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

**(11) PI 0708184-7 B1**

**(22) Data do Depósito:** 22/02/2007

**(45) Data de Concessão:** 15/10/2019

**(54) Título:** TOKEN, TERMINAL PARA PERMITIR O USO DE UM TOKEN SEM FIO PARA AUTENTICAÇÃO, E MÉTODO DE UTILIZAÇÃO DE UM TOKEN SEM FIO

**(51) Int.Cl.:** H04L 9/32; G06F 21/35; G07C 9/00.

**(52) CPC:** H04L 9/3234; G06F 21/35; G07C 9/00111.

**(30) Prioridade Unionista:** 22/02/2006 US 11/360,377.

**(73) Titular(es):** DIGITALPERSONA, INC..

**(72) Inventor(es):** VANCE C. BJORN.

**(86) Pedido PCT:** PCT US2007004812 de 22/02/2007

**(87) Publicação PCT:** WO 2007/100709 de 07/09/2007

**(85) Data do Início da Fase Nacional:** 22/08/2008

**(57) Resumo:** MÉTODO E APARELHO PARA UM TOKEN. A presente invenção refere-se a um método e aparelho de utilização de um token que compreende receber uma indicação de presença de um terminal próximo de curto alcance e ativar o token em resposta à recepção da indicação, O método ainda compreende a realização de autenticação entre o token e o terminal, sem requerer um usuário para interagir com o token.

Relatório Descritivo da Patente de Invenção para **"TOKEN, TERMINAL PARA PERMITIR O USO DE UM TOKEN SEM FIO PARA AUTENTICAÇÃO, E MÉTODO DE UTILIZAÇÃO DE UM TOKEN SEM FIO".**

## CAMPO DA INVENÇÃO

[001] A presente invenção refere-se a dispositivos de autenticação, e mais especificamente, a um token para identificação.

## ANTECEDENTES

[002] A necessidade de se identificar para acessar serviços é grande. É fácil pensar em vários exemplos encontrados diariamente – conexão com PC, sites da Internet, check-in de aeroporto, compras com cartão de crédito, acesso a prédios comerciais, quartos de hotel, salas de conferência, salas de aula, metrô, todo o tempo se sujeitando às chaves para ligar o carro e abrir a porta da frente da casa. Entretanto, nenhuma padronização surgiu e como tal isto causa grandes inconveniências para o usuário devido ao fardo de carregar vários cartões e chaves, e a necessidade de estar apto a se lembrar de vários nomes de usuário e senhas. Em adição à inconveniência, os métodos em uso comum atualmente não provam de forma nenhuma a identidade – eles simplesmente provam que o usuário está de posse de uma cópia de um token. Estas são questões que os governos atacam em termos de segurança nacional, e os consumidores devem combater devido ao excesso de fraude de identidade.

[003] Os cartões inteligentes são uma solução proposta. Os cartões inteligentes são cartões que incluem alguma capacidade de processamento e memória. Os cartões inteligentes são levados para cada uso, inseridos em uma leitora. Em alguns casos, o usuário pode adicionalmente precisar informar um número de identificação pessoal (PIN) para acessar os dados/localização, utilizando o cartão inteligente. Toda esta ação do usuário não somente toma tempo, mas também re-

quer que o usuário carregue um cartão. Em geral, as leitoras de cartão também são carregadas. O cartão pode ser facilmente esquecido na leitora ou perdido.

[004] Na outra extremidade do espectro, o reconhecimento de impressão digital é um modo extremamente conveniente de executar identificação que recentemente se tornou econômico para emprego, mas as questões de segurança, de privacidade e de capacidade de dimensionamento permanecem para o uso confiável além da conexão local do cliente.

## SUMÁRIO DA INVENÇÃO

[005] Um método e aparelho para utilizar um token que compreendem receber uma indicação de uma presença de um terminal próximo de curto alcance e acordar o token em resposta a receber a indicação. O método adicionalmente compreende executar autenticação entre o token e o terminal, sem requerer que um usuário interaja diretamente com o token.

## BREVE DESCRIÇÃO DOS DESENHOS

[006] A presente invenção é ilustrada a título de exemplo, e não de limitação, nas figuras dos desenhos acompanhantes e nas quais números de referência iguais se referem a elementos iguais, e nas quais:

[007] A Figura 1 é um diagrama de blocos de uma concretização de uma rede que pode ser utilizada com a presente invenção.

[008] A Figura 2 é um diagrama de blocos de uma concretização de um sistema de computador que pode ser utilizado com a presente invenção.

[009] A Figura 3 é um diagrama de blocos de uma concretização dos componentes do terminal e do token sem fio.

[0010] A Figura 4A é um diagrama de blocos de uma concretização dos elementos do token sem fio.

[0011] A Figura 4B é um diagrama de blocos de uma concretização dos elementos do terminal que interagem com o token sem fio.

[0012] A Figura 5 é um fluxograma de vista geral do presente processo.

[0013] As Figuras 6A até 6C são fluxogramas de uma concretização da utilização do token sem fio a partir da perspectiva do terminal.

[0014] As Figuras 7A e 7B são fluxogramas de uma concretização da utilização do token sem fio a partir da perspectiva do token sem fio.

[0015] A Figura 8 é um fluxograma de uma concretização para iniciar um novo token sem fio.

[0016] A Figura 9 é um fluxograma de uma concretização para inicialmente fazer a interface de um token sem fio com um terminal, para adicionar informações específicas do terminal.

[0017] As Figuras 10A e 10B são ilustrações de duas concretizações do token sem fio.

**DESCRIÇÃO DETALHADA**

[0018] Um método e aparelho para um token são descritos. O dispositivo pode ser pequeno, sem ser maior do que o dispositivo sem fio em um chaveiro utilizado para destravar um carro. O dispositivo inclui um processador seguro e um transceptor de curto alcance com largura de banda estreita. Para uma concretização, curto alcance é na ordem de 2 metros, enquanto a largura de banda é ~100 kbps. O processador pode ser similar aos processadores utilizados em cartões inteligentes, enquanto o transceptor pode ser similar ao que é utilizado nos mouses e teclados sem fios da Microsoft/Logitech/Intel. Em sua memória segura, o dispositivo mantém a informação de identidade do proprietário e um gabarito de impressão digital para uso na autenticação. Ao receber o dispositivo, o usuário inicializa o dispositivo por transferir informação de identidade para o mesmo e então por registrar uma ou mais impressões digitais a serem armazenadas e utilizadas pelo dispositivo.

[0019] O dispositivo pode ser mantido de forma conveniente próximo, tal como no chaveiro do usuário, na carteira do usuário, no pulso do usuário como um bracelete, ou em uma localização discreta.

[0020] O sistema, em uma concretização, ocupa-se com destravar um token via a extração de um aspecto biométrico no hospedeiro/terminal, onde a associação acontece no token. Os dados e/ou as teclas no token seriam, no sentido geral, públicos (pré-autenticação), públicos (pós-autenticação), privado para o emissor (pré-autorização), ou privado para o emissor (pós-autorização). Estes dados poderiam ser certificados, pseudônimos, chaves privadas, chaves simétricas, ou outros dados relevantes.

[0021] Em uma concretização, o dispositivo permanece em um modo de espera de baixo consumo de energia aguardando por um ping a partir de um transmissor próximo. Este ping significa que o usuário se aproximou de um terminal que pode aceitar uma autenticação – por exemplo, uma porta, um computador, ou um contador de check-in de aeroporto. O teclado do PC ou a tranca da porta contêm o transmissor e um sensor de impressão digital. Quando o dispositivo recebe o ping, ele responde e inicia um canal de comunicação seguro. O usuário não tem que tocar o dispositivo – não tem necessidade de levá-lo no bolso ou na bolsa – e nenhuma informação de identificação é passada neste ponto. O dispositivo então aguarda que um gabarito biométrico seja enviado. O terminal utiliza o sensor biométrico para obter os dados biométricos, os aspectos são extraídos, e os aspectos extraídos são enviados para o dispositivo de token sem fio do usuário. O dispositivo associa estes aspectos com o gabarito biométrico armazenado do usuário registrado. Se ele combinar, o dispositivo libera a informação de identidade armazenada para o terminal através de técnicas criptográficas aceitas. Deste modo, é proporcionado para o usuário um token de identidade sem fio, conveniente, sem toque.

[0022] Em outra concretização, o token não é sem fio, mas ao invés disso, recebe um sinal através do corpo do usuário. Ao invés de um ping a partir da estação base, o token é ativado pelo usuário colocando seus dedos na placa sensora da estação base. Isto envia um sinal de baixa voltagem (se originando a partir do polegar na placa) através do corpo do usuário para se comunicar com o token. Este é um dispositivo alternativo para ativar o token, ao invés do envio de ping. Enquanto esta concretização utiliza o corpo do usuário para transmitir dados, o usuário não precisa interagir diretamente com o token, desde que o token em um relógio ou em uma chave de segurança (*key fob*) está em contato suficiente com o corpo do usuário, para receber um sinal deste modo.

[0023] Os exemplos dados abaixo se referem a um token sem fio. Entretanto, os versados na técnica entenderiam como implementar o token utilizando a transmissão através do corpo.

[0024] A Figura 1 é um diagrama de blocos de uma concretização de uma rede que pode ser utilizada com a presente invenção. O usuário carrega um cartão inteligente sem toque 120, também referido como token sem fio. Estes dois termos são usados de forma intercambiável neste documento para um dispositivo que proporciona identidade pessoal e/ou informação confidencial em resposta a receber um ping do transceptor, sem requerer que o usuário fisicamente toque o dispositivo. Observe que para a transmissão através do corpo, o usuário não precisa "tocar" o dispositivo. O termo "tocar", neste contexto, se refere às interações afirmativas entre o usuário e o dispositivo, ou seja, o requerimento do usuário interagir com o dispositivo de alguma maneira. O uso da transmissão passiva através do corpo não requer um ato afirmativo, ou toque, pelo usuário. Portanto, o cartão inteligente utilizando a condutibilidade através do corpo pode ser referido como um cartão inteligente sem toque.

[0025] O usuário, transportando o token sem fio 120, fica próximo de um dispositivo/localização com acesso limitado 150, ou terminal. O token sem fio 120 recebe um ping a partir do terminal limitado 150 requisitando autenticação para acesso. O dispositivo/localização com acesso limitado protegido pelo terminal 150 pode ser um dentre um portão, uma porta, ou um recinto para um computador, terminal de aeroporto, ou outra localização onde a autenticação é requerida. O cartão inteligente sem toque 120 interage com o dispositivo/localização com acesso limitado 150. O usuário é requisitado para interagir com o sensor biométrico 130 acoplado com o dispositivo/localização com acesso limitado 150. O sensor biométrico 130 envia os dados biométricos para processamento para o processador 140. Para uma concretização, o dispositivo/localização com acesso limitado 150, o processador 140, e o sensor biométrico 130, podem ser um único dispositivo integrado. Para outra concretização, o sensor biométrico 130 pode ser diretamente acoplado com o dispositivo/localização com acesso limitado 150 e com o processador 140. Para outra concretização, o sensor biométrico 130 pode ser acoplado através de uma conexão segura através da rede 110.

[0026] A rede 110 pode ser uma rede sem fio, uma rede com fio, uma conexão por cabo, ou qualquer outro tipo de conexão que permita a comunicação segura, ou que possa ser segura, entre o dispositivo/localização 150, e o sensor biométrico 130. Por exemplo, a comunicação entre o dispositivo/localização 150, o processador 140, e o sensor 130, pode ser através de uma rede não segura, tal como a Internet, utilizando um protocolo seguro, tal como camadas de soquete de segurança (SSL).

[0027] A Figura 2 é uma concretização do sistema de computador no qual a presente invenção pode ser implementada. Será aparente para os versados na técnica, entretanto, que outros sistemas alternati-

vos de várias arquiteturas de sistemas, também podem ser utilizados.

[0028] O sistema de computador ilustrado na Figura 2 inclui um barramento ou outro dispositivo interno de comunicação 215 para comunicar informação, e um processador 210 acoplado com o barramento 215 para processar informações. O sistema adicionalmente compreende uma memória de acesso randômico (RAM) ou outro dispositivo de armazenamento volátil 250 (referido como memória), acoplado com o barramento 215 para armazenar informações e instruções a serem executadas pelo processador 210. A memória principal 250 também pode ser utilizada para armazenar variáveis temporárias ou outras informações intermediárias durante a execução de instruções pelo processador 210. O sistema também compreende uma memória somente para leitura (ROM) e/ou o dispositivo de armazenamento estático 220 acoplado com o barramento 215 para armazenar informação estática e instruções para o processador 210, e um dispositivo de armazenamento de dados 225 tal como um disco magnético ou disco óptico, e sua unidade de disco correspondente. O dispositivo de armazenamento de dados 225 é acoplado com o barramento 215 para armazenar informações e instruções.

[0029] O sistema adicionalmente pode ser acoplado com um dispositivo de vídeo 270, tal como um tubo de raio catódico (CRT) ou um vídeo de cristal líquido (LCD), acoplado com o barramento 215 através do barramento 265 para exibir informações para um usuário de computador. Um dispositivo de entrada alfanumérico 275, incluindo teclas alfanuméricas e outras teclas, também pode ser acoplado com o barramento 215 através do barramento 265 para comunicar informações e seleções de comando para o processador 210. Um dispositivo de entrada do usuário adicional é o dispositivo de controle de cursor 280, tal como um mouse, uma trackball, caneta, ou teclas de direção do cursor, acopladas com o barramento 215 através do barramento 265 para

comunicar informação de direção e seleções de comando para o processador 210, e para controlar o movimento do cursor no dispositivo de vídeo 270. Dispositivos de entrada adicionais podem incluir um scanner 285, para digitalizar códigos de barra associados com imagens, e o dispositivo de entrada de áudio 295, o qual recebe entrada verbal a partir de um usuário. Dispositivos de entrada alternativos também podem ser implementados.

[0030] Outro dispositivo que opcionalmente pode ser acoplado com o sistema de computador 200 é um dispositivo de comunicação 290 para acessar outros nós de um sistema distribuído via uma rede. O dispositivo de comunicação 290 pode incluir qualquer um dentre uma série de dispositivos periféricos de trabalho em rede comercialmente disponíveis, tal como estes utilizados para acoplamento com Ethernet, rede em anel, Internet, ou rede de área ampla. Observe que qualquer um ou todos os componentes deste sistema ilustrado na Figura 2 e hardware associado podem ser utilizados em várias concretizações da presente invenção.

[0031] Um sensor biométrico 295 adicionalmente pode ser acoplado com o sistema de computador 200. O sensor biométrico 295 pode ser um sensor de impressão digital, para uma concretização.

[0032] Para uma concretização, o vídeo 270, o dispositivo de entrada 275 e o controle de cursor 280 podem ser combinados em uma única tela de toque. O vídeo com tela de toque permite a entrada de dados utilizando uma tela sensível a toque.

[0033] Será apreciado pelos versados na técnica que qualquer configuração do sistema pode ser utilizada para vários propósitos, de acordo com a implementação particular. A lógica de controle ou software implementando a presente invenção pode ser armazenada na memória principal 220, no dispositivo de armazenamento em massa 225, ou em outro meio de armazenamento localmente ou remotamente

acessível para o processador 210. Outro meio de armazenamento pode incluir discos flexíveis, cartões de memória, memória flash, ou unidades de CD-ROM.

[0034] Será aparente para os versados na técnica que os métodos e processos descritos neste documento podem ser implementados como software armazenado na memória principal 250 ou na memória somente para leitura 220, e executado pelo processador 210. Esta lógica de controle ou software também pode estar residente em um artigo de fabricação compreendendo um meio legível por computador possuindo código de programa legível por computador, incorporado no mesmo, e sendo legível pelo dispositivo de armazenamento em massa 225, e para causar que o processador 210 opere de acordo com os métodos e instruções neste documento.

[0035] O software da presente invenção também pode ser incorporado em um aparelho dedicado contendo um subconjunto dos componentes de hardware de computador, descritos acima. Por exemplo, o aparelho dedicado pode ser configurado para conter somente o barramento 215, o processador 210, e a memória 250 e/ou 225, e uma tela de toque.

[0036] O dispositivo também pode ser configurado para incluir um conjunto de botões ou componentes de sinalização de entrada com os quais um usuário pode selecionar a partir de um conjunto de opções disponíveis. O aparelho dedicado também pode ser configurado para incluir um aparelho de saída, tal como um vídeo de cristal líquido (LCD) ou matriz de elemento de vídeo para exibir informação para um usuário do aparelho dedicado. Métodos convencionais podem ser utilizados para implementar tal aparelho dedicado. A implementação da presente invenção para tal dispositivo seria aparente para os versados na técnica dada a descrição da presente invenção como proporcionada neste documento.

