

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

(21) **PI0709392-6 A2**



(22) Data de Depósito: 14/03/2007
(43) Data da Publicação: 05/07/2011
(RPI 2113)

(51) *Int.Cl.:*
G06K 5/00 2006.01

(54) Título: **MÉTODO E APARELHO PARA PROPORCIONAR AUTENTICAÇÃO UTILIZANDO UM CARTÃO DE AUTENTICAÇÃO**

(30) Prioridade Unionista: 14/03/2006 US 11/376,678

(73) Titular(es): Verisign, INC.

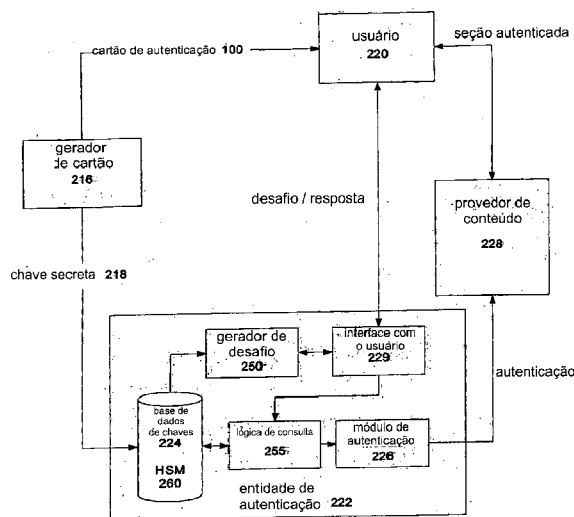
(72) Inventor(es): Davi M Raihi

(74) Procurador(es): Dannemann, Siemsen, Bigler & Ipanema Moreira

(86) Pedido Internacional: PCT US2007006549 de 14/03/2007

(87) Publicação Internacional: WO 2007/106566 de 20/09/2007

(57) **Resumo:** MÉTODO E APARELHO PARA PROPORCIONAR AUTENTICAÇÃO UTILIZANDO UM CARTÃO DE AUTENTICAÇÃO. A presente invenção refere-se a um método e a um aparelho para proporcionar autenticação. O método compreende enviar um desafio para um usuário a ser autenticado, o desafio incluindo uma referência em um cartão emitido para o usuário e receber um valor fornecido pelo usuário suposto pelo usuário como estando associado com a referência no cartão emitido para o usuário. O método adicionalmente compreende acessar uma chave secreta associada com o cartão emitido para o usuário e gerar uma senha utilizando uma função F da chave secreta e a referência. O método adicionalmente compreendendo mapear a função F para um valor em um alfabeto e autenticar o usuário por comparar o valor no alfabeto com o valor fornecido pelo usuário.



Relatório Descritivo da Patente de Invenção para "**MÉTODO E APARELHO PARA PROPORCIONAR AUTENTICAÇÃO UTILIZANDO UM CARTÃO DE AUTENTICAÇÃO**".

AVISO DE DIREITO AUTURAL

5 Neste documento está contido um material que está sujeito à proteção de direito autoral. O proprietário do direito autoral não tem objeção quanto à reprodução fac-símile da revelação de patente por qualquer pessoa, à medida que ela apareça nos arquivos ou registros de patente do Patent and Trademark Office, mas de outra forma reserva todos os direitos de direito autoral, quaisquer que sejam.

ANTECEDENTES

Campo

As concretizações da presente invenção se relacionam em geral com o campo de autenticação. Mais particularmente, as concretizações da presente invenção se relacionam com um segundo fator utilizado para autenticação.

Descrição da Técnica Relacionada

Autenticação é o processo para determinar se alguém ou alguma coisa é, na verdade, quem ou o que ele se declara como sendo. Nas redes de computadores privadas e públicas (incluindo a Internet), a autenticação normalmente é feita através do uso de senhas de conexão. O conhecimento da senha é assumido para garantir que o usuário é autêntico. Cada usuário se registra inicialmente utilizando uma senha designada ou autodeclarada. Em cada uso subsequente, o usuário deve conhecer e utilizar a senha anteriormente declarada. A senha é considerada um primeiro fator, porque ela é alguma coisa que o usuário sabe que presumidamente ninguém mais conhece.

Desde que as senhas são vulneráveis aos hackers talentosos, mais segurança pode ser proporcionada pela adição de um segundo fator para a autenticação. O segundo fator geralmente é alguma coisa que o usuário possui (oposto a alguma coisa que o usuário conhece). Segundos fatores comuns são cartões de crédito, teclas inteligentes, e outros objetos simi-

lares. Um segundo fator contendo somente um pedaço de informação é relativamente vulnerável. O que é necessário é um segundo fator contendo informação que possa ser gerada sistematicamente e verificada de forma eficiente ao mesmo tempo em que não consumindo memória excessiva na autoridade de autenticação.

BREVE DESCRIÇÃO DOS DESENHOS

As concretizações da presente invenção são ilustradas a título de exemplo, e não a título de limitação, nas figuras dos desenhos acompanhantes e nos quais números de referência iguais se referem a elementos similares, e nos quais:

a Figura 1A é um diagrama de blocos ilustrando um cartão de autenticação de acordo com uma concretização da presente invenção;

a Figura 1B é um diagrama de bloco ilustrando um cartão de autenticação de acordo com outra concretização da presente invenção;

a Figura 2 é um fluxograma ilustrando a otimização de uma busca antecipada ("prefetch") da técnica anterior, incluindo o cálculo estático de distância de busca antecipada;

a Figura 3 é um fluxograma ilustrando o processamento de autenticação de acordo com uma concretização da presente invenção;

a Figura 4A é um fluxograma ilustrando o processamento de autenticação de acordo com a outra concretização da presente invenção;

a Figura 4B é um fluxograma continuando a ilustração do processamento de autenticação de acordo com uma concretização da presente invenção; e

a Figura 5 é um diagrama de blocos ilustrando um sistema de computador ilustrativo de acordo com uma concretização da presente invenção.

DESCRIÇÃO DETALHADA

Cartão de Autenticação

Uma concretização da invenção proporciona um cartão de autenticação como um segundo fator para autenticação. Uma concretização de tal cartão de autenticação é agora descrita com referência à Figura 1A. Em

uma concretização, o cartão de autenticação 100 pode ser um cartão de plástico no formato de um cartão de crédito ou em outro formato similar, que encaixa dentro da maioria das carteiras. Em outras concretizações, o cartão de autenticação pode ser fabricado de papel, de cartolina, de metal, ou de qualquer outro material adequado.

