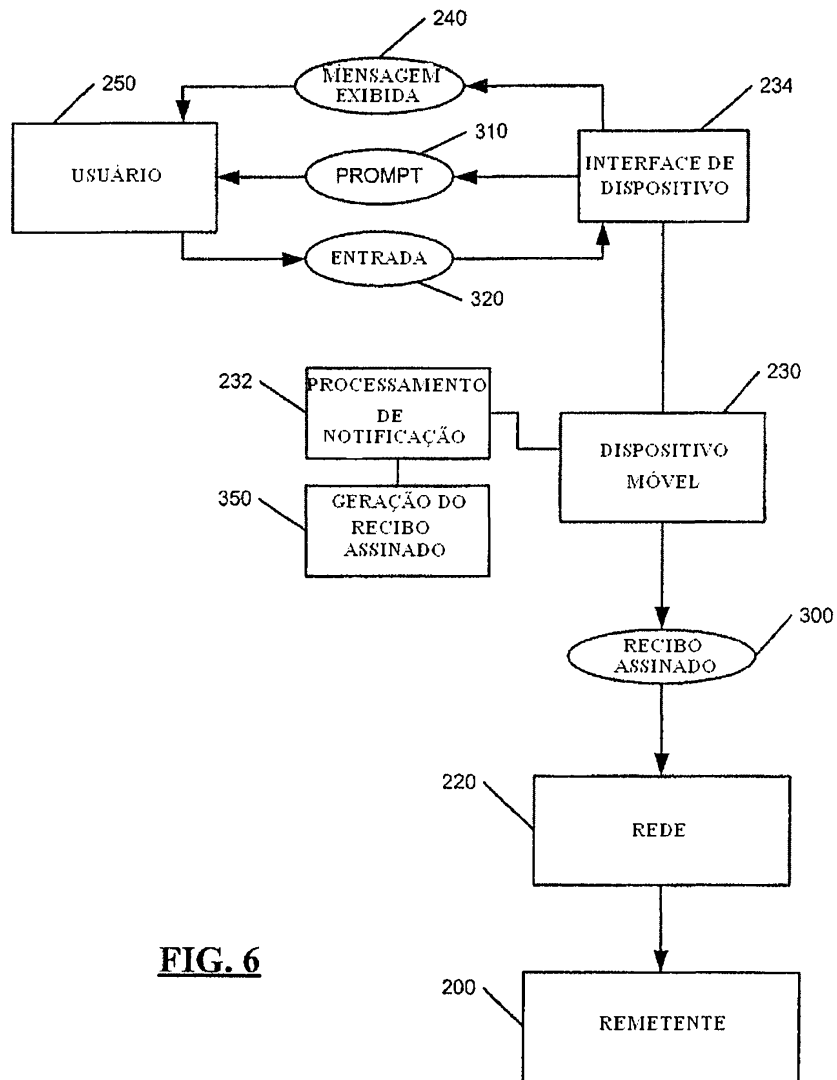


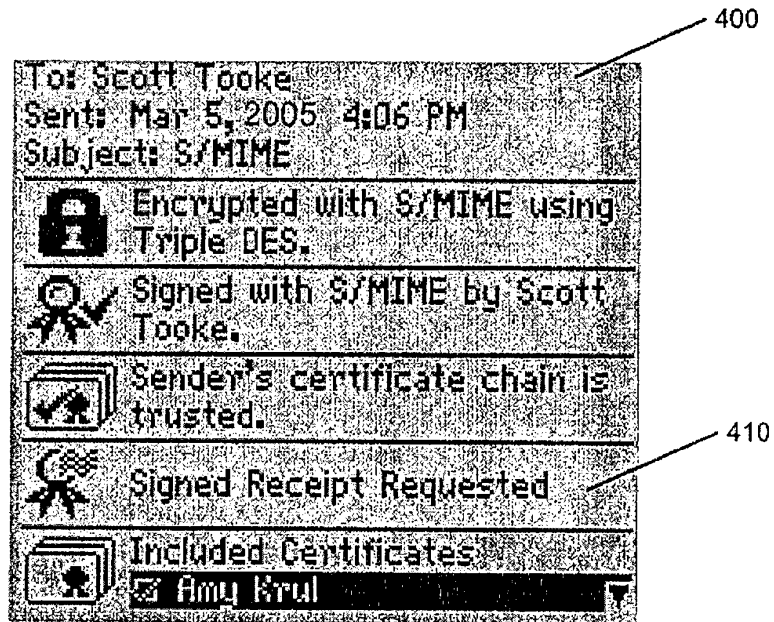
FIG. 2