[0037] A Figura 3 é um diagrama de blocos de uma concretização dos componentes do terminal e do token sem fio. O token sem fio 120 inclui um receptor de baixa potência 310, o qual geralmente está LIGADO, e monitora os pings. O token sem fio 120 é projetado para ser portátil, tal como em um chaveiro. Assim, uma fonte de energia 305, tal como uma bateria, energiza o token sem fio 120. Para uma concretização, a bateria 305 pode ser recarregável. Alternativamente, a bateria 305 pode ser uma bateria alcalina. Para outra concretização, a fonte de energia 305 pode ser uma fonte de energia alternativa, agora disponível ou posteriormente descoberta.

[0038] O receptor de baixa potência 310 está LIGADO, e monitora pings a partir de qualquer terminal 350. Como discutido acima, os terminais 350 incluem transmissores de baixo alcance 360 que periodicamente emitem um ping. O receptor de baixa potência 310 monitora tal ping.

[0039] Se um ping for recebido, ele é passado para o processador de baixa potência 320. O processador de baixa potência 320 determina se "acorda" o restante do sistema. Em geral, a maior parte do sistema está em uma condição de baixo consumo, desligada ou em espera, para reduzir o consumo de energia. O processador de baixa potência 320 determina se o ping merece um despertar do sistema. Para uma concretização, somente certos pings são respondidos. Por exemplo, o processador de baixa potência 320 pode exigir que o ping esteja em uma frequência particular para acordar o sistema. Isto permitiria uma distribuição de transceptores possuindo várias faixas de frequência.

[0040] Se o processador de baixa potência 320 acordar o sistema, o transceptor 315 é utilizado para interagir com o terminal 350. O transceptor 315 envia e recebe dados. Como será discutido em maiores detalhes abaixo, o sistema adicionalmente inclui um co-

processador criptográfico 325, para executar as operações criptográficas requisitadas pelo usuário. Isto permite o estabelecimento de uma conexão segura entre o token sem fio 120 e o terminal 350. Isto adicionalmente permite a troca de dados biométricos, como será descrito abaixo. O token sem fio 120 adicionalmente inclui uma memória segura 330 para armazenar a informação de identidade do usuário, bem como chaves criptográficas, e o gabarito biométrico do usuário para autenticação. Para uma concretização, somente o co-processador criptográfico 325 está apto a acessar a memória segura 330.

[0041] O sistema pode adicionalmente incluir uma interface de tecla 340. A interface de tecla 340 permite uma interação que não é baseada em dados biométricos, entre o usuário e o token sem fio 120. Em geral, o usuário não precisa tocar o token sem fio 120 para utilizar o token sem fio 120 para autenticação. Entretanto, algumas vezes um usuário pode não ter uma característica biométrica reconhecível – por exemplo, as impressões digitais podem não ser percebidas após um acidente raspar os dedos, ou as varreduras de íris podem estar indisponíveis após um exame do olho que dilata as pupilas. Neste caso, o usuário pode utilizar a interface de tecla 340 para interagir com o sistema.

[0042] Uma interface de botão 335 pode ser adicionalmente proporcionada. A interface de botão 335 pode liberar certos dados especializados somente se o usuário interagir com o token sem fio 120. Isto será descrito em mais detalhes abaixo.

[0043] O token sem fio 120 adicionalmente pode incluir uma interface/carregador com fio 345. Em geral, o token sem fio 120 faz a interface com dispositivos exteriores utilizando o transceptor 315 e o receptor de baixa potência 310. Entretanto, em alguns casos, o usuário pode desejar transferir dados para o token sem fio 120, pode desejar carregar a bateria 305, ou pode desejar interagir através de uma interface

com fio. Assim, o sistema inclui uma interface com fio 345 para estes propósitos. A interface com fio 345 pode ser um soquete para receber uma tomada, uma conexão USB, uma conexão firewire, uma conexão de rede para fazer interface com uma rede com fio, ou qualquer tipo de conexão.

[0044] O terminal 350 inclui um transceptor 360 que envia pings periódicos, bem como as interfaces com o token sem fio 120. O terminal 350 adicionalmente inclui um sensor biométrico 130. Para uma concretização, o sensor biométrico 130 é um sensor de impressão digital acoplado com o terminal 350. Adicionalmente, o terminal 350 inclui o processador 355 para processar os dados biométricos a partir do sensor 130, bem como para criar uma conexão segura entre o terminal 350 e o token sem fio 120.

[0045] A Figura 4A é um diagrama de blocos de uma concretização dos elementos do token sem fio. O token sem fio 120 inclui uma porção sempre ligada 410. A porção sempre ligada 410 do sistema inclui um receptor de baixa potência 310, o qual monitora pings a partir de transceptores na vizinhança. Se o receptor 310 receber um ping, ele passa o mesmo para a chave de ativação do sistema 415. Para uma concretização, a chave de ativação do sistema 415 determina se acorda o restante do sistema. Para outra concretização, a chave de ativação do sistema 415 automaticamente acorda o sistema quando um ping é recebido.

[0046] Ao acordar, o transceptor 315 retorna dados para o terminal a partir do qual o ping foi recebido. Utilizando um criador seguro de seção 435, uma seção segura é criada entre o token sem fio 120 e o terminal. Para uma modalidade, métodos padrões sem fios podem ser utilizados para criar uma seção segura, tal como SSL, ou protocolos similares. Para uma concretização, um codificador 420 e chaves 430 (chaves públicas e privadas, para uma concretização), junto com um

certificado da chave pública 430, são utilizados para criar tal seção segura. Isto é descrito em maiores detalhes abaixo com respeito às Figuras 6A e 6B.

[0047] Uma vez que uma seção segura seja criada, o pseudônimo do usuário, a partir da memória 425, é passado para o terminal. O terminal pode requisitar uma característica biométrica a partir do usuário. Em geral, isto pode ser feito por se iluminar o sensor biométrico. Por exemplo, para um sensor de impressão digital, a área do sensor pode ser acesa, quando o dado biométrico é recebido. O terminal – descrito com respeito à Figura 4B abaixo – retorna o gabarito biométrico para verificação para o token sem fio 120. O gabarito biométrico é passado para o verificador de identidade 450. O verificador de identidade 450 utiliza o gabarito biométrico do usuário 455, também na memória segura 425. Se o verificador de identidade 450 determinar que os dados biométricos do usuário combinam com os dados recebidos a partir do terminal, ele retorna estes dados para o transceptor 315. O transceptor 315 retorna reconhecimento para o terminal, indicando que o usuário foi autenticado.

[0048] Para uma concretização, o terminal pode estar apto a acessar dados adicionais 432 ligados com o pseudônimo do usuário 434. Em geral, o pseudônimo 434 é uma identidade ligada, a qual pode não incluir o nome, o endereço de correio eletrônico, ou dados similares reais do usuário. Por exemplo, para Vance Bjorn, o pseudônimo pode ser VB. Os dados adicionais 432, os quais podem ser acessíveis para terminais particulares, podem incluir o nome completo do VB, o endereço residencial, e um número de seguro social. Por exemplo, se o terminal for um check-in de aeroporto, tais dados adicionais são necessários. Assim, se o usuário e o terminal tiverem anteriormente feito um acordo em que dados adicionais sejam descritos, o sistema pode revelar estes dados adicionais 432. Para uma concretização, a negoci-

ação inicial estabelece a identidade do terminal. Esta identidade do terminal pode então ser utilizada para determinar quais dados adicionais 432 liberar para o terminal, após a verificação de identidade.

[0049] O token sem fio 120 adicionalmente pode incluir a lógica de botão 440. Certas informações, tal como um número de seguro social de um número de cartão de crédito podem ser suficientemente sensíveis, as quais um usuário pode desejar somente liberar após pressionar um botão. Isto é permitido utilizando a lógica de botão 440. O usuário pode escolher tais opções, bem como registrar dados adicionais junto ao token sem fio 120 utilizando a interface com o usuário 445. Para uma concretização, a interface com o usuário 445 realmente utiliza um computador ou sistema similar para fazer a interface com o usuário. Para uma concretização, a interface com o usuário 445 é desativada a não ser que o usuário esteja acoplado com um terminal seguro, ou acoplado com um sistema de computador através de uma conexão com fios.

[0050] A Figura 4B é um diagrama de blocos de uma concretização dos elementos do terminal que interagem com o token sem fio. O terminal 350 pode ser um único dispositivo monolítico, tal como um cofre utilizado para acesso através de uma porta. Para outra concretização, o terminal 350 pode ser um sistema distribuído, no qual os vários componentes descritos neste documento estão em localizações diferentes, e fazem interface utilizando uma rede.

[0051] O terminal 350 inclui um transceptor 360, o qual interage com outros dispositivos. O terminal 350 adicionalmente inclui um gerador de ping 460, o qual gera um ping periódico, para iniciar o contato com um token sem fio. O gerador de ping 460 periodicamente envia uma cadeia de caracteres, ou marcação de horário. Para uma concretização, a cadeia de caracteres é um número randômico, gerado pelo gerador de número randômico 465. O número randômico é utilizado

para identificar se o ping sendo respondido é uma resposta ao ping oportuno. Assim, por exemplo, se alguém capturar um ping, de modo a configurar uma conversação falsa com o terminal 350, a pessoa teria que responder ao ping dentro de um período de tempo preestabelecido, tal como 1/2 segundo. Após este tempo, o ping expira, e um novo número randômico é gerado e utilizado pelo gerador de ping 460. Isto reduz a habilidade de alguém lograr um terminal 350 ou um token sem fio 120.

[0052] Em alguns casos, o transceptor 360 recebe uma resposta a partir de um token sem fio. A resposta, em geral, inclui o número randômico do ping, bem como um certificado, identificando o token sem fio.

[0053] A lógica de seção segura 490 utiliza estes dados – se o verificador de certificado 470 indicar que o certificado do token sem fio é válido – para estabelecer uma seção segura entre o terminal 350 e o token sem fio. Para uma concretização, a seção segura utiliza criptografia, baseada em criptografia de chave pública para estabelecer o canal de comunicações seguras. Para uma concretização, a lógica de criptografia/decriptografia 475 é utilizada para criptografar e decriptografar o fluxo de dados.

[0054] Uma vez que uma seção segura é estabelecida, o terminal 350 recebe o pseudônimo do usuário a partir do token sem fio. O verificador de pseudônimo 480 determina se o pseudônimo do usuário está no banco de dados de acesso 485. Se o pseudônimo do usuário estiver no banco de dados de acesso 485, esta informação é passada para a lógica de controle de acesso 499. A lógica de controle de acesso 499 determina qual o tipo de verificação é necessária para acesso através do terminal. Como discutido acima, o terminal pode variar ser desde uma porta de baixa segurança até um sistema de computador de alta segurança. Assim, o nível de verificação pode variar de somen-

te um pseudônimo até a verificação biométrica.

[0055] Se a verificação biométrica for necessária, a lógica de controle de acesso 499 requisita dados biométricos a partir do usuário. Para uma concretização, isto é feito por se iluminar ou de outro modo chamar a atenção para um sensor biométrico. Isto pode ser feito via uma exibição, luzes, ou através de outros dispositivos. Ao receber os dados biométricos a partir do usuário, os dados biométricos são passados para uma lógica de extração de minúcia 495. A lógica de extração de minúcia 495 extrai os dados relevantes a partir dos dados biométricos e cria um gabarito biométrico. Obviamente, características únicas apropriadas dos dados biométricos são extraídas. Por simplicidade, o termo "minúcia" será utilizado para descrever estas características únicas.

[0056] O transceptor então envia este gabarito biométrico para o token sem fio para verificação. Se a verificação for positiva, a lógica de controle de acesso 499 pode proporcionar acesso ao sistema protegido pelo terminal 350. A lógica de controle de acesso 499 adicionalmente pode requerer informações adicionais vinculadas, a partir do token sem fio do usuário. Esta informação é liberada, mediante solicitação, para o terminal 350. Se a informação apropriada for recebida, a lógica de controle de acesso 499 permite acesso à área/sistema protegido.

[0057] Para uma modalidade, se a área/sistema protegido for continuamente acessada durante um período de tempo pelo usuário – como um sistema de computador seguro – o verificador de acesso continuado 498 tipicamente faz o ping do token sem fio para verificar que o token sem fio continua a estar nas vizinhanças do terminal 350. Deste modo, o terminal 350 proporciona continuamente acesso verificado para um sistema seguro.

[0058] A Figura 5 é um fluxograma de vista geral do presente pro-

cesso. O processo começa no bloco 510. No bloco 510, o terminal envia pings periódicos. Se um token sem fio estiver suficientemente próximo do terminal para receber o ping, ele responde. Para uma concretização, o alcance do terminal é aproximadamente 2 metros (6 pés). Para outra concretização, o alcance do terminal pode ser diferente dependendo do tipo de terminal. Assim, o alcance de um terminal de porta pode ser 1 metro (3 pés), enquanto o alcance de um terminal de computador pode ser 3 metros (10 pés), permitindo a um usuário andar ao redor de um escritório e permanecer conectado com o sistema. O alcance pode ser ajustável a partir de alguns pés até algumas jardas. Para uma concretização, a tecnologia de telefone sem fio ou de espectro de difusão digital é utilizada para a transmissão da base.

[0059] Quando um token sem fio responde a um ping, uma conexão segura, tal como uma ligação SSL, é estabelecida entre o terminal e o token sem fio, no bloco 520.

[0060] No bloco 530, os certificados públicos e os certificados privados disponíveis para este terminal particular são enviados para o terminal pelo token sem fio. Cada certificado e chave privada possuem controle de acesso de modo que ele é público ou privado – pode ser lido por qualquer pessoa ou somente pela autoridade que criou o mesmo. Adicionalmente, cada certificado possui uma autorização de liberação de modo que ele pode ser liberado sem autenticação ou requerer autenticação biométrica. Cada objeto de dado identidade possui estes dois atributos. Público/privado e autenticação necessária/não necessária. Neste ponto, os certificados que são privados ou públicos, e os quais não requerem autenticação, são enviados para o terminal.

[0061] No bloco 540, a autenticação biométrica do usuário é requisitada. Para uma concretização, isto somente ocorre se alguns dos certificados, autenticações, e/ou dados exigirem autenticação biométrica. Se nenhuma autenticação biométrica for necessária, o processo

pode terminar após o bloco 530. A autenticação pode ser através de uma impressão digital, colocada em um sensor de impressão digital. O sensor de impressão digital está associado com o terminal e pode ser controlado pelo terminal.

[0062] No bloco 550, os dados biométricos são processados pelo terminal, ou por um processador associado com o terminal, e o gabarito biométrico é gerado.

[0063] No bloco 560, o gabarito biométrico é enviado para o dispositivo, com uma cadeia de caracteres. A cadeia de caracteres indica a hora e o dia atual, bem como a identidade do terminal. Ele é adicionalmente criptografado com a chave pública do token sem fio, de modo que somente o token sem fio apropriado está apto a acessar a cadeia de caracteres e retornar o mesmo.

[0064] No bloco 570, é executada uma associação no dispositivo, verificando que o gabarito de impressão digital combina com o gabarito de impressão digital do usuário. Esta combinação é feita no token. Isto proporciona segurança adicional, porque o gabarito é armazenado em uma localização diferente para cada usuário, e não é acessível sem o token.

[0065] No bloco 580, o token sem fio retorna um reconhecimento de que a autenticação obteve sucesso, junto com a cadeia de caracteres decriptografada.

[0066] No bloco 590, o transceptor sem fio envia os certificados públicos e privados que exigem autenticação para o terminal neste ponto. O acesso é proporcionado para o usuário, como apropriado. O processo então termina no bloco 595.

[0067] O presente processo proporciona uma interação sem toque para um usuário, a qual permite ao usuário executar a autenticação para quatro tipos de dados. Os tipos de dados estão na faixa de dados privados (específicos do terminal) exigindo autenticação em uma ex-

tremidade do espectro, até dados públicos (liberados para todos os terminais) não exigindo autenticação.

[0068] As Figuras 6A até 6C são fluxogramas de uma concretização utilizando o token sem fio a partir da perspectiva do terminal. O processo começa no bloco 605. No bloco 610, um ping é enviado pelo terminal, e o sistema determina se existiu uma resposta. Se não existiu uma resposta, o processo retorna para o bloco 610, para enviar outro ping. Para uma concretização, os pings são enviados periodicamente, existam ou não sessões atualmente ativas com os tokens sem fio. Para uma concretização, o ping periódico pode ser uma vez por segundo. Para uma concretização, um processo separado monitora se uma resposta foi recebida. Para uma concretização, um novo processo é gerado para cada resposta. Assim, um único terminal pode estar apto a interagir com vários tokens sem fio diferentes ao mesmo tempo.