Em uma concretização, o cartão está de forma única associado com um número do cartão 112. Por exemplo, o número do cartão 112 para o cartão de autenticação 100 na Figura 1A é 4536 3657 2352 7658. Em uma concretização, os números no cartão podem incluir o próprio número do cartão (para propósitos de identificação) e o método de cálculo. Por exemplo, o número do cartão pode ser 45 36 3657 2352 7658 A1. O número 4536 3657 2352 7658 é um número do cartão para identificação, enquanto o A1 indica um método de cálculo. Vários métodos de cálculo podem ser utilizados, como é descrito em mais detalhes abaixo. Em uma concretização, o cartão de autenticação 100 também inclui um conjunto de pares de referência/valor. Um par de referência/valor descreve uma referência e um valor associado com a referência. Por exemplo, o cartão de autenticação 100 na Figura 1A possui doze pares de referência/valor, listados em ordem a partir de cima até embaixo em três colunas. A referência um possui o valor F, a referência dois possui o valor Q, e assim por diante, até a referência doze que possui o valor L. Enquanto as Figuras apresentam a matriz e o número do cartão no mesmo lado, obviamente, eles podem estar em lados opostos. Em uma concretização, um lado pode incluir o número do cartão e a informação de atribuição de marca, enquanto o outro inclui a matriz. Em uma concretização, ambos os lados podem incluir partes da matriz e/ou da informação do cartão. A distribuição de informação no próprio cartão pode ser variada sem afetar a invenção subjacente.

Os pares de referência/valor podem ser representados de vários modos no cartão de autenticação 100. Outro modo de representar os pares de referência/valor é apresentado na Figura 1B. Na Figura 1B, cada referência é uma célula em uma grade, representada por sua coordenada (fileira, coluna). Por exemplo, na Figura 1B, a referência (1, 1) possui o valor F, a

referência (2, 1) possui o valor Q, e assim por diante até a referência (4, 3) que possui um valor L. Existem vários outros modos de representar os pares de referência/valor incluindo uma lista ou uma série de dispositivos gráficos, tal como codificação de cor, codificação de formato, e assim por diante. O conceito de um par de referência/valor, o qual é uma referência e um valor associado com a referência, permanece constante independente da representação física.

Em uma concretização, os cartões de autenticação emitidos por uma entidade (tal como um banco ou outra organização que deseja autenticar o usuário), todos possuem o mesmo número de referências e valores associados. Por exemplo, os cartões de autenticação 100 nas Figuras 1A e 1B possuem doze referências. Em outras concretizações, os cartões podem ter um número variável de referências.

Em uma concretização, os valores associados com as referências são gerados metodicamente. Em uma concretização, uma chave secreta associada com o cartão é utilizada para gerar valores para os números de referência. Em tal concretização, quando o cartão está sendo produzido, uma chave secreta é gerada e associada com o cartão. Esta associação pode ser armazenada utilizando o número do cartão 112 associado com o número do cartão 100.

Em uma concretização, o valor associado com cada referência é gerado pela execução de uma operação unidirecional (por exemplo, uma função hash unidirecional tal como MD5 ou SHA-1) em uma combinação da chave secreta com a referência. Em uma concretização, a função unidirecional utilizada é o algoritmo de Senha Casual Baseada em Hash (HOTP), um algoritmo publicamente disponível publicado por uma Iniciativa Aberta Para Autenticação (OATH). Veja o Internet Engineering Task Force (IETF) HMAC OTP Draft 4, disponível em <http://www.openauthentication.com>. Por exemplo, usando o cartão de autenticação 100 na Figura 1A, o valor associado com a referência 6 seria HOTP (K, 6), onde K é a chave secreta e os argumentos da função hash são concatenados. No exemplo da Figura 1A, o hash resultante seria mapeado para um alfabeto resultando em "I".

O algoritmo HOTP resulta em um código de 6 dígitos, e assim está apto a suportar qualquer alfabeto com até 999.999 "letras" ou membros. Outras funções unidirecionais podem suportar alfabetos maiores ou menores. Nos exemplos apresentados nas Figuras 1A e 1B, um alfabeto padrão de A até Z é apresentado. Entretanto, qualquer alfabeto poderia ser utilizado, incluindo caracteres, números hexadecimais e decimais, ou quaisquer outros símbolos. Em uma concretização, todos os valores possíveis no alfabeto utilizado podem ser representados utilizando um teclado padrão QWERTY.

Outro exemplo da utilização do algoritmo HOTP para gerar pares de referência/valor é agora dado com referência à Figura 1B. As coordenadas x-y de uma célula podem ser combinadas com a chave secreta para fornecer o valor. Por exemplo, a célula (2, 3) pode ser mapeada como um HOTP (K, 23). Neste exemplo, as coordenadas x-y são simplesmente concatenadas, o que produz uma referência única para cada célula. As coordenadas x-y podem ser combinadas de algum outro modo, tal como por multiplicação, apesar de que a multiplicação em particular não irá produzir referências únicas.

Sistema de Autenticação

Com o entendimento de algumas concretizações de um cartão de autenticação 100, uma concretização de um sistema de autenticação utilizando o cartão de autenticação 100 é agora descrita com referência à Figura 2. A Figura 2 apresenta um gerador de cartão 216 que gera o cartão de autenticação 100 utilizando a chave secreta 218. O gerador de cartão 216 pode ser uma entidade ou companhia separada especializada em autenticação ou em impressão ou prensa de cartão. O gerador de cartão 216 pode ele próprio gerar a chave secreta 218, ou pode receber a chave secreta 218 a partir de outra entidade.

Em uma concretização, a chave secreta 218 é um número aleatório gerado por um gerador de número aleatório. A chave secreta 218 pode ser criada por qualquer outro dispositivo. Uma característica da chave secreta é que ela não é conhecida por qualquer pessoa fora do gerador de cartão 216. O gerador de cartão 216 proporciona o cartão de autenticação 100 para

um usuário 220 e a chave secreta 218 para uma entidade de autenticação 222. Em uma concretização, a chave secreta 218 pode ser liberada em um meio físico seguro, ou através da transmissão em um canal de comunicação seguro criptografado. O cartão 100 pode primeiro ser proporcionado para um intermediário (tal como um banco que irá emitir o mesmo para um cliente), antes de ficar de posse do usuário 220 que irá utilizar o mesmo para a autenticação.

A entidade de autenticação 222 pode ser a entidade requisitando a autenticação (por exemplo, o banco) ou uma entidade ou companhia especializada em autenticação contratada pela entidade requisitando a autenticação. Em uma concretização, a chave secreta 218 é armazenada em uma base de dados de chaves 224. Em uma concretização, a chave secreta é associada com o número do cartão do cartão de autenticação que ela foi usada para gerar. Por exemplo, a Chave1 foi utilizada pelo gerador de cartão 216 para gerar o cartão com o número de cartão 1234 5678 9101, então um registro na base de dados de chaves 224 irá associar a Chave1 com um número do cartão 1234 5678 9101. Em uma concretização, a base de dados de chave pode ser pesquisada pelo número do cartão. Em uma concretização, para proteger as chaves secretas, a base de dados de chaves é armazenada em um módulo de segurança de hardware (HSM).