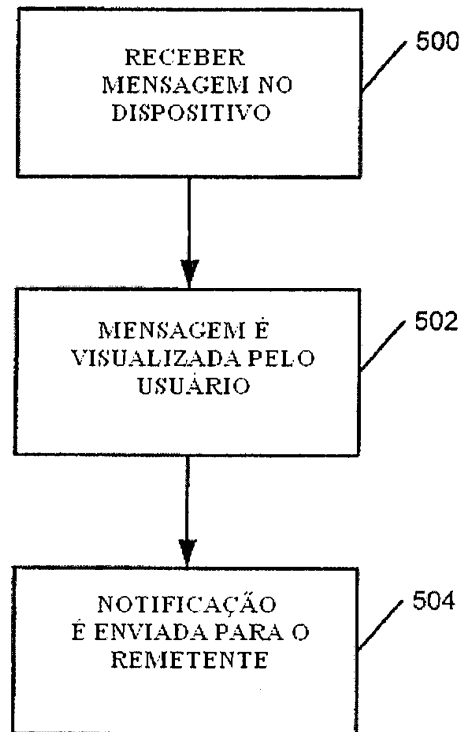
**FIG. 3**

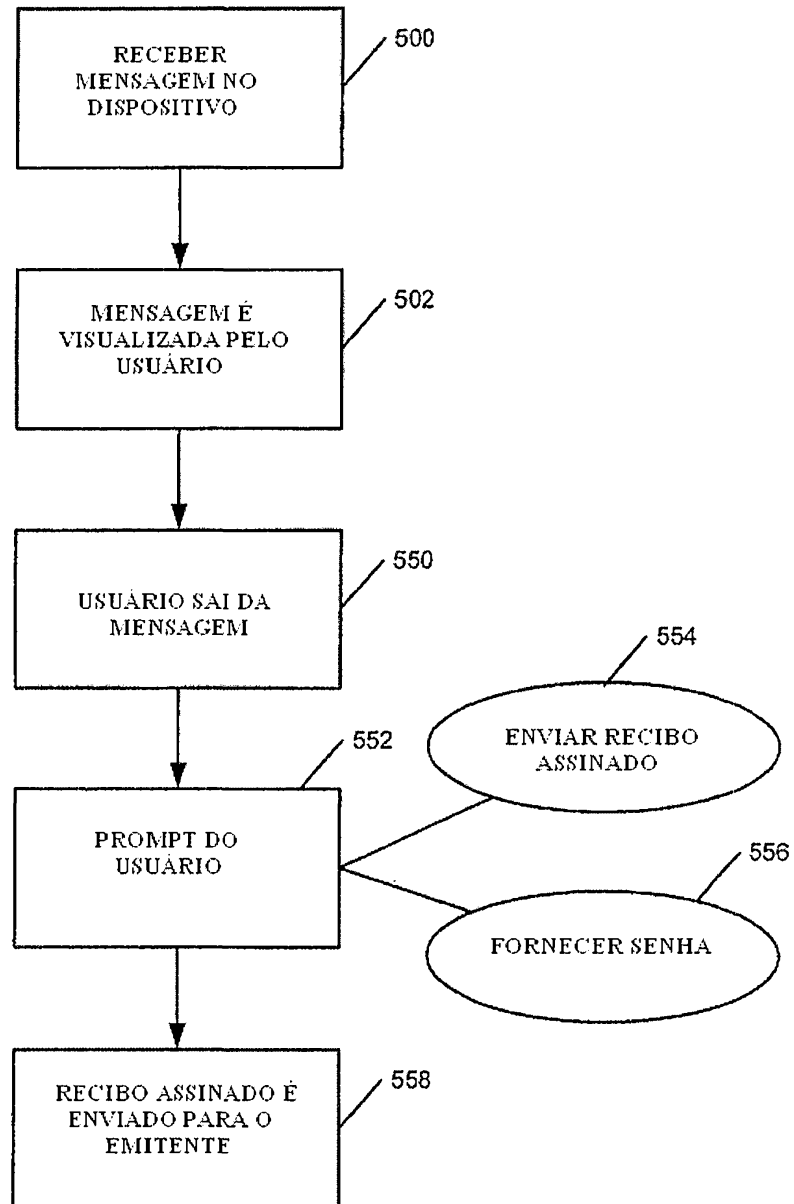
**FIG. 4**

**FIG. 5**