[0069] Como discutido acima, o ping pode ou não incluir um número randômico. Se o ping não incluir um número randômico, um token sem fio que deseja interagir com o sistema envia uma requisição por um número randômico, no bloco 612, o qual é prontamente enviado. Alternativamente, o próprio ping pode ser um número randômico, caso em que o bloco 612 pode ser saltado.

[0070] No bloco 614, o número randômico criptografado é recebido de volta. O número randômico criptografado adicionalmente inclui uma cópia da chave pública certificada do token sem fio que está respondendo ao ping do terminal.

[0071] No bloco 616, o processo determina se o certificado acompanhando a chave pública do token sem fio ainda é válido. Os certificados podem ser inválidos devido a eles terem expirado, ou porque um usuário relatou que seu token quebrou. Assim, para uma concretização, o sistema acessa um servidor de certificado para verificar se o certificado recebido é autêntico, garantido por um servidor de certifica-

do aceito, e válido. Se o certificado não for bom, o processo continua para o bloco 618, e a conexão é recusada. O processo então termina no bloco 619.

[0072] Se o certificado for válido, o processo continua para o bloco 620. No bloco 620, o processo determinar se a autenticação integral do token sem fio é aceitável. Para uma concretização, cada token sem fio é proporcionado com um sistema de autenticação integral, tal como um "número de série". Esta autenticação integral do token sem fio é utilizada para impedir alguém de fabricar "tokens sem fio falsos" e passar os mesmos adiante. Se a autenticação integral do token sem fio falhar, o processo continua para o bloco 618, e termina. Caso contrário, o processo continua para o bloco 622.

[0073] No bloco 622, o número randômico criptografado, retornado pelo token sem fio, é decriptografado, utilizando a chave pública proporcionada no certificado.

[0074] No bloco 624, o processo determina se o número randômico que foi recebido era um número válido que foi enviado por este terminal. Isto impede o terminal errado de aceitar uma conexão com um token sem fio. Adicionalmente, isto impede um token sem fio falso de retornar um número randômico antigo, velho para autenticação. Se o número randômico for inválido, o processo continua para o bloco 618 e termina. Caso contrário, o processo continua para o bloco 626.

[0075] Algumas ou todas as etapas de autenticação acima podem ser saltadas em algumas implementações. No mínimo, o terminal deve receber uma resposta a partir do token sem fio, a qual indica que o token sem fio está na área.

[0076] No bloco 626, é criada uma conexão segura entre o token sem fio e o terminal. Para uma concretização, a chave pública do token sem fio é utilizada para criptografar uma chave de sessão, a qual é utilizada para a sessão segura.

[0077] No bloco 628, o terminal recebe o pseudônimo do usuário. O pseudônimo do usuário é um pseudônimo persistente, o qual está associado com um usuário particular, e com o token sem fio particular. O pseudônimo pode não ter conexão rastreável facilmente para o nome real do usuário.

[0078] No bloco 630, o processo determina se o pseudônimo proporcionado pelo usuário está no conjunto de pseudônimos aceitos. O terminal, como discutido acima, é um dispositivo de interconexão de rede que proporciona acesso restrito e seguro para alguma localização ou sistema. Assim, existe uma lista de usuários para os quais pode ser dado este acesso. O sistema determina se o pseudônimo do usuário está entre estes que têm acesso permitido. Se o pseudônimo do usuário não for encontrado no conjunto de acesso autorizado, o processo continua para o bloco 618, e termina. Observe que em cada um destes casos, pode existir uma comunicação com o usuário indicando que o acesso não está sendo proporcionado. Para outra concretização, a comunicação com o usuário pode indicar a razão para o acesso não permitido – por exemplo, certificado inválido, autenticação integral com falha, número randômico não válido, ou usuário não autorizado. Para outra concretização, o sistema pode não comunicar qualquer coisa para o usuário, e simplesmente terminar a conexão entre o terminal e o token sem fio. Para uma concretização, as preferências do terminal em nível de comunicação podem ser estabelecidas por um administrador.

[0079] No bloco 632, o processo determina se um dado biométrico é necessário para acesso. O sistema pode exigir um dado biométrico do usuário para autenticação, ou a informação de pseudônimo sozinha pode ser suficiente. Se o pseudônimo for suficiente, o processo continua para o bloco 662. No bloco 662, o acesso é proporcionado para o usuário.

[0080] Se um dado biométrico for necessário para acesso, o pro-

cesso continua para o bloco 634. No bloco 634, o dado biométrico é requisitado. Isto pode ser feito pela comunicação com o usuário através de uma mensagem, ou pela indicação para o usuário de alguma maneira que informação biométrica é requerida.

[0081] No bloco 636, o processo determina se uma informação biométrica foi recebida. Para uma concretização, este processo pode adicionalmente testar se uma informação biométrica legível foi recebida. Se nenhuma informação biométrica foi recebida, ou a qualidade da informação biométrica recebida é tal que ela não pode ser utilizada, o processo retorna para o bloco 634, para requisitar outra informação biométrica. Se uma informação biométrica foi recebida, o processo continua para o bloco 638.

[0082] No bloco 638, o sistema extrai um gabarito a partir da informação biométrica. Para uma impressão digital, o gabarito inclui as minúcias da impressão digital, bem como várias outras características. Para uma concretização, o processo descrito na Patente US Nº pode ser utilizado para gerar o gabarito biométrico.

[0083] No bloco 640, o gabarito biométrico extraído é enviado para o token sem fio. Como citado acima, a conexão entre o terminal e o token sem fio é segura. Para uma concretização, o token pode adicionalmente ser criptografado, antes do envio do mesmo para o token sem fio.

[0084] No bloco 642, o processo determina se uma aprovação foi recebida a partir do token sem fio, verificando que o gabarito biométrico combina com a informação biométrica do proprietário do token sem fio. Se nenhuma aprovação tiver sido recebida, o processo continua para o bloco 644. No bloco 644, o processo determina se um tempo limite foi alcançado. Se nenhum tempo limite tiver sido alcançado, o processo continua a aguardar pela aprovação. Se o tempo limite tiver sido alcançado, o processo continua para o bloco 646, e termina. Para

outra concretização, o processo pode retornar para o bloco 634 e requisitar uma nova informação biométrica para verificação. Esta preferência pode ser estabelecida pelo administrador.

[0085] Se a aprovação tiver sido recebida, o processo continua para o bloco 648. No bloco 648, o processo determina se informação adicional é necessária para o acesso. Como discutido acima, o pseudônimo não inclui o nome legal do usuário, ou dados similares, inicialmente. Assim, para alguns terminais, tal como os terminais utilizados para acesso em aeroporto, o nome legal do usuário pode ser requerido. Se informação adicional for necessária para o acesso, o processo continua para o bloco 650. Caso contrário, o processo continua para o bloco 662, onde o acesso é permitido.

[0086] No bloco 650, o processo determina qual tipo de autenticação foi utilizada, quando os dados foram inicialmente dispostos entre o terminal e o usuário. A autenticação pode ser autenticação baseada em terminal onde os dados são criptografados, mas liberados para todos os terminais sob demanda, ou autenticação baseada no token sem fio, onde os dados somente são liberados para o terminal que autorizou a recepção dos dados.

[0087] Se a autenticação baseada no token sem fio foi utilizada, o processo continua para o bloco 652. No bloco 652, a chave criptografada com a chave privada do terminal, junto com a chave pública certificada do terminal, é enviada para o token sem fio. Para uma concretização, estes dados podem ter sido trocados anteriormente, caso em que o sistema não precisa enviar outra cópia da chave pública do terminal. O token sem fio então tenta decriptografar o envelope envolvendo os dados adicionais, com a chave pública do terminal. Se a chave pública decriptografar com sucesso os dados, então o terminal está autorizado a acessar os dados. Portanto, o token sem fio envia dados adicionais para o terminal.

[0088] No bloco 654, apresentado o processo a partir da perspectiva do terminal, o processo determina se os dados requisitados foram recebidos. Como descrito acima, a autenticação dos dados é feita pelo token sem fio. Assim, se a autenticação obtiver sucesso, os dados são recebidos no bloco 654. Se os dados não forem recebidos, o processo continua a aguardar. Para uma concretização, após um período de tempo, o processo pode enviar novamente a requisição e a chave pública. Se os dados forem recebidos, o processo continua para o bloco 660.

[0089] No bloco 660, o processo determina se os dados recebidos combinam com os dados de autenticação associados com o usuário. Se combinarem, o processo continua para o bloco 662, e o acesso é permitido. Caso contrário, o processo termina no bloco 646.

[0090] Se, no bloco 650, a autenticação baseada em terminal for utilizada, o processo continua para o bloco 656. No bloco 656, os dados adicionais são requisitados e recebidos a partir do token sem fio. Os dados recebidos, entretanto, são criptografados com a chave do terminal que originalmente tinha sido autorizado para os dados. Assim, os dados somente são acessíveis se o terminal tiver a chave.

[0091] No bloco 658, os dados são decriptografados utilizando a chave do terminal. Para uma concretização, a chave é a chave privada do terminal. Para outra concretização, uma "chave de dados adicional" separada pode ser utilizada para este processo.

[0092] Os dados adicionais são armazenados no token sem fio criptografados com a chave pública do terminal, e assim, inacessíveis para qualquer pessoa que não possua a chave privada do terminal. O processo então continua para o bloco 660, para verificar se os dados combinam com os dados de autenticação.

[0093] Se o usuário for autenticado com sucesso – através somente do pseudônimo, do pseudônimo e da informação biométrica, ou do

pseudônimo, da informação biométrica e da informação adicional – no bloco 662, o acesso aos dados/localização restritos é proporcionados.

[0094] No bloco 664, o processo determina se o acesso é um acesso contínuo, utilizando um computador, ou um acesso ocasional, como através de uma porta ou portão. Se o acesso for um acesso ocasional, o processo continua para o bloco 670. No bloco 670, a conexão com o token sem fio é fechada, e no bloco 672, o processo termina. Se a conexão for uma conexão contínua, o processo continua para o bloco 666.

[0095] No bloco 66, o terminal faz um ping para o token sem fio para verificar se o token sem fio continua a estar próximo do terminal. O ping pode ser periódico. Para uma concretização, o ping é uma vez por minuto. Entretanto, o período entre os pings pode variar, dependendo do nível de segurança necessário. Em situações de segurança extrema, a conexão pode ser mantida continuamente entre o token sem fio e o terminal. Em situações menos seguras, o ping pode ser reduzido para uma vez a cada 30 minutos ou mesmo para períodos maiores. Para uma concretização, este período pode ser ajustado pelo administrador.

[0096] No bloco 668, o processo determina se o token sem fio permanece próximo do terminal. Se permanecer, o processo retorna para o bloco 666, para novamente fazer um ping após o período preestabelecido ter decorrido. Se o token sem fio não estiver mais próximo do terminal, o processo continua para o bloco 670.

[0097] No bloco 670, a conexão, se ela permanece aberta, com o token sem fio, é fechada. Qualquer acesso não bloqueado é novamente bloqueado, para requerer nova verificação para acesso adicional. O processo então termina no bloco 672. Deste modo, o terminal proporciona acesso seguro contínuo, em um dentre vários níveis de segurança, utilizando um token sem fio que não requer que o usuário realmen-

te toque no token sem fio.

[0098] As Figuras 7A e 7B são fluxogramas de uma concretização utilizando o token sem fio a partir da perspectiva do token sem fio. O processo começa no bloco 705. Para uma concretização, este é um processo contínuo de monitoramento, sempre que energia estiver disponível para o token sem fio.

[0099] No bloco 710, o processo determina se um ping foi recebido. Um ping é recebido quando o token sem fio entra dentro do alcance de difusão do terminal. Se nenhum ping for recebido, o token sem fio continua a monitorar. Para uma concretização, a parte do token sem fio que é utilizada para monitorar é uma parte analógica, a qual possui um consumo de energia extremamente baixo. Assim, este processo de monitoramento pode ser mantido por um longo período sem troca ou recarga das baterias. Se um ping for recebido, o processo continua para o bloco 715.

[00100] No bloco 715, o sistema é acordado. Como citado acima, a parte de monitoramento do sistema é um sistema de baixo consumo de energia, enquanto para as etapas de comunicação segura, de criptografia e de autenticação, um sistema com maior consumo de energia é necessário.

[00101] No bloco 720, um número randômico é requisitado e recebido a partir do terminal, a partir do qual o ping foi recebido. Para uma concretização, o próprio ping incorpora um número randômico, caso em que este bloco pode ser eliminado.

[00102] No bloco 725, o número randômico é criptografado com a chave privada do usuário, e com a própria chave do token sem fio.

[00103] No bloco 730, o número randômico criptografado, junto com o pseudônimo público e a informação do usuário, e com uma chave pública certificada do usuário, é enviado para o terminal. Para outra concretização, o(s) pseudônimo (s) público(s) não é enviado até que

uma sessão segura seja estabelecida.

[00104] No bloco 735, o processo determina se uma requisição por conexão segura foi recebida a partir do terminal. A requisição por conexão segura, para uma concretização, inclui uma chave de sessão criptografada com a chave pública do usuário. Se a requisição por conexão segura ainda não tiver sido recebida, o processo continua para o bloco 740. No bloco 740, o processo determina se o período de espera excede o período limite. Para uma concretização, o período limite pode ser tão curto quanto uma fração ou um segundo, ou tão longo quanto alguns minutos. Se o período limite ainda não tiver sido excedido, o processo retorna para o bloco 735, para aguardar por uma requisição por conexão segura. Se o período limite for excedido, o processo continua para o bloco 745. No bloco 745, o sistema novamente dorme, deixando somente a parte de monitoramento de ping do sistema acordada. O processo então retorna para o bloco 710.

[00105] Se uma requisição por conexão segura for recebida, no bloco 735, o processo continua para o bloco 750.

[00106] No bloco 750, uma conexão segura é criada entre o terminal e o token sem fio. Se os pseudônimos e a informação não requerendo autenticação não foram enviadas anteriormente, elas são enviadas neste ponto, no bloco 753. Esta informação pode incluir informação pública. Bem como informação específica para o terminal requisitante.

[00107] O token sem fio não monitora outros pseudônimos ou informações relacionadas que ele tem disponível que podem ser aplicáveis para este terminal. Ao invés disso, o token sem fio simplesmente aguarda para determinar se um gabarito biométrico foi recebido, no bloco 755. Se um gabarito biométrico não foi recebido, o processo continua para o bloco 760. No bloco 760, o processo determinar se o período de espera excedeu o período limite. Para uma concretização, o

período limite pode ser tão curto quanto uma fração ou um segundo, ou tão longo quanto uns poucos minutos. Se o período limite ainda não tiver sido excedido, o processo retorna para o bloco 755, para aguardar por um gabarito biométrico. Se o período limite for excedido no bloco 760, o processo continua para o bloco 745. No bloco 745, o sistema novamente dorme, deixando somente a parte de monitoramento de ping do sistema acordada. O processo então retorna para o bloco 710.

[00108] Se um gabarito biométrico for recebido, no bloco 755, o processo continua para o bloco 765.

[00109] No bloco 765, o processo compara os dados biométricos recebidos a partir do terminal com o gabarito biométrico do usuário, armazenado na memória segura. No bloco 770, o processo determina se o gabarito biométrico do usuário combina com os dados biométricos a partir do terminal. Se os dois não combinarem, o processo continua para o bloco 745, e vai dormir. Para uma concretização, uma notícia de combinação com falha é enviada para o terminal. Para uma concretização, o terminal rastreia combinações consecutivas com falha. Para uma concretização, após um número preestabelecido de combinações com falha, ou um número preestabelecido de combinações com falha consecutivas, os dados seguros são apagados do token. Neste caso, o usuário deve se registrar novamente com um servidor acreditado de modo a utilizar o token novamente. Isto impede um ladrão de roubar o token e então tentar acessar repetidamente com vários modelos biométricos até que o acesso seja proporcionado.

[00110] Se o gabarito biométrico combinar com os dados biométricos, o processo continua para o bloco 775. No bloco 775, a cadeia de caracteres é decriptografada com a chave privada do usuário. A cadeia de caracteres é uma marcação de tempo ou de data ou identificador de dados similar que verifica se os dados biométricos recebidos pelo

token sem fio são os dados biométricos que foram extraídos pelo terminal. A cadeia de caracteres, para uma concretização, os dados biométricos são criptografados com a chave pública do token sem fio, pelo terminal. Para uma concretização, a cadeia de caracteres pode ser novamente criptografada com a chave pública do terminal (por exemplo, assinada).