A entidade de autenticação 222 também inclui um módulo de autenticação 226. Em uma concretização, a entidade de autenticação 222 cria os desafios apresentados para o usuário 220 e avalia a resposta recebida a partir do usuário 220. O módulo de autenticação 226 pode conter uma interface com o usuário 229 para comunicar os desafios e para receber as respostas a partir do usuário 220. Em outra concretização, uma entidade separada (tal como o banco) faz a interface com o usuário, e envia a resposta ao desafio para a entidade de autenticação 222. Em outras concretizações, uma entidade manipula tanto a interface com o usuário como a autenticação.

Em uma concretização, um gerador de desafio 250 na entidade de autenticação 222 apresenta um desafio para o usuário 220 na forma de

solicitar o valor associado com uma ou mais referências no cartão de autenticação 100 emitido para o usuário. Por exemplo, em uma concretização, em adição à conexão e senha do usuário (primeiro fator), a interface de conexão também irá solicitar os valores associados com três referências aleatoriamente escolhidas. Menos ou mais referências podem ser utilizadas.

Por exemplo, um usuário de posse do cartão de autenticação 100 apresentado na Figura 1A pode ser solicitado para proporcionar os valores das referências 3 e 10. As respostas corretas para este exemplo são P e S. Uma lógica de consulta 255 na entidade de autenticação 220 pode consultar o número do cartão do cartão 100 emitido para o usuário 220 e acessar a base de dados de chaves 224 para acessar a chave secreta ligada com o número do cartão. O módulo de autenticação 226 pode então gerar novamente os valores solicitados no desafio utilizando o algoritmo utilizado para gerar o cartão. Desta maneira, o módulo de autenticação 226 pode verificar a posse do cartão 100 pelo usuário 220 sem estar de posse de todos os pares de referência/valor no cartão 100. Isto permite a proteção de hardware eficiente da informação necessária para verificar o usuário 220.

Se um módulo de autenticação autenticar com sucesso o usuário 220, então o módulo de autenticação 226 pode enviar uma mensagem de autenticação para um provedor de conteúdo 228 que o usuário 220 deseja acessar. Esta comunicação pode ser implementada por um módulo de interface especial do provedor de conteúdo que pode ser separado da interface com o usuário 229. O provedor de conteúdo 228 pode ser um banco, uma companhia de seguro, um provedor de serviço da Internet ou qualquer outro provedor de conteúdo ou de serviço que possua usuários que o provedor de conteúdo 228 deseja autenticar. O provedor de conteúdo 228 pode ser a mesma entidade que a entidade de autenticação 222, se o provedor de conteúdo 228 estiver manipulando a autenticação de forma interna.

Ao receber a autenticação a partir do módulo de autenticação 226, o usuário 220 e o provedor de conteúdo 228 podem se envolver em uma seção autenticada que pode incluir transações bancárias on-line, navegação na Internet, jogos ou qualquer outro conteúdo ou serviço proporciona-

do. Se a autenticação não tiver sucesso, o módulo de autenticação 226 informa ao provedor de conteúdo que a autenticação falhou na mensagem de autenticação. O usuário 220 é então considerado não autenticado, e não será concedido acesso autenticado ao provedor de conteúdo 228.

5 Protocolos de Desafio-Resposta

Uma concretização de um protocolo de desafio-resposta para autenticar um usuário possuindo um cartão de autenticação de segundo fator como descrito acima é agora exposta com referência à Figura 3. O processo descrito com referência à Figura 3 pode ser executado, por exemplo, pela entidade de autenticação 222 na Figura 2.

No bloco 302, um desafio é enviado para um usuário desejando acesso a algum conteúdo ou serviço. O desafio pode ser apresentado junto com uma interface padrão de conexão que solicita um identificador do usuário (ID) ou algum outro nome de conexão e uma senha. Por exemplo, um programa de correio eletrônico tipicamente solicita um endereço de correio eletrônico (por exemplo, joe_smith@company.com) e uma senha.

Em uma concretização, em adição à tela normal de conexão, a conexão também apresenta um desafio para identificar um ou mais valores específicos no cartão de autenticação emitido para o usuário. Os valores podem ser identificados pela referência (tal como um número ou coordenadas de célula) ou de alguma outra maneira. O desafio pode solicitar mais do que um valor, entretanto somente um valor é discutido por simplicidade e facilidade de entendimento. Por exemplo, um desafio solicitando três valores pode solicitar a um usuário um ID do usuário, uma senha, e os valores de referência 4, 9 e 12. Para um usuário de posse do cartão 100 apresentado na Figura 1A, os valores corretos seriam T, N e L.

No bloco 304, um valor fornecido pelo usuário (ou valores no caso de vários desafios de referência) é recebido junto com o ID do usuário, em resposta ao desafio enviado no bloco 302. Por exemplo, se o desafio solicitou o valor de referência 4, o usuário de posse do cartão 100 na Figura 1A pode ter entrado com T como o valor fornecido pelo usuário. Entretanto, um usuário que não está de posse do cartão 100 (um usuário se equivocan-

do) pode ter entrado com um valor diferente (incorreto). O valor fornecido pelo usuário pode ter sido informado pelo usuário via a interface de conexão descrita acima, ou através de alguma outra interface de desafio-resposta.

No bloco 306, o ID do usuário é mapeado para um número do cartão do cartão de autenticação emitido para o usuário e ligado com o ID do usuário. O ID do usuário para o mapeamento do número de cartão pode estar contido em uma tabela de clientes ou base de dados de clientes. No bloco 308, o número do cartão é utilizado para acessar a chave secreta associada com um número do cartão. Em uma concretização, a chave secreta foi utilizada para gerar os pares de referência/valor contidos no cartão, como descrito acima.

Em uma concretização, acessar a chave secreta pode incluir pesquisar uma base de dados segura utilizando o número do cartão como o termo de pesquisa. A base de dados então inclui a chave secreta associada com o número do cartão. A chave secreta pode ser armazenada em forma criptografada, e pode precisar ser decriptografada após ser acessada antes que ela possa ser utilizada.

No bloco 310, o valor associado com a referência solicitada no desafio enviado no bloco 302 é calculado pelo cálculo da HOTP da concatenação da chave secreta com a referência. Como descrito acima, desde que este algoritmo foi utilizado para gerar o valor associado com a referência pelo gerador de cartão, este cálculo gera novamente o valor associado com a referência solicitada no desafio. Em outras concretizações, outros algoritmos podem ser utilizados. Contanto que o algoritmo utilizado seja o mesmo algoritmo utilizado para inicialmente gerar o valor no cartão requisitado no desafio, qualquer algoritmo adequado (tal como algoritmos hash) pode ser utilizado.