**FIG. 6**

**FIG. 7**

**FIG. 8**

**FIG. 9**

72

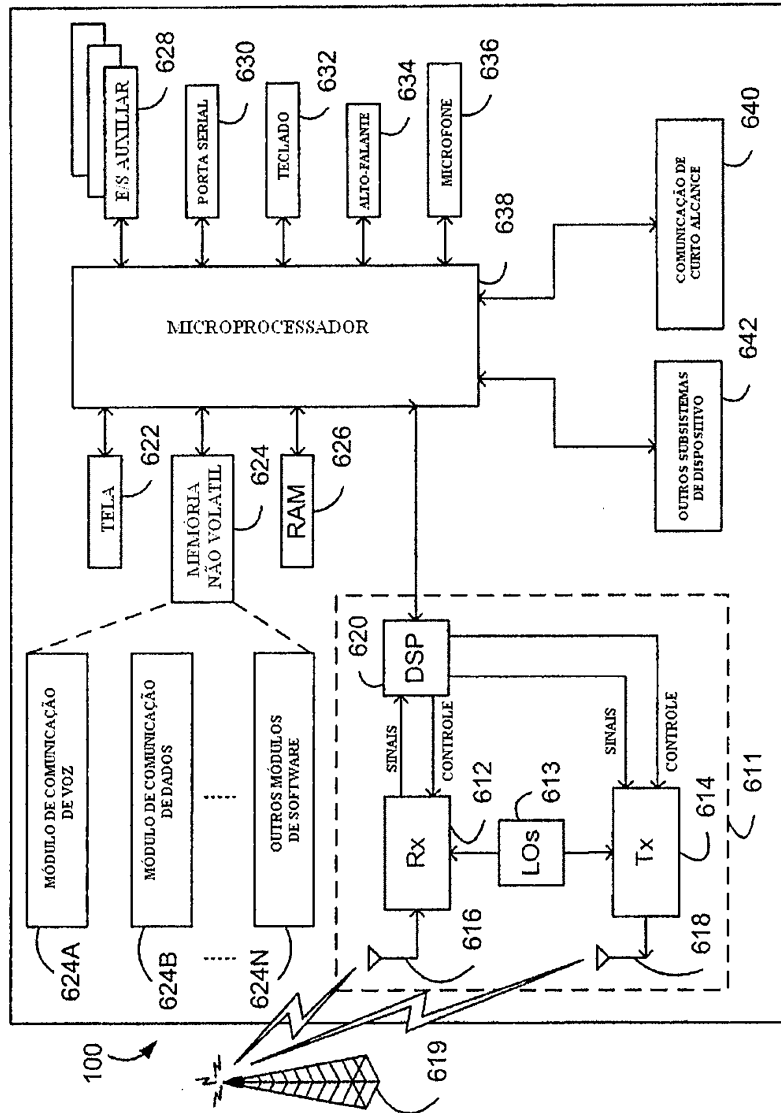


FIG. 10