[00111] No bloco 780, o reconhecimento de uma combinação é retornado para o terminal, junto com a cadeia de caracteres decriptografada, e qualquer pseudônimo/dados adicionais que requeiram autenticação biométrica. Para uma concretização, o reconhecimento, a cadeia de caracteres e outros dados, são enviados criptografados com a chave pública do terminal, assim como para proporcionar segurança adicional.

[00112] No bloco 782, o processo determina se uma requisição por dados adicionais específicos do terminal foi recebida. Se não, o processo continua diretamente para o bloco 790.

[00113] Se uma requisição por dados adicionais específicos do terminal for recebida, o processo determina se a requisição incluía uma chave ou não. Se nenhuma chave estiver incluída, o processo continua para o bloco 786. No bloco 786, os dados específicos do terminal são enviados, se eles estiverem criptografados. Desde que os dados são criptografados com a chave pública do terminal, assim são somente acessíveis para o terminal.

[00114] Se uma chave estiver incluída, a chave é assinada com a chave privada do terminal, e inclui uma cópia certificada da chave pública do terminal. O processo continua para o bloco 784. No bloco 784, a identidade do terminal, e fato de que estes dados estão associados com o terminal requisitante, são verificados, utilizando as chaves. Se o processo de decriptografia obtiver sucesso, o processo continua para o bloco 786, e os dados são enviados para o terminal. O processo então

continua para o bloco 790. No bloco 790, o processo determina se um ping de manutenção foi recebido. O ping de manutenção é periodicamente enviado pelo terminal para verificar se o token sem fio permanece nas vizinhanças.

[00115] Se nenhum ping de manutenção for recebido, o processo determina se um processo esgotou o tempo, no bloco 792. Para uma concretização, existe um período de tempo de espera preestabelecido para o ping de manutenção. Para outra concretização, o terminal pode comunicar seu período de ping de manutenção para o token sem fio na conexão inicial. O tempo limite é então dinamicamente estabelecido. Para uma concretização, o tempo limite é estabelecido para ser ligeiramente mais longo do que o período do ping de manutenção do terminal. Se o sistema esgotar o tempo, no bloco 792, o processo retorna para o bloco 745, para dormir novamente. Se o período limite não tiver decorrido, o processo continuar a monitorar um ping de manutenção no bloco 790.

[00116] Se um ping de manutenção for recebido, o processo, no bloco 795, retorna um sinal de "vivo" para o terminal, indicando que o token sem fio permanece nas proximidades do terminal. Para uma concretização, durante o período de manutenção, partes do sistema podem ser colocadas para dormir – tal como os elementos de criptografia e de decriptografia, a lógica de acesso à memória e assim por diante – enquanto os elementos de comunicação são mantidos acordados. O processo então retorna para o bloco 790, para aguardar por um próximo ping de manutenção.

[00117] Deste modo, um token sem fio pode ser utilizado, sem requerer qualquer interação humana com o próprio token. Isto é vantajoso para autenticação e acesso em um grande número de ambientes, de corporações, para acesso físico, transações financeiras, verificações de segurança de linha aérea, portas de quatro de hotel, ligar car-

ros, ou quaisquer outros usos.

[00118] A Figura 8 é um fluxograma de uma concretização para iniciar um novo token sem fio. O processo começa no bloco 805. No bloco 810, uma conexão é recebida a partir de um novo token sem fio não iniciado. Para uma concretização, esta conexão pode ser com uma página da Internet. Para outra concretização, esta conexão pode ser com um servidor seguro na mesma rede. Por exemplo, uma corporação pode ter um servidor interno que proporciona tais serviços de inicialização. A conexão é uma conexão segura.

[00119] No bloco 815, o servidor solicita ao token sem fio para criar um par de chaves pública-privada. No bloco 820, o usuário é solicitado a criar um pseudônimo. O pseudônimo é um pseudônimo anônimo persistente, e não precisa ter qualquer conexão com o nome real e/ou com a identidade do usuário. Entretanto, em um ambiente corporativo, a política pode ser ter um pseudônimo que seja idêntico ao nome real do usuário, ou ao endereço de correio eletrônico do usuário, ou a algum identificador único similar. Não existe limitação inerente em relação aos pseudônimos possíveis. Entretanto, cada organização/instituição/servidor impõem suas próprias limitações preferidas.

[00120] No bloco 825, o servidor requisita, e recebe, a chave pública e o pseudônimo a partir do token sem fio. Para uma concretização, o par de chaves e o pseudônimo são interativamente criados, com a interface com o usuário, proporcionada pelo servidor. Neste caso, o servidor pode enviar o pseudônimo para o usuário.

[00121] No bloco 827, o servidor recebe um dado biométrico a partir do usuário. O dado biométrico pode ser uma impressão digital, várias impressões digitais, uma varredura de íris, uma impressão de mão, uma impressão de voz, qualquer outro tipo de dado biométrico, ou uma combinação dos vários dados biométricos.

[00122] No bloco 829, o servidor extrai os dados biométricos subja-

centes a partir do dado biométrico do usuário. Para uma impressão digital, um gabarito é criado, incluindo minúcias, e potencialmente aspectos adicionais. De forma similar, uma listagem de aspectos únicos que podem ser utilizados para identificar o usuário é criada para cada tipo de dado biométrico.

[00123] No bloco 830, o servidor requisita verificação de identidade. A verificação de identidade pode ser através de um cartão de crédito e de informação de faturamento, uma licença de motorista, ou a verificação por um indivíduo acreditado tal como um administrador.

[00124] No bloco 835, o processo determina se a verificação de identidade foi recebida e verificada. Se não, o processo, no bloco 840, aguarda a verificação. Este processo pode neste ponto ser descontinuado. Por exemplo, se prova por papel físico está sendo enviada para o servidor, o processo de inicialização pode ser descontinuado, até que a verificação seja recebida. Assim, o usuário pode ser informado que ele ou ela deve conectar o token sem fio com o servidor novamente em algum momento futuro, após a identidade ter sido verificada com sucesso.

[00125] Se a identidade tiver sido verificada com sucesso no bloco 835, o processo continua para o bloco 845. Alternativamente, o processo do bloco 830, 835 e 840 pode ser saltado, e o usuário pode não ser requerido de proporcionar qualquer dado pessoal verdadeiramente autenticado.

[00126] No bloco 845, o servidor, o qual é uma autoridade de certificação, gera um certificado com a chave pública do usuário, e retorna a chave pública certificada para o token sem fio. Para outra concretização, o servidor pode utilizar um servidor de certificado convencional para proporcionar um certificado para a chave pública do usuário. O servidor adicionalmente retorna o gabarito biométrico para o token sem fio.

[00127] No bloco 850, a chave pública certificada, a chave privada, o gabarito biométrico, e o pseudônimo, são armazenados na memória segura no token sem fio. Neste ponto, o token sem fio pode ser utilizado por um terminal. Para uma concretização, se o servidor estiver dentro de uma corporação, no bloco 855, o(s) pseudônimo(s) do usuário é (são) adicionado(s) para o banco de dados de acesso dentro da corporação. O processo então termina no bloco 860. Deste modo, o token sem fio pode ser inicializado utilizando um servidor seguro, o qual pode ser local ou remoto. Se o servidor seguro for local, e um administrador acreditado estiver disponível para fazer o registro, a verificação de identidade pode ser simplificada. Por exemplo, o administrador pode colocar sua impressão digital autenticada em um sensor biométrico para indicar que uma identificação com sucesso aconteceu.

[00128] A Figura 9 é um fluxograma de uma concretização da realização da interface de um token sem fio com um terminal, e para adicionar informação específica do terminal. O processo começa no bloco 910, quando a conexão entre o token sem fio e um servidor é inicialmente estabelecida. O servidor pode ser um terminal, um servidor que atende a vários terminais, um sistema independente que é utilizado para atualizar um banco de dados de acesso, ou outro sistema.

[00129] No bloco 915, o token sem fio interage com o servidor. Este processo inclui estabelecer uma ligação segura entre o token sem fio e o sistema. Para uma concretização, a conexão pode ser uma conexão com fios, uma conexão sem fios, ou uma conexão direta ligada na tomada. Se a conexão for uma conexão direta, nenhuma sessão segura precisa ser estabelecida.

[00130] No bloco 920, a identidade do usuário é verificada. Para uma concretização, isto pode ser feito pela conexão com o servidor de autenticação original, pela requisição de algum tipo de autenticação adicional, tal como um cartão de crédito ou licença de motorista, ou

através de algum outro dispositivo. Para uma concretização, o sistema adicionalmente pode verificar a impressão digital do usuário – por exemplo, esta pessoa sendo identificada é a mesma pessoa cujo gabarito de impressão digital está armazenado no token sem fio como o proprietário do token. Para outra concretização, o sistema é atendido por um administrador, o qual pode executar a verificação.

[00131] No bloco 925, o pacote de dados adicionais é criado para o token sem fio. O pacote de dados adicionais são os dados que os terminais desejam utilizar no futuro. Por exemplo, para um terminal de linha aérea, o registro pode ser em um contador de check-in de linha aérea. O pacote de dados adicionais pode incluir o nome legal completo do usuário, o endereço residencial, e o país de origem. Informações adicionais, tal como número de licença de motorista e número de passaporte, também podem estar incluídas. Tudo isto é gerado no servidor, interativamente com o usuário.

[00132] No bloco 930, o processo determina se a preferência é ter a autenticação baseada no terminal ou não. A autenticação baseada no terminal significa que o pacote de dados é liberado para qualquer terminal requisitante. Entretanto, o pacote de dados é criptografado, de modo que somente o terminal possuindo a chave apropriada está apto a decriptografar os dados. Entretanto, isto pode ser menos seguro, desde que um hacker determinado pode ter acesso a estes dados através de um longo período. Portanto, a alternativa é ter o token sem fio determinando se libera estes dados ou não.

[00133] Se a autenticação baseada em terminal for selecionada, o processo continua para o bloco 935. No bloco 935, uma chave é utilizada para criptografar o pacote de dados. Isto garante que somente o(s) terminal(is) que possui(em) a chave está(ao) apto(s) a acessar estes dados. Para uma concretização, a chave é uma chave pública associada com estes dados, e a chave privada apropriada está dispo-

nível para cada um dos terminais que acessariam estes dados. Para outra concretização, a chave pode ser uma chave simétrica. Cópias da chave simétrica então estariam disponíveis para cada um dos terminais que possui permissão para acessar estes dados. O processo então continua para o bloco 945.

[00134] Se, no bloco 930, a autenticação baseada no token sem fio for selecionada, o processo continua para o bloco 940. No bloco 940, os dados são embalados em um "envelope" que é criptografado com a chave privada do terminal. De modo a acessar os dados, o terminal deve transmitir sua chave pública certificada, a qual então deve desembalar o envelope. O processo então continua para o bloco 945.

[00135] No bloco 945, o pacote de dados é enviado para o token sem fio.

[00136] No bloco 950, o processo determina se o sistema deseja ter os dados liberados somente em resposta a um usuário apertando uma interface de botão no token sem fio. Se não, os dados são armazenados, no bloco 955, e o processo termina no bloco 960. Se o sistema desejar forçar um botão, o token sem fio armazena os dados como um pacote de dados ativado por botão, no bloco 965. O processo então termina no bloco 960.

[00137] Deste modo, um sistema pode adicionar dados adicionais que seriam úteis para seus processos de autenticação e acesso. Um único sistema pode adicionar este pacote de dados, e por distribuir as chaves para o terminal apropriado, todos os terminais relacionados podem acessar estes dados.

[00138] As Figuras 10A e 10B são ilustrações de duas concretizações do token sem fio. Um exemplo de um token sem fio é uma chave de segurança 1010, a qual pode ser facilmente carregada no porta-chaves do usuário. A chave de segurança 1010 geralmente inclui o mecanismo de comunicação sem fios, o processador e a memória

descritos acima. A chave de segurança 1010 pode adicionalmente incluir botões 1030 para permitir a interação se um dado biométrico não estiver disponível ou for inaceitavelmente ruim, e os conectores 1020, para permitir uma conexão com fio.

[00139] Um token sem fio alternativo é um relógio 1050, o qual inclui os botões 1060. Qualquer outro formato nativo que geralmente seria carregado pelo usuário em todos os momentos pode ser utilizado. Assim, o formato do token sem fio pode variar de uma chave de segurança até um formato de cartão inteligente, de um relógio, de um bracelete ou de qualquer outro dispositivo que seria por padrão carregado por uma pessoa usuária todos os momentos.

[00140] No relatório descritivo precedente, a invenção foi descrita com referência às concretizações ilustrativas específicas da mesma. Entretanto, será evidente que várias modificações e alterações podem ser feitas junto à mesma sem se afastar do espírito e do escopo mais amplo da invenção como expostos nas reivindicações anexas. O relatório descritivo e os desenhos, por consequência, são para serem considerados em um sentido ilustrativo ao invés do que em um sentido restritivo.

## REIVINDICAÇÕES

1. Token, caracterizado pelo fato de que compreende:

um receptor de baixa potência, no token, para receber uma indicação indicando uma presença de um terminal de alcance curto próximo; a indicação incluindo informação que expira;

um processador de baixa potência, no token, para determinar se a indicação deve ser respondida, o processador de baixa potência incluindo uma lógica de despertar para despertar o token em resposta à determinação pelo processador de baixa potência que a indicação deve ser respondida;

um transceptor para retornar um pedido de conexão ao terminal de alcance curto, o pedido de conexão incluindo a informação que expira, para provar que o ping é recente; e

um verificador de identidade, no token, para executar a autenticação entre o token e o terminal, a autenticação sendo uma autenticação biométrica de um usuário, com base nos dados biométricos recebidos do terminal, comparando os dados biométricos recebidos do terminal com os dados do padrão biométrico do usuário armazenados com segurança no token, sem exigir que um usuário toque fisicamente no token, criando assim uma autenticação de dois fatores baseada no token que o usuário possui e na biometria do usuário, e sem liberar os dados do padrão biométrico para o terminal.

2. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que é implementado como uma chave de segurança.

3. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreende um criador seguro de sessão para configurar um canal de comunicações seguras entre o token sem fio e o terminal de alcance curto.

4. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreende:

um transceptor para enviar um pseudônimo e uma chave pública certificada ao terminal; e

um criador seguro de sessão para estabelecer um canal de comunicações seguras entre o token sem fio e o terminal que utiliza a chave pública certificada.

5. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreende:

um transceptor para receber um gabarito biométrico vindo do terminal, através de um canal de comunicações seguro; e

o verificador de identidade para determinar se o gabarito biométrico combina um gabarito biométrico do proprietário do token sem fio.

6. Token, de acordo com a reivindicação 5, caracterizado pelo fato de que o gabarito biomédico do proprietário do token sem fio é armazenado em memória segura no token sem fio

7. Token, de acordo com a reivindicação 5, caracterizado pelo fato de que adicionalmente compreende o transceptor para adicionalmente enviar resultados de autenticação para o terminal, para permitir o acesso de usuário, conforme proporcionado pelo terminal.

8. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreendendo:

o transceptor para receber pings de manutenção periódicos após autenticação; e

o transceptor para adicionalmente responder aos pings periódicos verificando a proximidade continuada do token sem fio para o terminal.

9. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreende:

pseudônimos inseguros liberados para um terminal em resposta a um pedido, quando uma sessão segura for estabelecida; e

pseudônimos seguros liberados para um terminal em resposta a um pedido somente depois da autenticação biométrica do usuário.

10. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreende:

pseudônimos públicos liberados para qualquer terminal em resposta a um pedido, quando uma sessão segura foi estabelecida; e

pseudônimos privados liberados somente ao terminal que estabeleceu inicialmente os pseudônimos privados.

11. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que adicionalmente compreende um temporizador para colocar o token sem fio de volta à espera depois que um processo de autenticação foi terminado.

12. Token, de acordo com a reivindicação 11, caracterizado pelo fato de que adicionalmente compreende uma porção sempre ligada do token sem fio, que permanece ligada depois que o token sem fio foi posto a esperar, para continuar monitorando os pings, a porção sempre ligada do token sem fio incluindo o receptor de baixa potência.

13. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que o token se comunica com o terminal usando frequências sem fio.

14. Token, de acordo com a reivindicação 1, caracterizado pelo fato de que o token se comunica com o terminal usando a condutibilidade da pele humana.