No bloco 312, é feita uma determinação quanto a se o valor fornecido pelo usuário recebido no bloco 304 combina com a HOTP calculada no bloco 310. Desde que a HOTP calculada no bloco 310 é a mesma que o valor original da referência impressa no cartão, se o valor fornecido pelo usuário combinar com a HOTP, então isto é uma forte evidência de que o u-

usuário está de posse do cartão associado com o ID do usuário. Portanto, se existir uma combinação no bloco 312, então, no bloco 314, o usuário é autenticado, e tem acesso permitido ao conteúdo ou serviço requisitado pelo usuário.

5 Se, por outro lado, a HOTP e o valor fornecido pelo usuário não combinarem no bloco 312, então, no bloco 316, o usuário não é autenticado, e não é permitido a acessar o conteúdo ou serviço requisitado pelo usuário. Se não autenticado, a conta do ID do usuário pode ser alertada da autenticação com falha, e a conta pode ser bloqueada para impedir ataque adicional. Em uma concretização, é dada uma ou mais chances adicionais para o
10 usuário corretamente responder ao desafio. Em uma concretização, as chances adicionais solicitam valores associados com a mesma referência ou referências que a tentativa de autenticação inicial com falha. Em outra concretização, são utilizadas referências diferentes.

15 Uma concretização de um protocolo diferente de desafio-resposta utilizando o cartão de autenticação é agora descrita com referência às Figuras 4A e 4B. No bloco 402, uma requisição de conexão é recebida a partir do usuário, tal como uma conexão com uma conta de correio eletrônico ou algum outro serviço ou conteúdo on-line. A conexão irá incluir um ID
20 do usuário (tal como um endereço de correio eletrônico) como descrito acima. No bloco 404, o ID do usuário é mapeado para um número do cartão, e no bloco 406, a chave secreta associada com um número do cartão é acessada.

 No bloco 408, um conjunto de pares de referência/valor é calculado utilizando a chave secreta. Isto pode ser feito pelo cálculo de um conjunto de HOTP utilizando a chave secreta e um conjunto de referências, como descrito acima. Em outra concretização, o processo e a função utilizada para gerar o cartão são utilizados para novamente gerar os valores associados com um conjunto de referências selecionadas. Por exemplo, se quatro
25 referências forem selecionadas (por exemplo, 2, 6, 9 e 11 do cartão ilustrado pela Figura 1A) então quatro pares de referência/valor são calculados (por exemplo, 2-Q, 6-I, 9-N e 11-W utilizando o cartão ilustrado pela Figura 1A).
30

No bloco 410, uma exibição gráfica é liberada para o usuário, exibindo um ou mais pares de referência corretos. Em uma concretização, os outros pares de referência/valor são propositalmente exibidos de forma incorreta. No exemplo acima, a referência 9 pode ser selecionada para a

5 exibição correta, resultando em uma exibição apresentando 2-J, 6-O, 9-N e 11-R. Em outra concretização, mais do que um par de referência/valor pode ser exibido corretamente. Dito de forma geral, um subconjunto do conjunto de pares de referência/valor é exibido corretamente e o restante (todos os outros pares de referência/valor calculados) é exibido incorretamente. Em

10 uma concretização, o número de pares de referência/valor corretos é menor do que o número de pares incorreto de referência/valor para tornar a suposição da resposta correta mais difícil.

No bloco 412, uma referência fornecida pelo usuário é recebida, indicando qual referência o usuário acredita apresentar o valor correto associado. Em uma concretização, onde vários pares de valor/referência são exibidos, várias referências fornecidas pelo usuário podem ser recebidas. Entretanto, neste exemplo, somente um par de referência e valor é exibido corretamente, e assim, somente uma referência fornecida pelo usuário é esperada a partir do usuário no bloco 412. Em uma concretização, o usuário pode

20 indicar a seleção do usuário do par correto de referência/valor por clicar com o mouse ou cursor em uma representação gráfica do par de referência/valor. Desta maneira, o valor real do par correto de valor/referência não precisa ser transmitido entre o usuário e a entidade de autenticação, resultando em segurança adicional.

25 No bloco 414, é feita uma determinação quanto a se a referência fornecida pelo usuário corresponde ao par correto de referência/valor do bloco 410. Em outras palavras, o usuário realmente identifica qual par de referência/valor exibido no desafio no bloco 410 corretamente combinou com o par de referência/valor no cartão de autenticação emitido para o usuário?

30 Se, for determinado que a referência (ou referências) fornecida pelo usuário realmente corresponde ao par correto de referência/valor, então, no bloco 416, o usuário é autenticado. Entretanto, se for determinado que a referência

(ou referências) fornecida pelo usuário não corresponde ao par correto de referência/valor, então, no bloco 416, o usuário não é autenticado.

Sistema de Computador Ilustrativo

Várias concretizações da presente invenção foram descritas no contexto de um compilador que gera código que é inserido em um programa sendo compilado pelo compilador. Um sistema de computador ilustrativo no qual tal compilador pode ser implementado é agora descrito com referência à Figura 5. O sistema de computador 500 pode ser utilizado para executar uma ou mais das operações descritas neste documento. Em concretizações alternativas, a máquina pode compreender um roteador de rede, um comutador de rede, uma ponte de rede, um Assistente Pessoal Digital (PDA), um telefone celular, uma aparelhagem de rede ou qualquer máquina capaz de executar uma seqüência de instruções que especifica ações a serem executadas por esta máquina.

O sistema de computador 500 inclui um processador 502, uma memória principal 504 e uma memória estática 506, os quais se comunicam uns com os outros via um barramento 508. O sistema de computador 500 pode adicionalmente incluir uma unidade de exibição de vídeo 510 (por exemplo, um vídeo de cristal líquido (LCD) ou um tubo de raio catódico (CRT)). O sistema de computador 500 também inclui um dispositivo de entrada alfanumérico 512 (por exemplo, um teclado), um dispositivo de controle de cursor 514 (por exemplo, um mouse), uma unidade de controle de disco 516, um dispositivo de geração de sinal 520 (por exemplo, um alto-falante) e um dispositivo de interface de rede 522.

A unidade de disco 516 inclui um meio legível por máquina 524 no qual é armazenado um conjunto de instruções (isto é, software) 526 incorporando qualquer uma, ou todas as metodologias descritas acima. O software 526 também é apresentado como residindo, completamente ou pelo menos parcialmente, dentro da memória principal 504 e/ou dentro do processador 502. O software 526 pode ser adicionalmente transmitido ou recebido via o dispositivo de interface de rede 522. Para os propósitos deste relatório descritivo, o termo "meio legível por máquina" deve ser considerado

como incluindo qualquer meio que seja capaz de armazenar ou codificar uma seqüência de instruções para execução pelo computador e que causam que o computador execute qualquer uma das metodologias da presente invenção. Por conseqüência, o termo "meio legível por máquina" deve ser considerado como incluindo, mas não sendo limitado, a memórias de estado sólido, discos ópticos e magnéticos e sinais de onda portadora.

Questões Gerais

Na descrição acima, para o propósito de explicação, vários detalhes específicos foram expostos. Entretanto, é entendido que as concretizações da invenção podem ser praticadas sem estes detalhes específicos. Em outros casos, circuitos, estruturas e técnicas, bem-conhecidos, não foram apresentados em detalhes de modo a não obscurecer o entendimento desta descrição.

As concretizações da presente invenção incluem vários processos. Os processos podem ser executados por componentes de hardware ou podem ser incorporados em instruções executáveis por máquina, as quais podem ser utilizadas para causar que um ou mais processadores programados com as instruções executem os processos. Alternativamente, os processos podem ser executados por uma combinação de hardware e software.

As concretizações da presente invenção podem ser proporcionadas como um produto de programa de computador que pode incluir um meio legível por máquina tendo armazenado no mesmo instruções, as quais podem ser utilizadas para programar um computador (ou outro dispositivo eletrônico) para executar um processo de acordo com uma ou mais concretizações da presente invenção. O meio legível por máquina pode incluir, mas não está limitado, a disquetes flexíveis, discos ópticos, memórias somente para leitura de disco compacto (CD-ROMs), e discos magnetos-ópticos, memórias somente para leitura (ROMs), memórias de acesso aleatório (RAMs), memórias de leituras programáveis e apagáveis (EPROMs), memórias de leitura programáveis e eletricamente apagáveis (EEPROMs), cartões magnéticos ou ópticos, memória flash, ou outro tipo de mídia/meio legível por máquina adequado para armazenar instruções. Além disso, as concreti-

zações da presente invenção também podem ser transferidas como um produto de programa de computador, onde o programa pode ser transferido a partir de um computador remoto para um computador requisitante por meio de sinais de dados incorporados em uma onda portadora ou em outro meio de propagação através de um link de comunicação (por exemplo, um modem ou conexão de rede).

Enquanto a invenção foi descrita em termos de várias concretizações, os versados na técnica irão reconhecer que a invenção não está limitada às concretizações descritas, mas pode ser praticada com modificação e alteração dentro do espírito e do escopo das reivindicações anexas. Assim, a descrição é para ser considerada como ilustrativa, ao invés de limitativa.

REIVINDICAÇÕES

1. Método, compreendendo:

enviar um desafio para um usuário a ser autenticado, o desafio incluindo uma referência em relação a um cartão emitido para o usuário;

5 receber, a partir do usuário, em resposta ao desafio, um valor fornecido pelo usuário, suposto pelo usuário, como estando associado com a referência no cartão emitido para o usuário;

 acessar uma chave secreta associada com o cartão emitido para o usuário;

10 gerar uma senha utilizando uma função F da chave secreta e a referência;

 mapear a função F para um valor em um alfabeto; e

 autenticar o usuário por comparar o valor no alfabeto com o valor fornecido pelo usuário.

15 2. Método, de acordo com a reivindicação 1, onde a função F compreende uma senha ocasional baseada em hash (HOTP).

 3. Método, de acordo com a reivindicação 1, adicionalmente compreendendo receber um identificador do usuário a partir do usuário em resposta ao desafio, onde acessar a chave secreta compreende mapear o
20 identificador do usuário para um número de cartão associado com o identificador do usuário, o número do cartão sendo o número do cartão do cartão emitido para o usuário.

 4. Método, de acordo com a reivindicação 1, onde gerar a função F compreende gerar a função F utilizando uma concatenação da chave secreta e da referência.
25

 5. Método, de acordo com a reivindicação 1, onde o alfabeto compreende um conjunto de caracteres consistindo no alfabeto A até Z da linguagem inglesa e os números árabes 0 até 9.

 6. Método, de acordo com a reivindicação 1, onde acessar a
30 chave secreta compreende acessar a chave secreta utilizada para gerar todos os valores no cartão emitido para o usuário quando o cartão foi originalmente criado.

7. Método, compreendendo:

enviar um desafio para um usuário a ser autenticado, o desafio solicitando informação contida em um cartão emitido para o usuário;

5 receber uma resposta para o desafio, a resposta compreendendo informação fornecida pelo usuário;

acessar uma chave secreta associada com um cartão emitido para o usuário;

gerar a informação requisitada no desafio, utilizando a chave secreta; e

10 autenticar o usuário por comparar a informação gerada com a informação fornecida pelo usuário na resposta recebida.

8. Método, de acordo com a reivindicação 7, onde enviar um desafio compreende enviar um conjunto de referências correspondendo a um conjunto de pares de valores de referência contidos no cartão, e onde a in-
15 formação fornecida pelo usuário pretende ser um conjunto de valores correspondendo ao conjunto de pares de valores de referência.

9. Método, de acordo com a reivindicação 7, onde acessar a chave secreta compreende acessar um módulo de segurança de hardware (HSM).

20 10. Método, de acordo com a reivindicação 7, onde gerar a informação compreende calcular um hash da chave secreta e pelo menos uma parte do desafio.

11. Método, de acordo com a reivindicação 10, onde a parte do desafio compreende uma referência contida no cartão.

25 12. Método, de acordo com a reivindicação 7, onde receber a resposta para o desafio compreende receber uma indicação de pares de valores de referência corretos de um conjunto de pares de valores de referência exibidos.

13. Sistema de autenticação, compreendendo:

30 uma interface com o usuário para enviar um desafio para um usuário a ser autenticado, o desafio incluindo uma referência em um cartão emitido para o usuário, e, para receber uma resposta ao desafio, a resposta

compreendendo um valor fornecido pelo usuário suposto pelo usuário como estando associado com a referência no cartão emitido para o usuário;

uma base de dados de chave contendo uma chave secreta associada com o cartão emitido para o usuário; e

5 um módulo de autenticação para autenticar o usuário pela geração da informação requisitada no desafio, utilizando uma função da chave secreta e da referência, mapeando a função para um valor, e comparando o valor com a informação fornecida pelo usuário na resposta recebida para autenticação.

10 14. Sistema de autenticação, de acordo com a reivindicação 13, adicionalmente compreendendo:

um gerador de desafio para gerar um desafio compreendendo um conjunto de referência correspondendo a um conjunto de pares de valores de referência contidos no cartão.

15 15. Sistema de autenticação, de acordo com a reivindicação 13, onde acessar a base de dados de chave compreende um módulo de segurança de hardware (HSM).

20 16. Sistema de autenticação, de acordo com a reivindicação 13, onde o módulo de autenticação gera a informação por calcular um hash unidirecional da chave secreta e pelo menos uma parte do desafio.

17. Sistema de autenticação, de acordo com a reivindicação 13, onde um módulo de autenticação gera a informação por calcular senha ocasional baseada em hash (HOTP) utilizando uma concatenação da chave secreta e de pelo menos uma parte do desafio.