15. Terminal para permitir o uso de um token sem fio para autenticação, o terminal caracterizado pelo fato de que compreende:

um gerador de ping para gerar pings periódicos, um ping tendo um tempo de vida temporário baseado na informação que expira, para uma resposta a ser usada por um token sem fio;

um transceptor para receber um pedido de conexão de um

token sem fio que recebeu o ping, o token sem fio enviando o pedido de conexão em resposta ao recebimento do ping, o pedido de conexão incluindo as informações do ping, em que o ping é recebido quando o token sem fio está dentro de um raio associado ao terminal, o raio associado ao terminal com base em um tipo de terminal;

um sensor biométrico para receber uma biometria a partir do usuário;

o transceptor para enviar a biometria ao token sem fio, e para receber uma autenticação a partir do token sem fio confirmando uma identidade do usuário, sem liberar um gabarito biométrico para o terminal;

uma lógica segura da sessão para estabelecer uma sessão segura com o token sem fio quando as informações dentro do pedido de conexão não estão expiradas e o token sem fio é autorizado; e

uma lógica de controle de acesso para fornecer o acesso a um sistema de acesso limitado, em resposta a receber a informação de autenticação do token sem fio, as informações de autenticação com base na biometria enviada pelo terminal ao token sem fio.

16. Terminal, de acordo com a reivindicação 15, caracterizado pelo fato de que adicionalmente compreende:

um sensor biométrico para receber dados biométricos de um usuário para a autenticação;

uma lógica da extração da minúcia para extrair um gabarito biométrico a partir dos dados biométricos; e

o transceptor para enviar o gabarito biométrico via a sessão segura para o token sem fio para autenticação do usuário pelo token sem fio.

17. Terminal, de acordo com a reivindicação 15, caracterizado elo fato de que compreende ainda um verificador de pseudônimo para verificar se um pseudônimo, incluído como parte da informação

de autenticação, e recebido a partir do usuário está em um banco de dados de acesso.

18. Terminal, de acordo com a reivindicação 17, caracterizado elo fato de que compreende ainda dados adicionais requisitados pela lógica de controle de acesso, se dados adicionais forem necessários para proporcionar acesso.

19. Terminal, de acordo com a reivindicação 15, caracterizado elo fato de que compreende ainda um verificador de acesso continuado para periodicamente enviar um ping de manutenção após ter sido proporcionado acesso a um usuário a um sistema de acesso limitado para verificar se o usuário permanece em proximidade ao sistema de acesso limitado.

20. Terminal, de acordo com a reivindicação 15, caracterizado elo fato de que compreende ainda um gerador de número randômico usado para gerar números randômicos para uma conexão inicial entre o terminal e o token sem fio, de modo que somente um ping corrente esteja disponível para resposta.

21. Terminal, de acordo com a reivindicação 15, caracterizado elo fato de que  o sistema de acesso limitado pode incluir um ou mais do que:

um edifício, uma sala, um sistema de computador, um terminal de segurança de aeroporto, um veículo, um caixa automático ou sistema de transação financeira similar;

um transceptor para retornar um pedido de conexão um terminal de alcance curto, o pedido de conexão incluindo a informação que expira, para provar que o ping é recente; e

um verificador de identidade, no token, para executar a autenticação entre o token e o terminal.

22. Método de utilização de um token sem fio caracterizado pelo fato de que compreende as etapas de:

receber um ping pelo token sem fio indicando uma presença de um terminal de alcance curto próximo, a indicação incluindo infomação que expira;

determinar, por um receptor de baixa potência no token sem fio, se o ping deve ser respondido sem acordar o token sem fio;

acordar o token sem fio por uma lógica de despertar em resposta para determinar que o ping deve ser respondido; e

retornar um pedido de conexão por um transceptor ao terminal de curto alcance, o pedido de conexão incluindo a informação que expira, para provar que o ping é recente; e

executar autenticação entre o token sem fio e o terminal, por um verificador de identidade, a autenticação sendo uma autenticação biométrica de um usuário, com base nos dados biométricos recebidos do terminal, comparando os dados biométricos recebidos do terminal com os dados do padrão biométrico do usuário armazenados com segurança no token, sem exigir que um usuário toque fisicamente o token sem fio, criando assim uma autenticação de dois fatores com base no token que o usuário possui e no biométrico que o usuário possui, e sem liberar os dados do padrão biométrico para o terminal.

23. Método, de acordo com a reivindicação 22, caracterizado pelo fato de que o token sem fio é implementado em uma chave de segurança.

24. Método, de acordo com a reivindicação 22, caracterizado pelo fato de que compreende ainda a etapa de estabelecer um canal seguro de comunicações entre o token sem fio e o terminal de alcance curto.

25. Método, de acordo com a reivindicação 22, caracterizado pelo fato de que a etapa de executar autenticação compreende as etapas de:

enviar um pseudônimo e uma chave pública ao terminal; e

estabelecer um canal seguro de comunicações entre o token sem fio e o terminal que utiliza a chave pública certificada.

26. Método, de acordo com a reivindicação 22, caracterizado pelo fato de que ainda compreendendo as etapas de:

receber um gabarito biométrico a partir do terminal através do canal seguro de comunicações; e

determinar se o gabarito biométrico casa com o gabarito biométrico do proprietário do token sem fio.

27. Método, de acordo com a reivindicação 26, caracterizado pelo fato de que ainda compreende a etapa de:

enviar os resultados de autenticação para o terminal, para permitir o acesso do usuário, conforme provido pelo terminal.

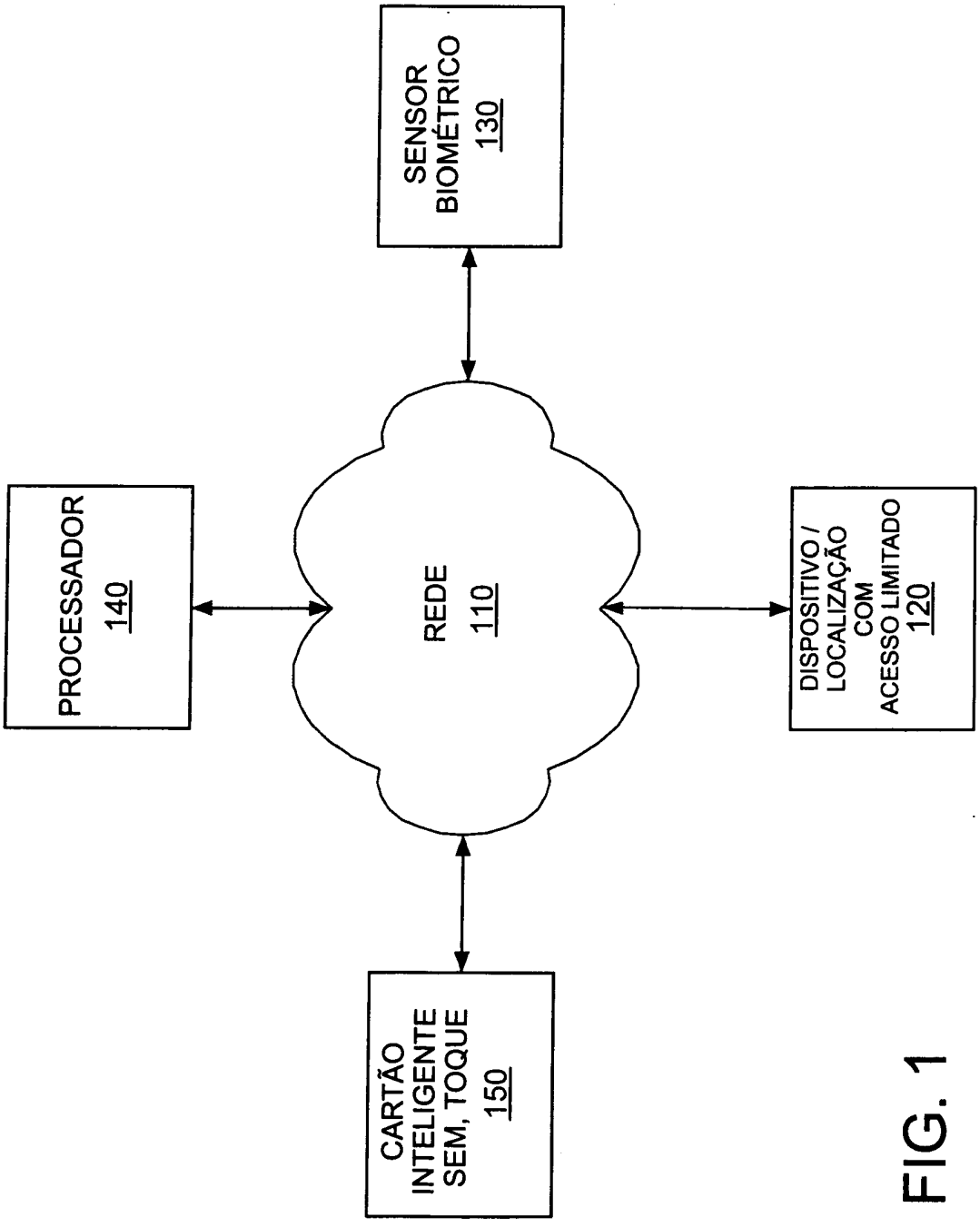
SENSOR BIOMÉTRICO 130
PROCESSADOR 140
REDE 110
DISPOSITIVO / LOCALIZAÇÃO COM ACESSO LIMITADO 120
CARTÃO INTELIGENTE SEM, TOQUE 150

FIG. 1

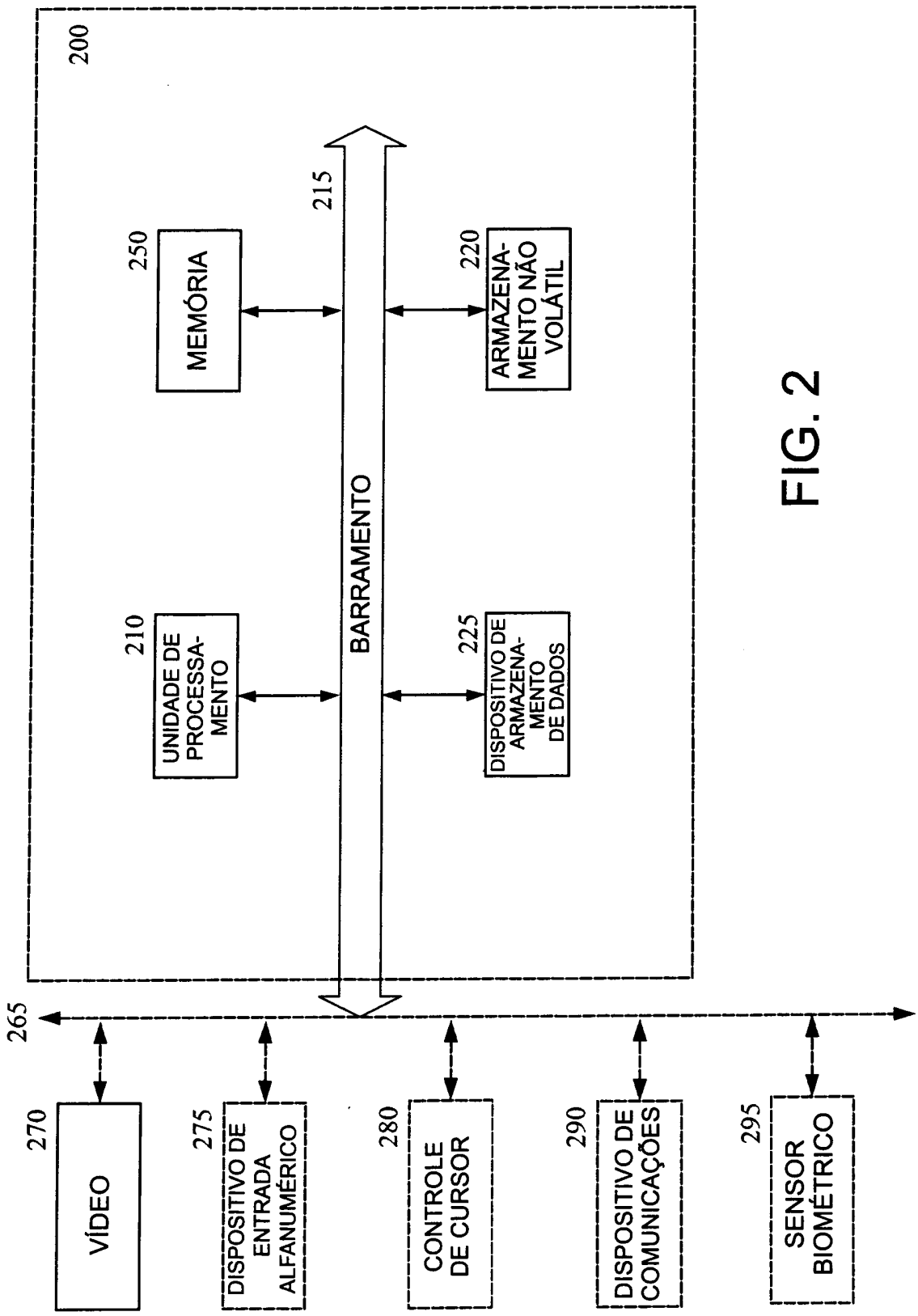
200
215
250
MEMÓRIA
220
ARMAZENA-MENTO NÃO VOLÁTIL
210
UNIDADE DE PROCESSA-MENTO
BARRAMENTO
225
DISPOSITIVO DE ARMAZENA-MENTO DE DADOS
265
270
VÍDEO
275
DISPOSITIVO DE ENTRADA ALFANUMÉRICO
280
CONTROLE DE CURSOR
290
DISPOSITIVO DE COMUNICAÇÕES
295
SENSOR BIOMÉTRICO

FIG. 2

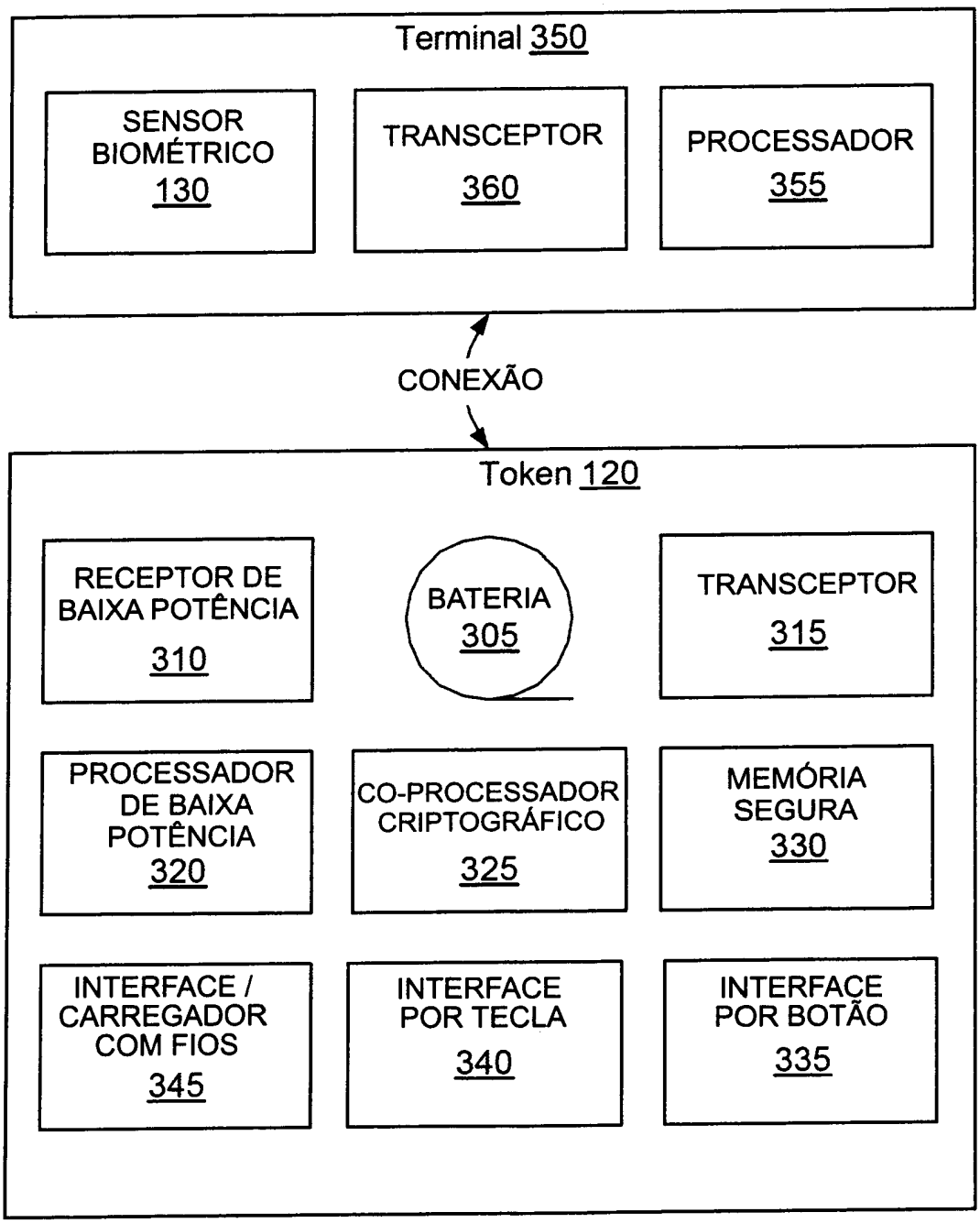
Terminal 350
SENSOR BIOMÉTRICO 130
TRANSCEPTOR 360
PROCESSADOR 355
CONEXÃO
Token 120
RECEPTOR DE BAIXA POTÊNCIA 310
BATERIA 305
TRANSCEPTOR 315
PROCESSADOR DE BAIXA POTÊNCIA 320
CO-PROCESSADOR CRIPTOGRÁFICO 325
MEMÓRIA SEGURA 330
INTERFACE / CARREGADOR COM FIOS 345
INTERFACE POR TECLA 340
INTERFACE POR BOTÃO 335