25 18. Método, compreendendo:

criar uma chave secreta;

associar a chave secreta com um cartão a ser utilizado como um segundo fator durante a autenticação;

30 popular o cartão com vários pares de valores de referência utilizando a chave secreta.

19. Método, de acordo com a reivindicação 18, onde popular o cartão compreende gerar vários valores dos pares de valores de referência

por calcular uma senha ocasional baseada em hash (HOTP) de uma concatenação da chave secreta e das várias referências dos pares de valores de referência.

20. Método, de acordo com a reivindicação 18, adicionalmente
5 compreendendo proporcionar o cartão para um usuário de um serviço de acesso limitado, e proporcionar a chave secreta para uma entidade de autenticação que executa autenticação do usuário para o serviço de acesso limitado.

21. Método, compreendendo:
10 enviar um desafio para um usuário a ser autenticado, o desafio compreendendo uma exibição de vários pares de valores de referência;
receber uma resposta a partir do usuário indicando um primeiro par de valores de referência dos vários pares de valores de referência que combinam com um par de valores de referência impresso em um cartão emitido para o usuário;
15 acessar uma chave secreta associada com o cartão emitido para o usuário;
autenticar o usuário utilizando a chave secreta e a resposta recebida.

20 22. Método, de acordo com a reivindicação 21, onde autenticar o usuário compreende gerar os valores corretos para os vários pares de valores de referência utilizando a chave secreta, e determinar se o primeiro par de valores de referência identificado pelo usuário foi corretamente exibido no desafio.

25 23. Método para uma autenticação de segundo fator baseada no cartão, o método compreendendo:
requisitar informação a partir de um usuário baseado em um par de valores de referência a partir do cartão;
calcular um par de valores de referência baseado em uma chave
30 secreta associada com o cartão; e
autenticar o usuário se a informação requisitada combinar com o valor calculado.

24. Método, de acordo com a reivindicação 23, onde o usuário é requerido a entrar com um valor do par de valores de referência quando proporcionado com a referência do par de valores de referência.

5 25. Método, de acordo com a reivindicação 23, onde o usuário é requerido a selecionar um par de valores de referência correto a partir de um conjunto incluindo vários pares de valores de referência incorretos.

CARTÃO DE AUTENTICAÇÃO 100

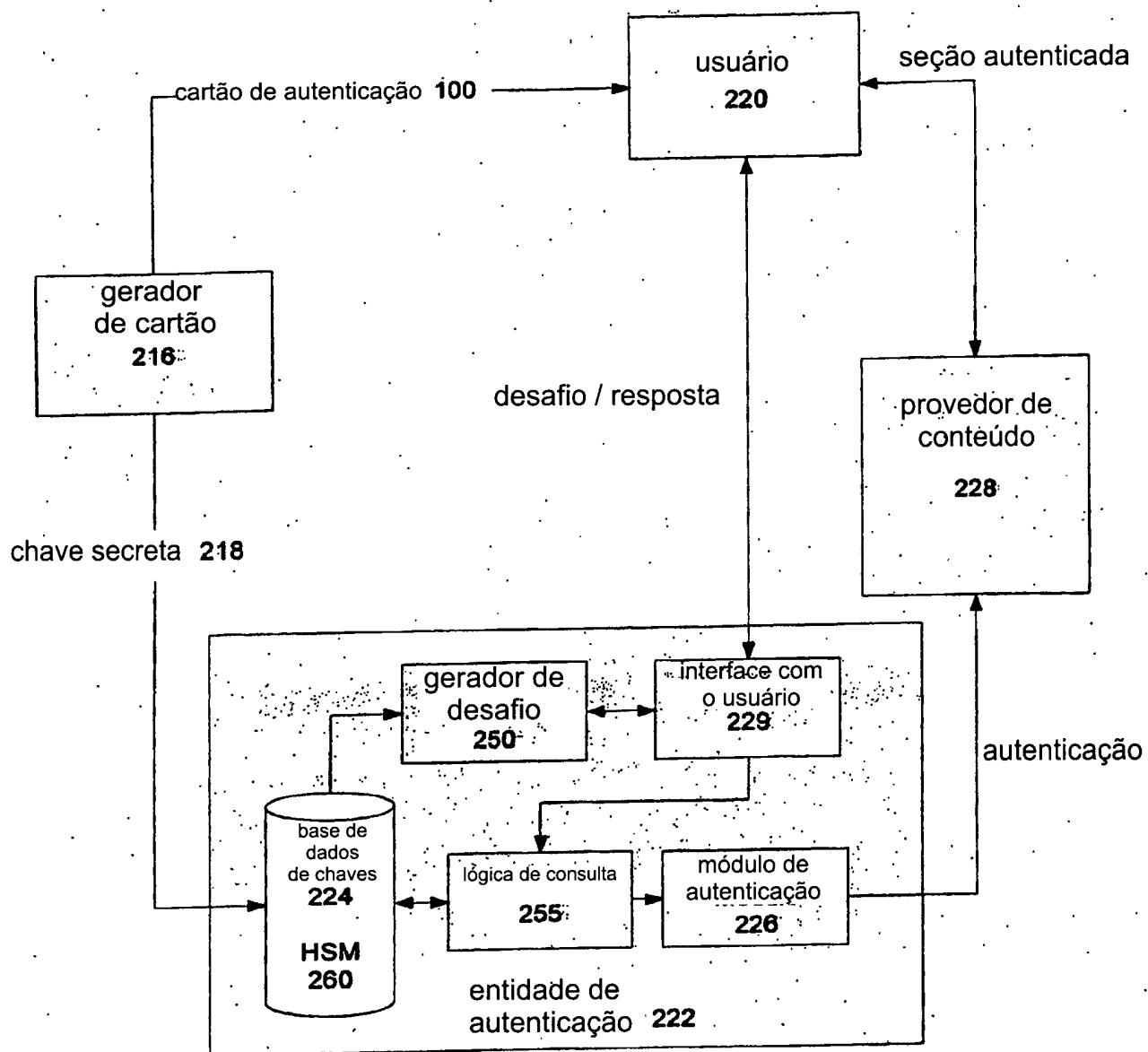
4536 3657 2352 7658					
NÚMERO DO CARTÃO 120					
1	F	5	V	9	N
2	Q	6	I	10	S
3	P	7	D	11	W
4	T	8	E	12	L

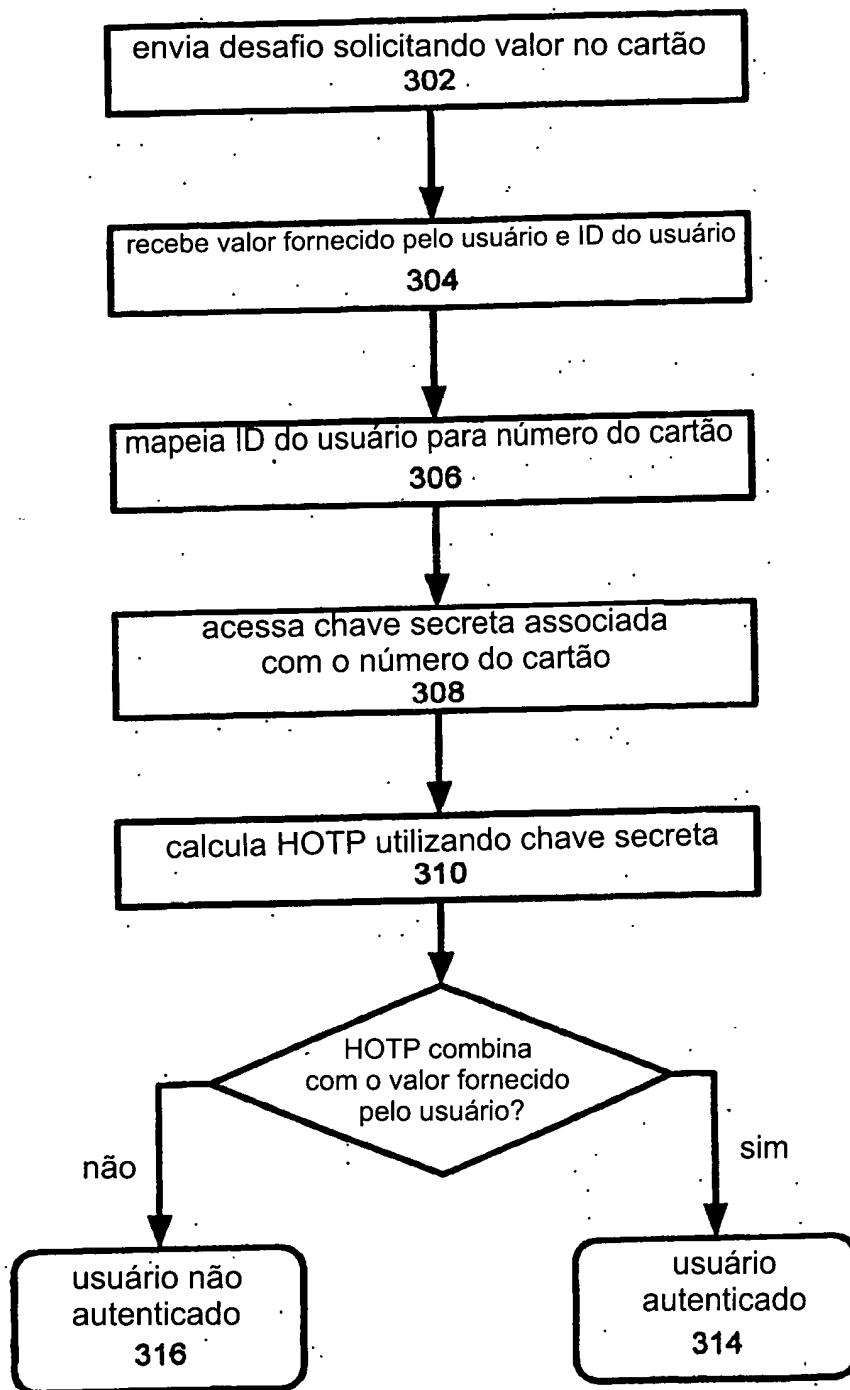
Fig 1A

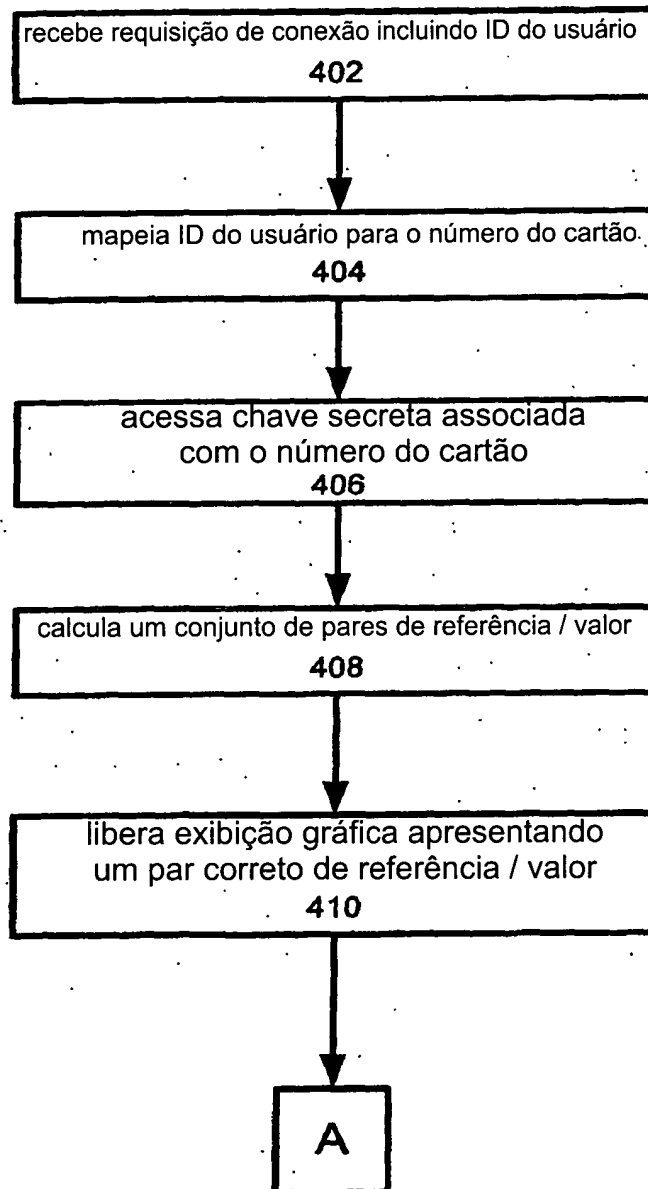
CARTÃO DE AUTENTICAÇÃO 100

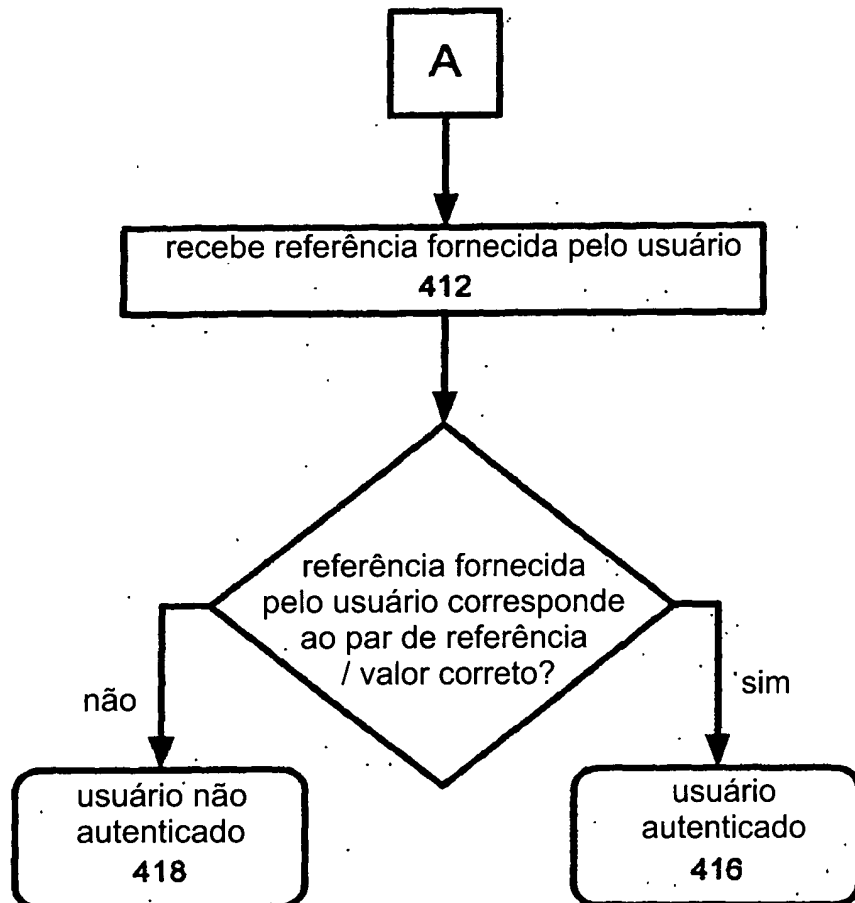
4536 3657 2352 7658			
NÚMERO DO CARTÃO 120			
	1	2	3
1	F	V	N
2	Q	I	S
3	P	D	W
4	T	E	L

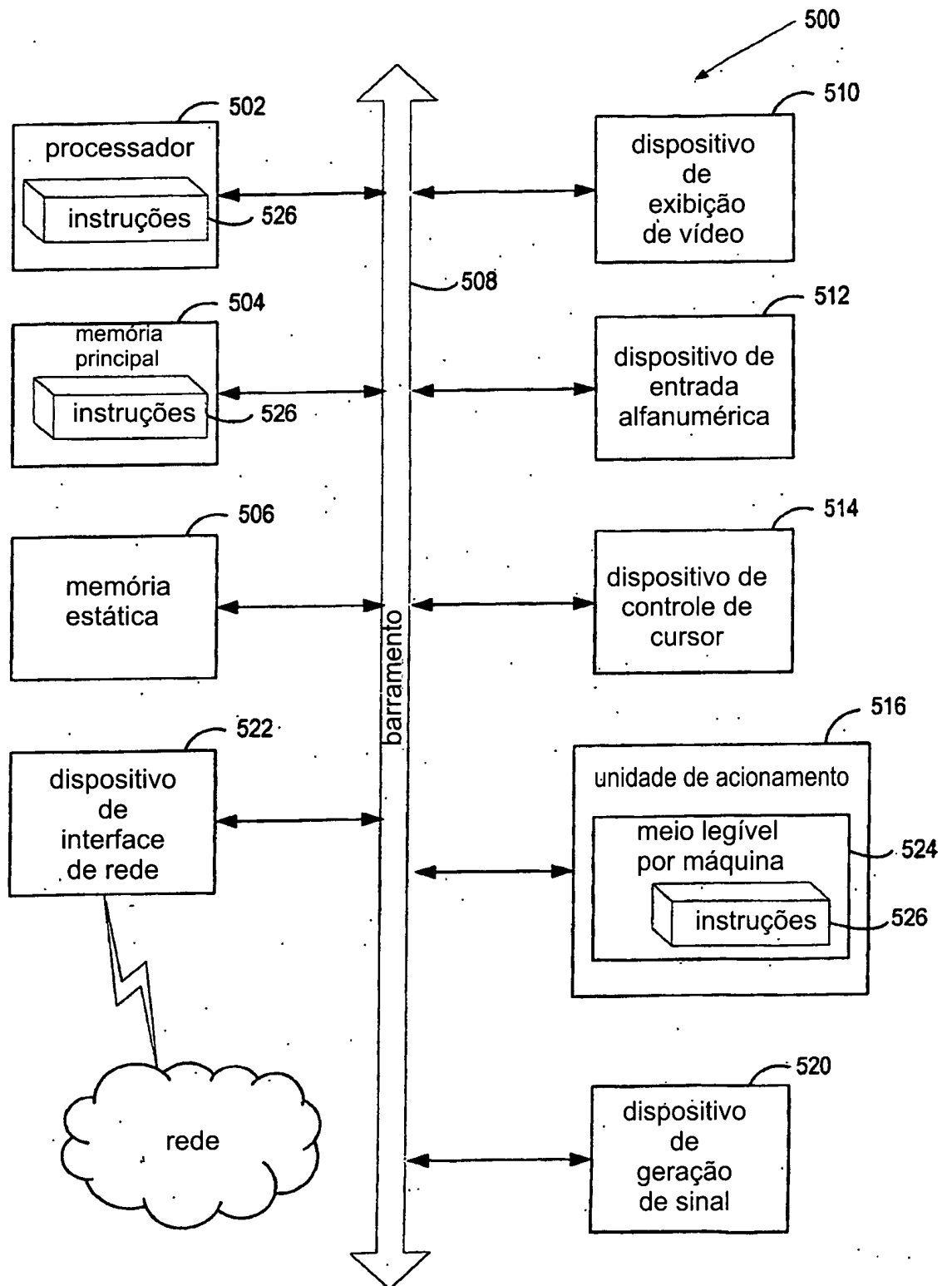
Fig 1B

**Fig 2**

**Fig 3**

**Fig 4A**

**Fig 4B**

**Fig 5**

RESUMO

Pedido de Patente: **"MÉTODO E APARELHO PARA PROPORCIONAR AUTENTICAÇÃO UTILIZANDO UM CARTÃO DE AUTENTICAÇÃO"**.

- A presente invenção refere-se a um método e a um aparelho
- 5 para proporcionar autenticação. O método compreende enviar um desafio para um usuário a ser autenticado, o desafio incluindo uma referência em um cartão emitido para o usuário e receber um valor fornecido pelo usuário suposto pelo usuário como estando associado com a referência no cartão emitido para o usuário. O método adicionalmente compreende acessar uma
- 10 chave secreta associada com o cartão emitido para o usuário e gerar uma senha utilizando uma função F da chave secreta e a referência. O método adicionalmente compreendendo mapear a função F para um valor em um alfabeto e autenticar o usuário por comparar o valor no alfabeto com o valor fornecido pelo usuário.