FIG. 3

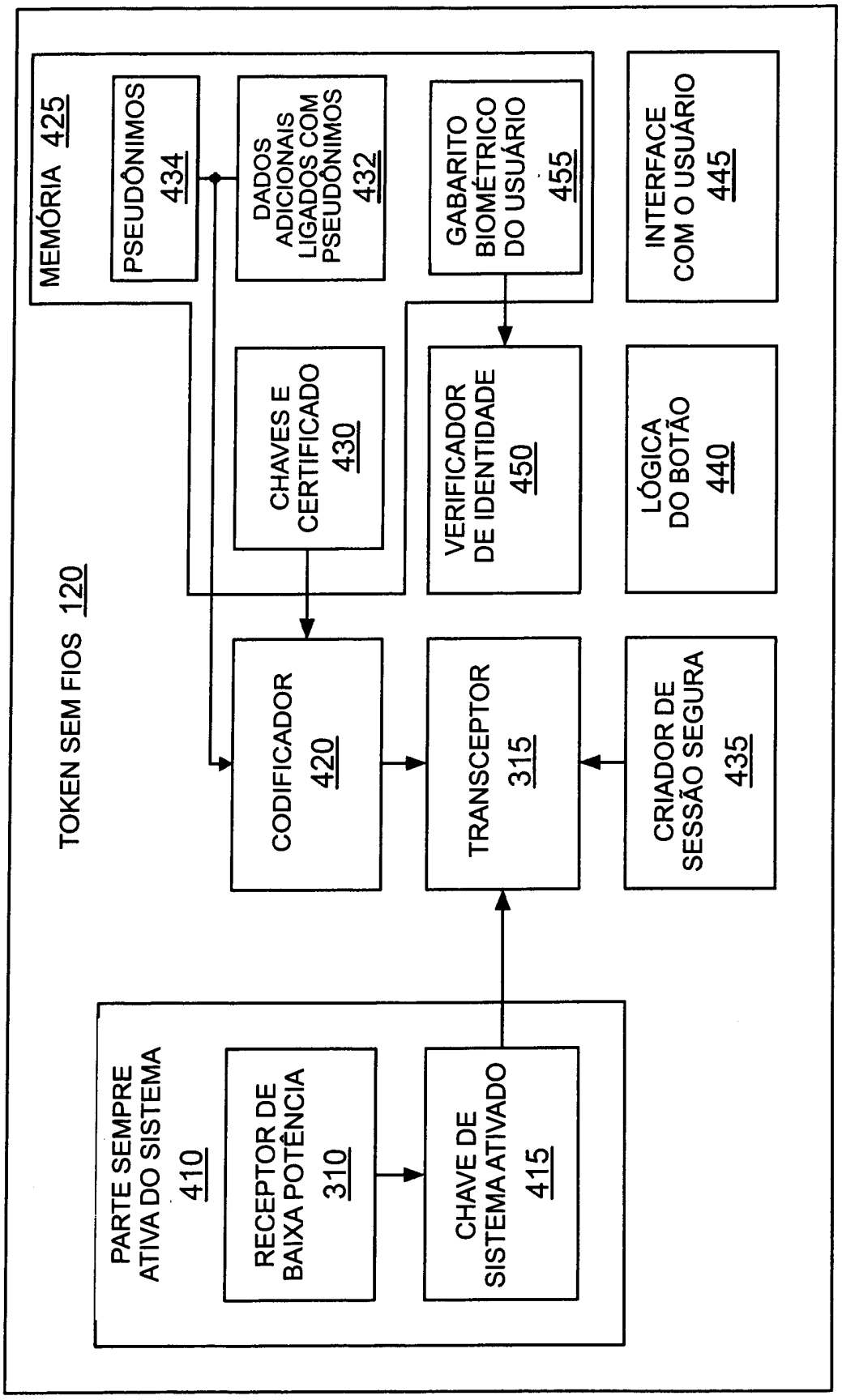
TOKEN SEM FIOS 120
MEMÓRIA 425
PSEUDÔNIMOS 434
DADOS ADICIONAIS LIGADOS COM PSEUDÔNIMOS 432
GABARITO BIOMÉTRICO DO USUÁRIO 455
INTERFACE COM O USUÁRIO 445
CHAVES E CERTIFICADO 430
VERIFICADOR DE IDENTIDADE 450
LÓGICA DO BOTÃO 440
CODIFICADOR 420
TRANSCEPTOR 315
CRIADOR DE SESSÃO SEGURA 435
PARTE SEMPRE ATIVA DO SISTEMA 410
RECEPTOR DE BAIXA POTÊNCIA 310
CHAVE DE SISTEMA ATIVADO 415

FIG. 4A

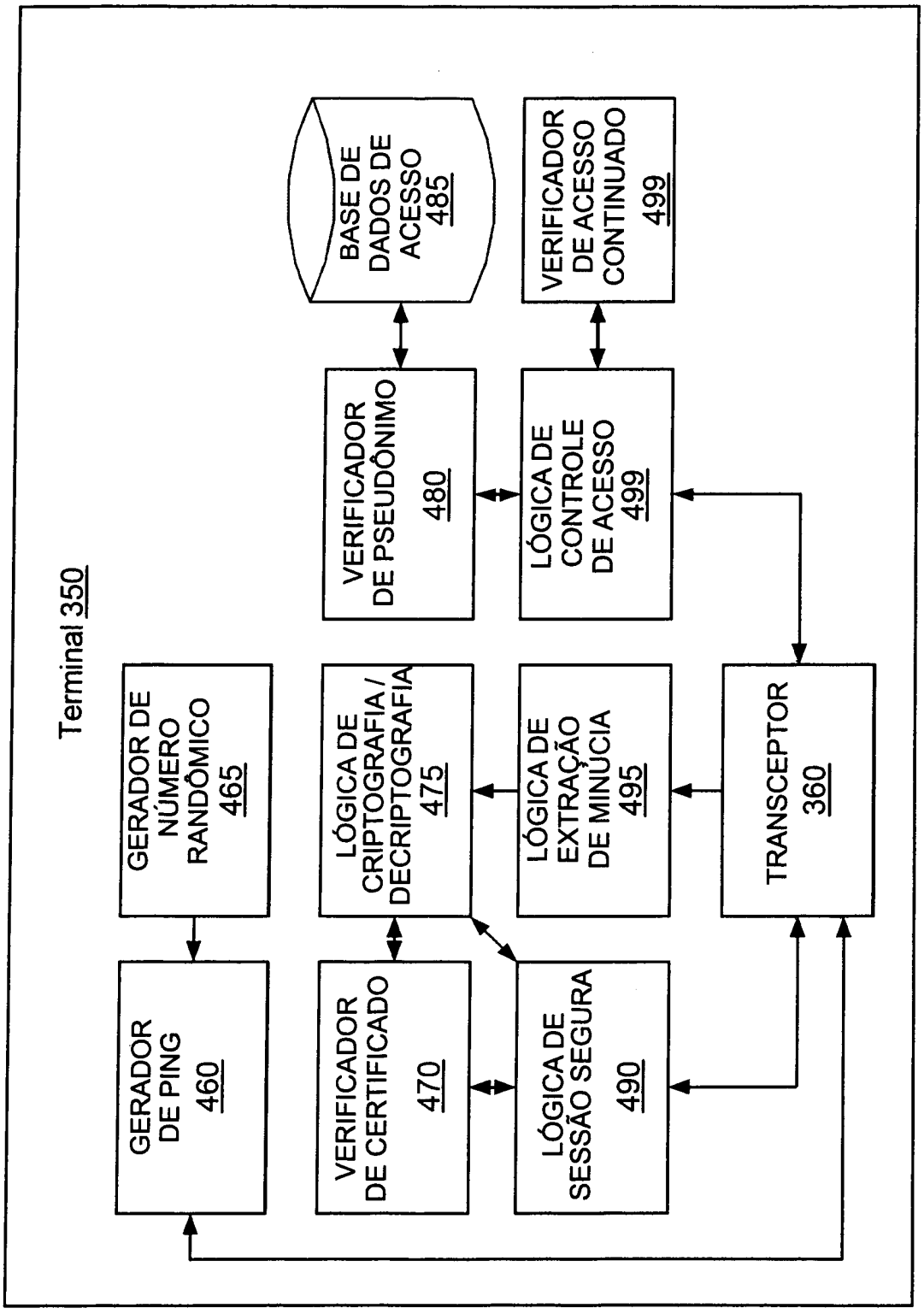
Terminal 350
GERADOR DE NÚMERO RANDÔMICO 465
GERADOR DE PING 460
LÓGICA DE CRIPTOGRAFIA / DECRIPTOGRAFIA 475
VERIFICADOR DE CERTIFICADO 470
LÓGICA DE EXTRAÇÃO DE MINÚCIA 495
LÓGICA DE SESSÃO SEGURA 490
TRANSCEPTOR 360
VERIFICADOR DE PSEUDÔNIMO 480
LÓGICA DE CONTROLE DE ACESSO 499
BASE DE DADOS DE ACESSO 485
VERIFICADOR DE ACESSO CONTINUADO 499

FIG. 4B

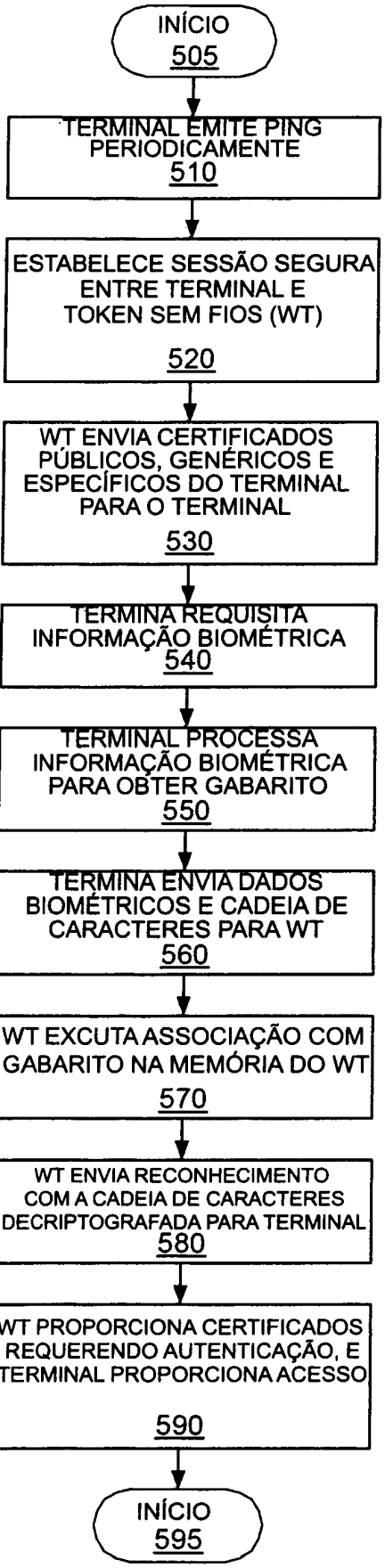
INÍCIO
505
TERMINAL EMITE PING PERIODICAMENTE
510
ESTABELECE SESSÃO SEGURA ENTRE TERMINAL E TOKEN SEM FIOS (WT)
520
WT ENVIA CERTIFICADOS PÚBLICOS, GENÉRICOS E ESPECÍFICOS DO TERMINAL PARA O TERMINAL
530
TERMINA REQUISITA INFORMAÇÃO BIOMÉTRICA
540
TERMINAL PROCESSA INFORMAÇÃO BIOMÉTRICA PARA OBTER GABARITO
550
TERMINA ENVIA DADOS BIOMÉTRICOS E CADEIA DE CARACTERES PARA WT
560
WT EXCUTA ASSOCIAÇÃO COM GABARITO NA MEMÓRIA DO WT
570
WT ENVIA RECONHECIMENTO COM A CADEIA DE CARACTERES DECRIPTOGRAFADA PARA TERMINAL
580
WT PROPORCIONA CERTIFICADOS REQUERENDO AUTENTICAÇÃO, E TERMINAL PROPORCIONA ACESSO
590
INÍCIO
595

FIG. 5

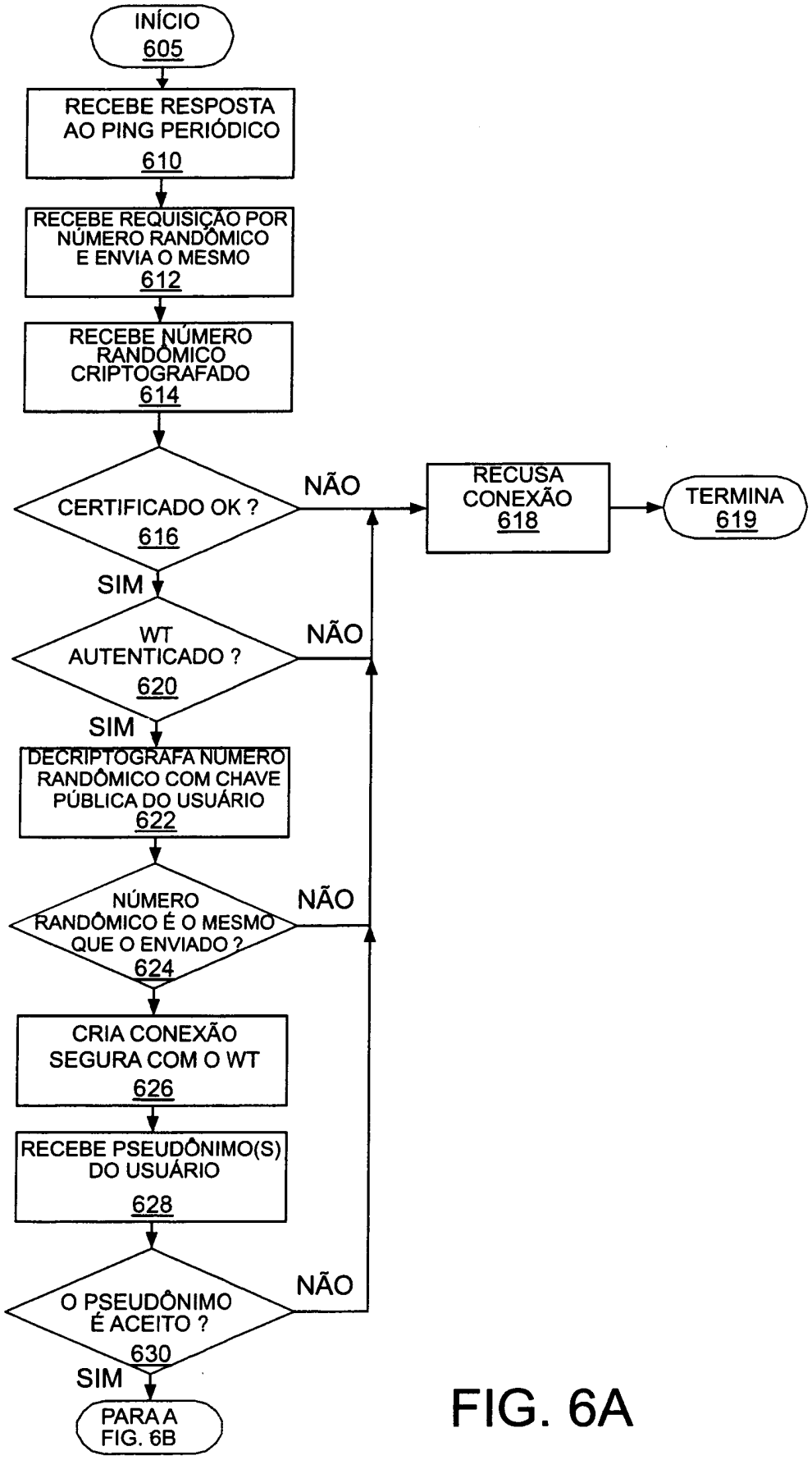
INÍCIO
605
RECEBE RESPOSTA AO PING PERIÓDICO
610
RECEBE REQUISIÇÃO POR NÚMERO RANDÔMICO E ENVIA O MESMO
612
RECEBE NÚMERO RANDÔMICO CRIPTOGRAFADO
614
CERTIFICADO OK ?
616
NÃO
RECUSA CONEXÃO
618
TERMINA
619
SIM
WT AUTENTICADO ?
620
NÃO
SIM
DECRIPTOGRAFA NÚMERO RANDÔMICO COM CHAVE PÚBLICA DO USUÁRIO
622
NÚMERO RANDÔMICO É O MESMO QUE O ENVIADO ?
624
NÃO
CRIA CONEXÃO SEGURA COM O WT
626
RECEBE PSEUDÔNIMO(S) DO USUÁRIO
628
O PSEUDÔNIMO É ACEITO ?
630
NÃO
SIM
PARA A FIG. 6B

FIG. 6A

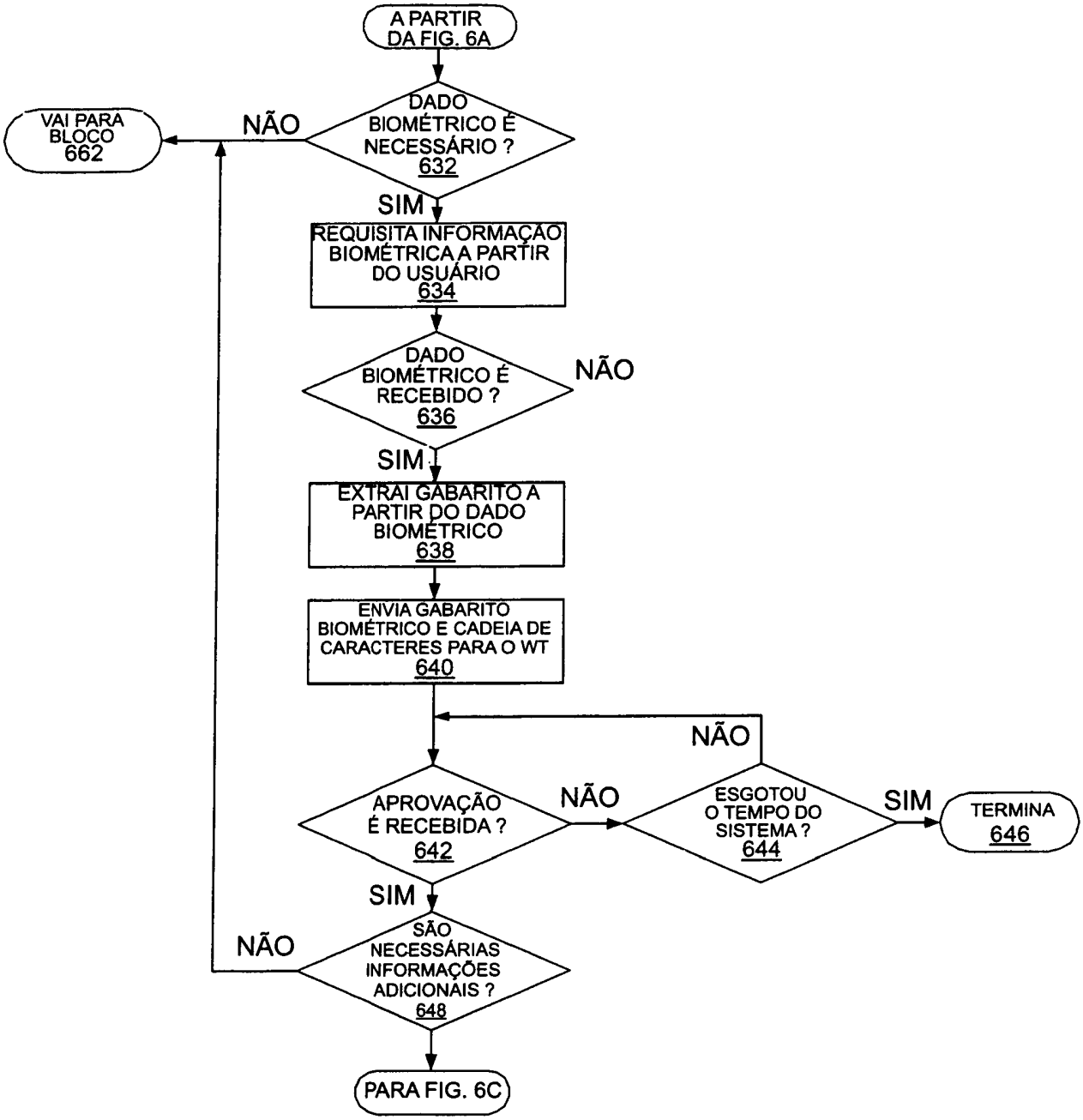
A PARTIR DA FIG. 6A
DADO BIOMÉTRICO É NECESSÁRIO ? 632
NÃO
VAI PARA BLOCO 662
SIM
REQUISITA INFORMAÇÃO BIOMÉTRICA A PARTIR DO USUÁRIO 634
DADO BIOMÉTRICO É RECEBIDO ? 636
NÃO
SIM
EXTRAI GABARITO A PARTIR DO DADO BIOMÉTRICO 638
ENVIA GABARITO BIOMÉTRICO E CADEIA DE CARACTERES PARA O WT 640
NÃO
APROVAÇÃO É RECEBIDA ? 642
NÃO
ESGOTOU O TEMPO DO SISTEMA ? 644
SIM
TERMINA 646
SIM
SÃO NECESSÁRIAS INFORMAÇÕES ADICIONAIS ? 648
NÃO
PARA FIG. 6C

FIG. 6B

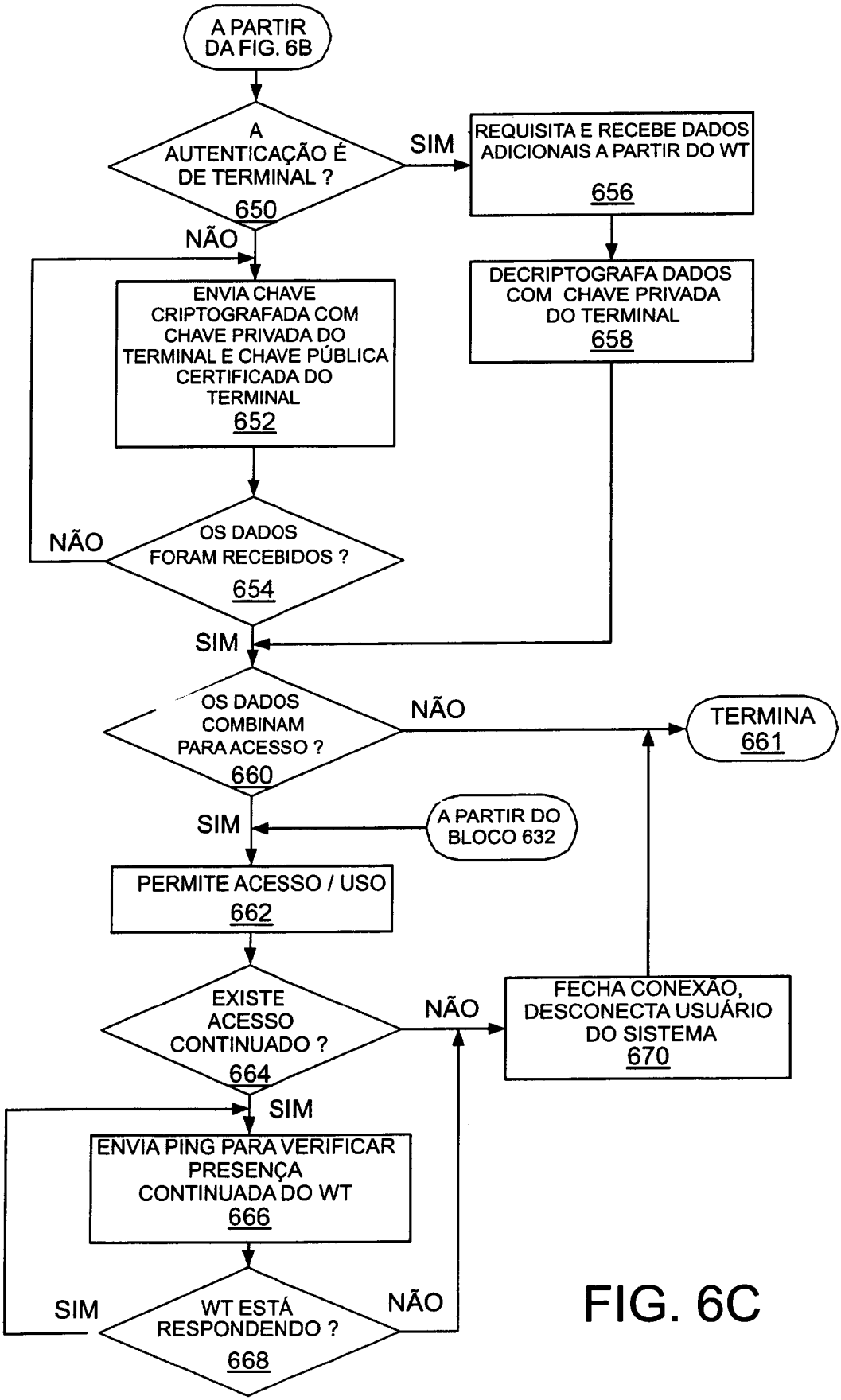
A PARTIR DA FIG. 6B
A AUTENTICAÇÃO É DE TERMINAL ?
650
SIM
REQUISITA E RECEBE DADOS ADICIONAIS A PARTIR DO WT
656
NÃO
DECRIPTOGRAFA DADOS COM CHAVE PRIVADA DO TERMINAL
658
ENVIA CHAVE CRIPTOGRAFADA COM CHAVE PRIVADA DO TERMINAL E CHAVE PÚBLICA CERTIFICADA DO TERMINAL
652
NÃO
OS DADOS FORAM RECEBIDOS ?
654
SIM
OS DADOS COMBINAM PARA ACESSO ?
660
NÃO
TERMINA
661
SIM
A PARTIR DO BLOCO 632
PERMITE ACESSO / USO
662
EXISTE ACESSO CONTINUADO ?
664
NÃO
FECHA CONEXÃO, DESCONECTA USUÁRIO DO SISTEMA
670
SIM
ENVIA PING PARA VERIFICAR PRESENÇA CONTINUADA DO WT
666
SIM
WT ESTÁ RESPONDENDO ?
668
NÃO

FIG. 6C

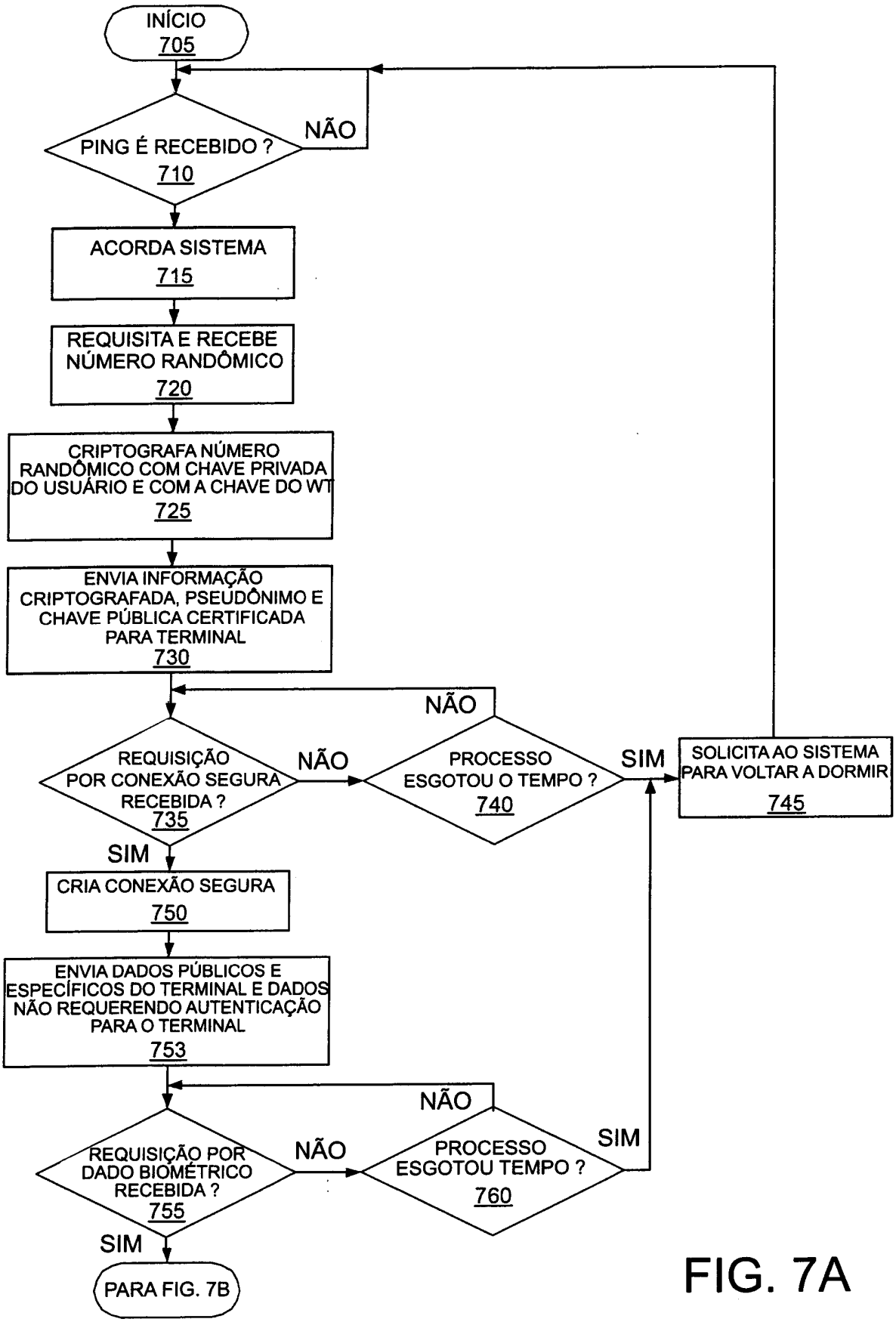
INÍCIO
705
PING É RECEBIDO ?
710
NÃO
ACORDA SISTEMA
715
REQUISITA E RECEBE NÚMERO RANDÔMICO
720
CRIPTOGRAFA NÚMERO RANDÔMICO COM CHAVE PRIVADA DO USUÁRIO E COM A CHAVE DO WT
725
ENVIA INFORMAÇÃO CRIPTOGRAFADA, PSEUDÔNIMO E CHAVE PÚBLICA CERTIFICADA PARA TERMINAL
730
NÃO
REQUISIÇÃO POR CONEXÃO SEGURA RECEBIDA ?
735
NÃO
PROCESSO ESGOTOU O TEMPO ?
740
SIM
SOLICITA AO SISTEMA PARA VOLTAR A DORMIR
745
SIM
CRIA CONEXÃO SEGURA
750
ENVIA DADOS PÚBLICOS E ESPECÍFICOS DO TERMINAL E DADOS NÃO REQUERENDO AUTENTICAÇÃO PARA O TERMINAL
753
NÃO
REQUISIÇÃO POR DADO BIOMÉTRICO RECEBIDA ?
755
NÃO
PROCESSO ESGOTOU TEMPO ?
760
SIM
SIM
PARA FIG. 7B

FIG. 7A

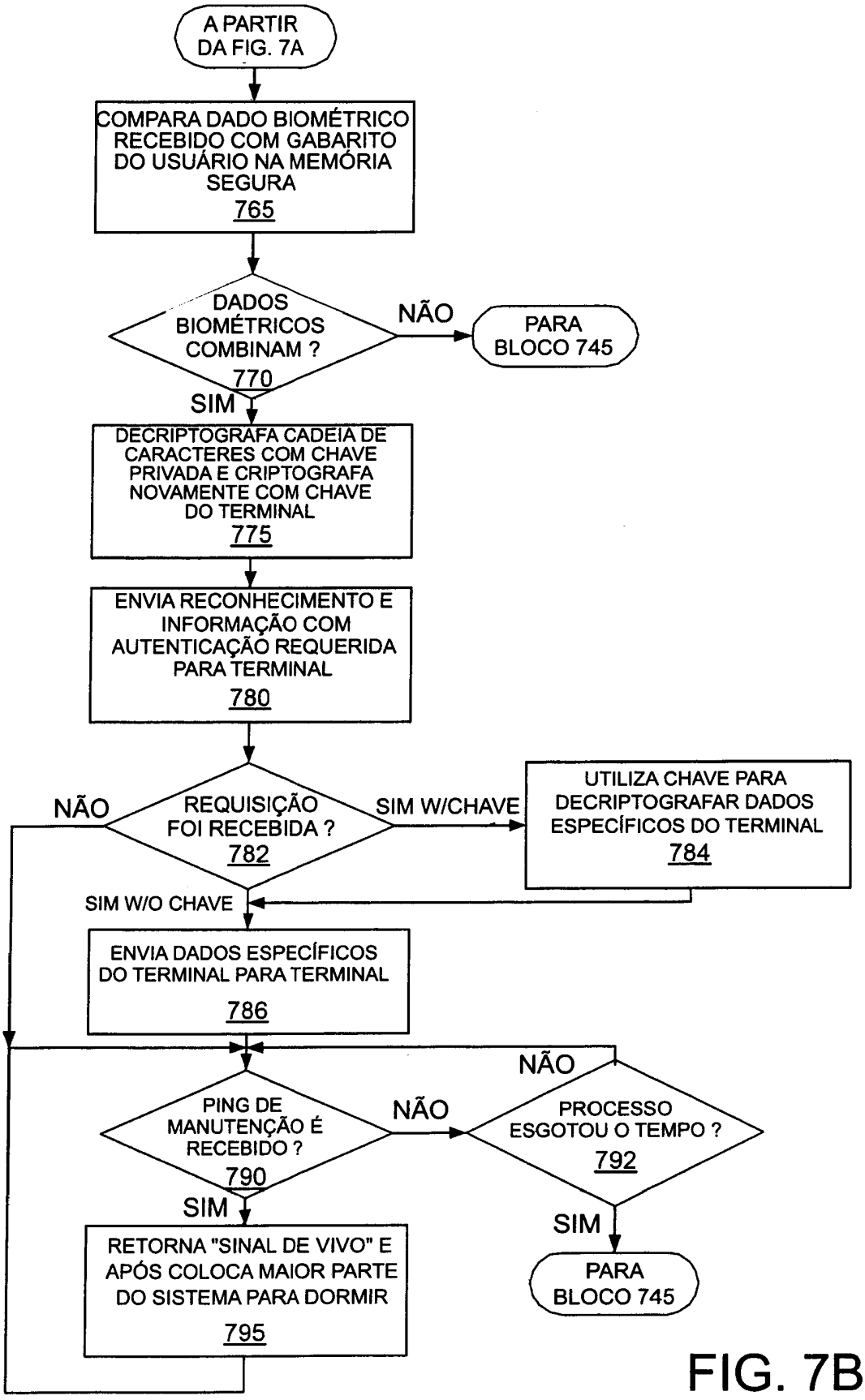
A PARTIR DA FIG. 7A
COMPARA DADO BIOMÉTRICO RECEBIDO COM GABARITO DO USUÁRIO NA MEMÓRIA SEGURA
765
DADOS BIOMÉTRICOS COMBINAM ?
770
NÃO
PARA BLOCO 745
SIM
DECRIPTOGRAFA CADEIA DE CARACTERES COM CHAVE PRIVADA E CRIPTOGRAFA NOVAMENTE COM CHAVE DO TERMINAL
775
ENVIA RECONHECIMENTO E INFORMAÇÃO COM AUTENTICAÇÃO REQUERIDA PARA TERMINAL
780
NÃO
REQUISIÇÃO FOI RECEBIDA ?
782
SIM W/CHAVE
UTILIZA CHAVE PARA DECRIPTOGRAFAR DADOS ESPECÍFICOS DO TERMINAL
784
SIM W/O CHAVE
ENVIA DADOS ESPECÍFICOS DO TERMINAL PARA TERMINAL
786
NÃO
PING DE MANUTENÇÃO É RECEBIDO ?
790
NÃO
PROCESSO ESGOTOU O TEMPO ?
792
SIM
RETORNA "SINAL DE VIVO" E APÓS COLOCA MAIOR PARTE DO SISTEMA PARA DORMIR
795
SIM
PARA BLOCO 745

FIG. 7B

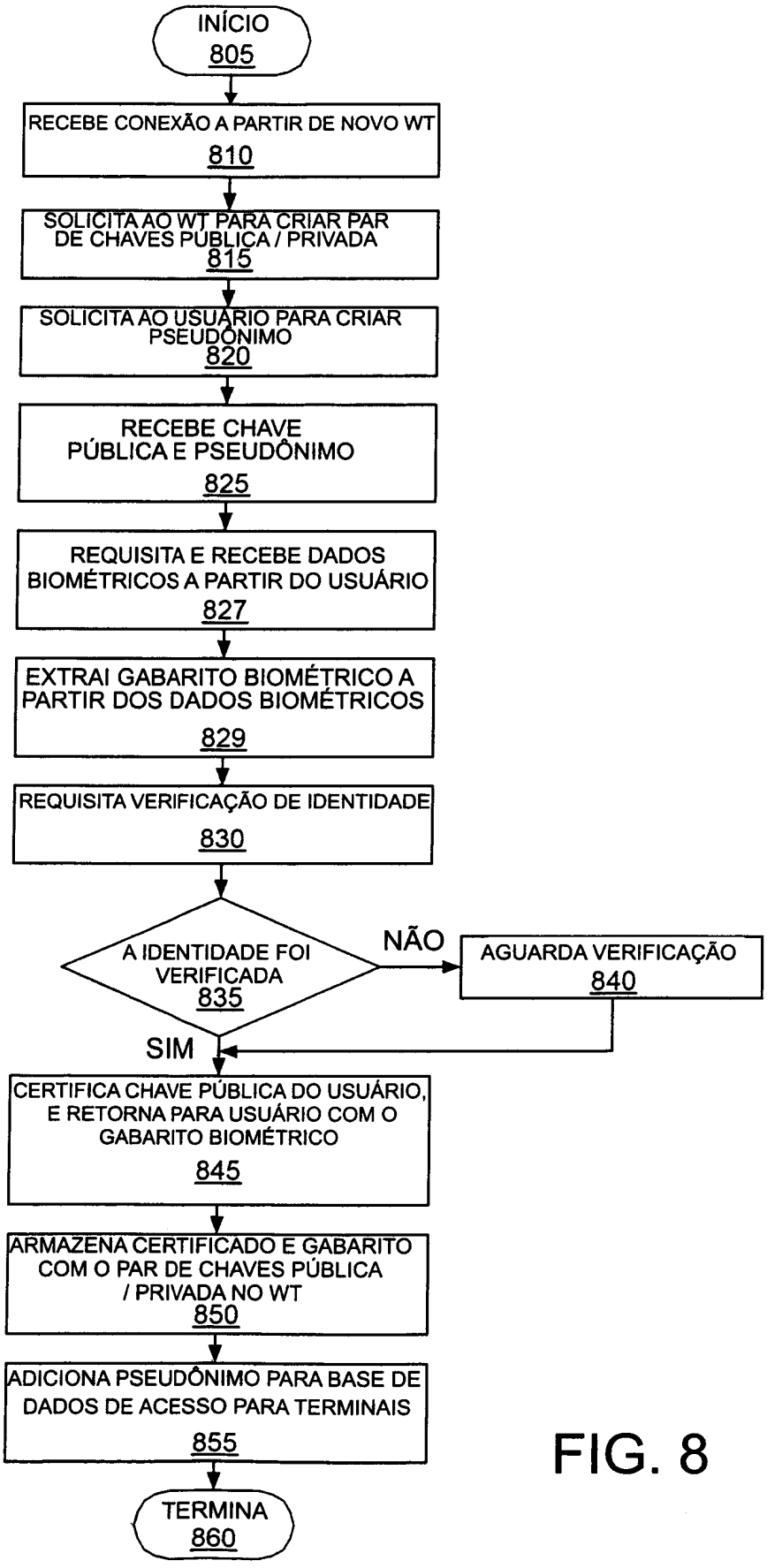
INÍCIO
805
RECEBE CONEXÃO A PARTIR DE NOVO WT
810
SOLICITA AO WT PARA CRIAR PAR DE CHAVES PÚBLICA / PRIVADA
815
SOLICITA AO USUÁRIO PARA CRIAR PSEUDÔNIMO
820
RECEBE CHAVE PÚBLICA E PSEUDÔNIMO
825
REQUISITA E RECEBE DADOS BIOMÉTRICOS A PARTIR DO USUÁRIO
827
EXTRAI GABARITO BIOMÉTRICO A PARTIR DOS DADOS BIOMÉTRICOS
829
REQUISITA VERIFICAÇÃO DE IDENTIDADE
830
A IDENTIDADE FOI VERIFICADA
835
NÃO
AGUARDA VERIFICAÇÃO
840
SIM
CERTIFICA CHAVE PÚBLICA DO USUÁRIO, E RETORNA PARA USUÁRIO COM O GABARITO BIOMÉTRICO
845
ARMAZENA CERTIFICADO E GABARITO COM O PAR DE CHAVES PÚBLICA / PRIVADA NO WT
850
ADICIONA PSEUDÔNIMO PARA BASE DE DADOS DE ACESSO PARA TERMINAIS
855
TERMINA
860

FIG. 8

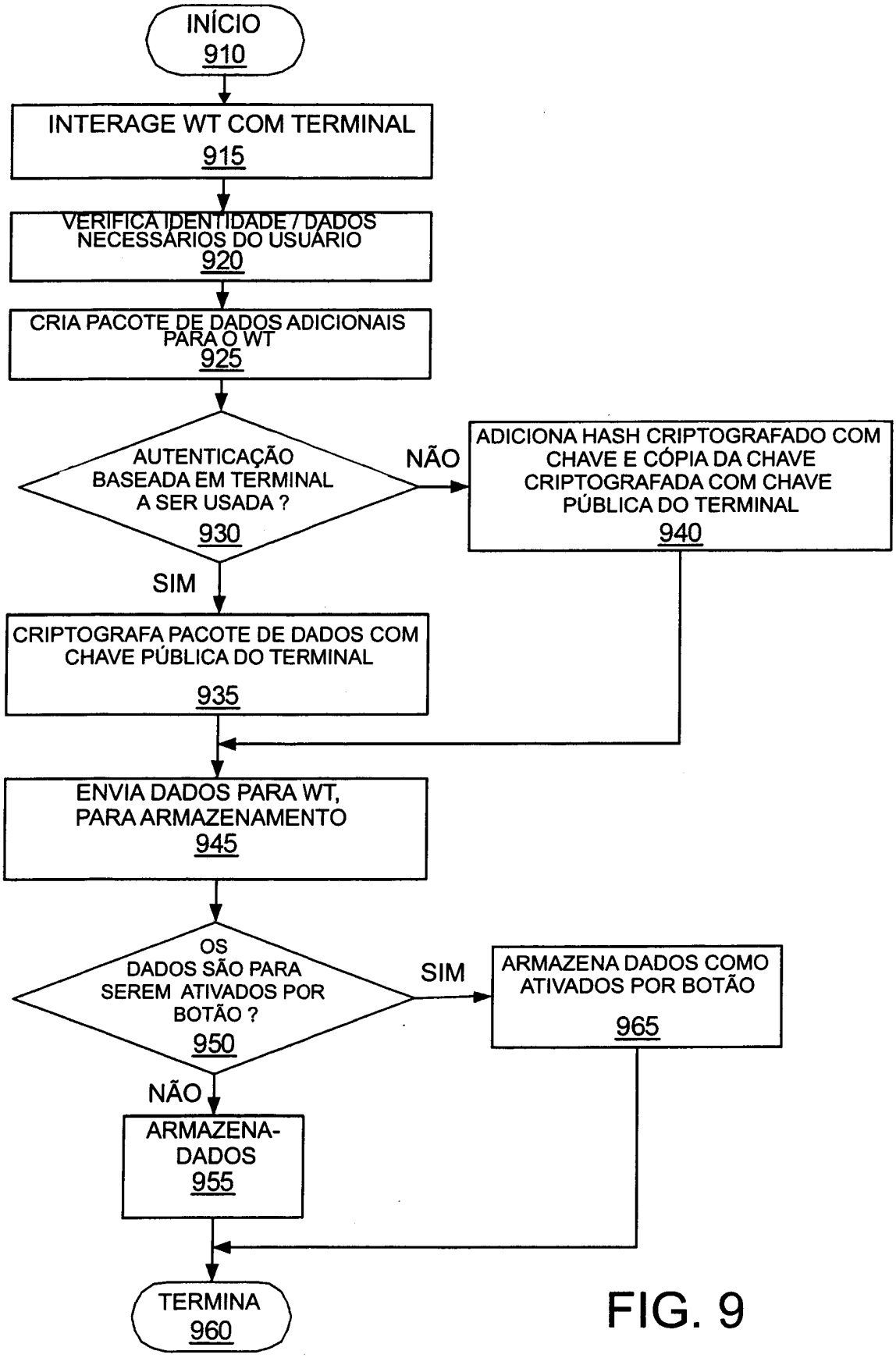
INÍCIO
910
INTERAGE WT COM TERMINAL
915
VERIFICA IDENTIDADE / DADOS NECESSÁRIOS DO USUÁRIO
920
CRIA PACOTE DE DADOS ADICIONAIS PARA O WT
925
AUTENTICAÇÃO BASEADA EM TERMINAL A SER USADA ?
930
NÃO
ADICIONA HASH CRIPTOGRAFADO COM CHAVE E CÓPIA DA CHAVE CRIPTOGRAFADA COM CHAVE PÚBLICA DO TERMINAL
940
SIM
CRIPTOGRAFA PACOTE DE DADOS COM CHAVE PÚBLICA DO TERMINAL
935
ENVIA DADOS PARA WT, PARA ARMAZENAMENTO
945
OS DADOS SÃO PARA SEREM ATIVADOS POR BOTÃO ?
950
SIM
ARMAZENA DADOS COMO ATIVADOS POR BOTÃO
965
NÃO
ARMAZENA-DADOS
955
TERMINA
960

FIG. 9

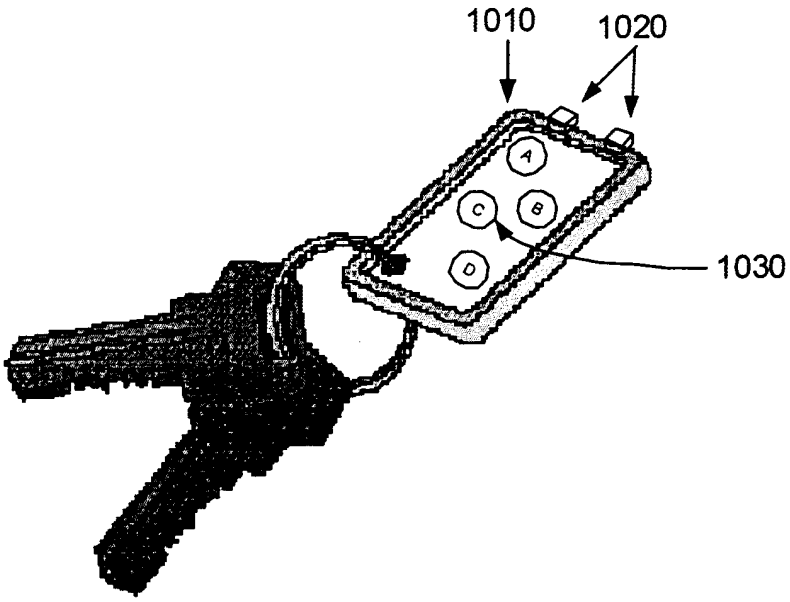


FIG. 10A

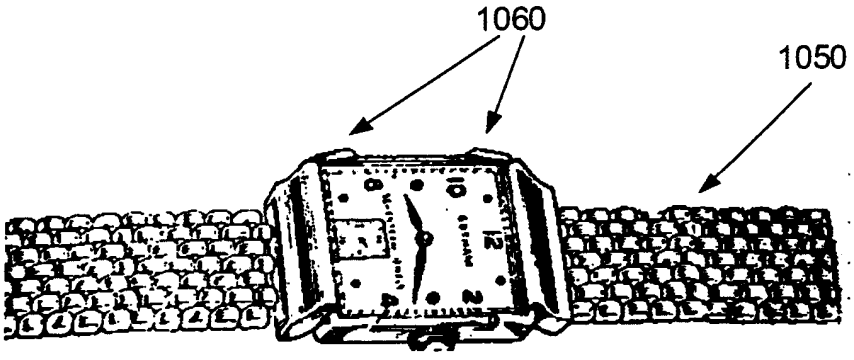


FIG. 10B