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

(21) **PI0608576-8 A2**

BRPI0608576A2

(22) Data de Depósito: 06/01/2006
(43) Data da Publicação: 12/01/2010
(RPI 2036)

(51) Int.Cl.:
G07F 7/10 (2010.01)

(54) Título: **PROCESSO PARA COMUNICAÇÃO DE DADOS SEGURA**

(30) Prioridade Unionista: 07/03/2005 GB 05 04545.5

(73) Titular(es): TRICERION LTD

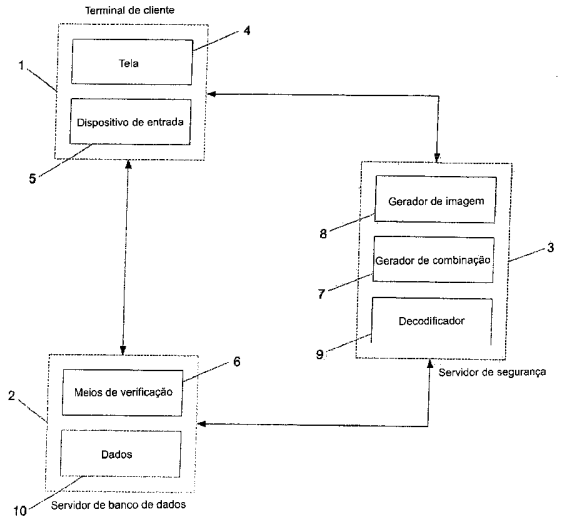
(72) Inventor(es): NORMAN FRASER, SANJAY HARIA, STUART MORRIS

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

(86) Pedido Internacional: PCT GB2006050002 de 06/01/2006

(87) Publicação Internacional: WO 2006/095203de 14/09/2006

(57) Resumo: PROCESSO PARA COMUNICAÇÃO DE DADOS SEGURA. A presente invenção refere-se a uma troca de dados entre um cliente terminal (1) e um servidor de banco de dados seguro (2) os dados são codificados usando uma informação posiciona! gerada por um gerador de combinação (7) em um servidor de segurança separado (3). A informação posiciona! é usada para produzir uma imagem específica para uma ocorrência de comunicação que é acessada por um cliente terminal (1) e é a base para a entrada de dados sensíveis no termina! do cliente (1). A conexão de comunicação de três vias entre o cliente terminal, o servidor de banco de dados e o servidor de segurança aumenta imensamente a dificuldade de interceptação bem-sucedida e a decodificação dos dados que foram inseridos no terminal do cliente. Este processo de comunicação de dados seguro é particularmente adequado para a comunicação de dados de senhas, por exemplo, em uma instituição bancária.



PI0608576-8

Relatório Descritivo da Patente de Invenção para "**PROCESSO PARA COMUNICAÇÃO DE DADOS SEGURA**".

FUNDAMENTOS DA INVENÇÃO

Campo da invenção

A presente invenção refere-se a um processo de comunicação de dados segura e um sistema utilizando um tal processo. Em particular, a presente invenção refere-se a um processo de comunicação de dados entre um cliente terminal e um servidor remoto que impede interceptações efetivas não autorizadas de dados que estão sendo comunicados e, conseqüentemente, no caso de dados criptografados apresenta um risco insignificante de decodificação de dados criptografados. A presente invenção é particularmente bem-adequada, mas não exclusivamente, para aplicações financeiras tais como ATMs e transações bancárias online nas quais os dados de autorização para acessar dados financeiros seguros é transmitida pelos terminais de clientes através de conexões potencialmente não seguras a um servidor remoto onde os dados de autorização são então verificados.

Descrição da técnica relacionada:

Naturalmente, é importante que o acesso a dados seguros seja somente concedido a pessoas autorizadas. No entanto, em muitas áreas a necessidade por segurança deve estar ajustada à necessidade de acesso rápido e remoto dos dados. Por exemplo, a capacidade de uma equipe de emergência e de acidentes de um hospital de acessar imediatamente os registros médicos privados de um paciente pode significar salvar a vida. No caso de clientes de bancos, atualmente os mesmos demandam que tenham acesso rápido e fácil a seus fundos sem ser obrigado a uma ida à agência do banco durante as horas normais de expediente. Para esta finalidade, têm sido desenvolvidos sistemas seguros que mantêm os dados em servidores de banco de dados seguros e que permitem o acesso aos dados por meio de terminais remotos de cliente.

Em tais sistemas seguros, a identidade do usuário geralmente é verificada através do uso de dados de autorização, por exemplo, nome do usuário, senha ou um número de identificação pessoal (PIN) que é enviado

entre o terminal do cliente e o servidor do banco de dados. Apesar das medidas que podem ser empreendidas pelo usuário de um terminal de cliente para assegurar que os dados de autorização permaneçam confidenciais, os dados de autorização, apesar disso, podem ser observados por outros ao serem inseridos pelo usuário ou podem ser eletronicamente interceptados em algum ponto entre o terminal do cliente e o servidor do banco de dados.

O acesso não autorizado a dados financeiros, tais como por menores bancários da pessoa, evidentemente traz recompensas financeiras tornando-o alvo de crescente atividade criminosa. Atualmente, muitos cartões de crédito ou débito utilizam uma tarja magnética ou um chip eletrônico que porta parte dos dados de autorização do portador do cartão. O restante dos dados de autorização são conhecidos pelo portador do cartão, por exemplo, na forma de um PIN. Quando o cartão é inserido na máquina eletrônica automática (ATM) ou máquina de cartão de crédito "PDQ", a informação armazenada na tarja magnética ou chip eletrônico bem como o PIN inserido pelo portador do cartão é passado para um servidor de banco de dados remoto, ou um servidor de autorização separado, para verificação. Se os dados de autorização estão corretos, o acesso aos dados financeiros é concedido ao portador do cartão.

Uma forma simples de fraude de cartão é observar o portador do cartão no momento de inserir o seu PIN em uma ATM e então roubar o cartão. Alternativamente, ao invés de roubar o cartão, o que naturalmente vai alertar o portador do cartão, os dados armazenados no cartão podem ser copiados usando leitores de cartão magnético publicamente disponíveis durante as transações financeiras. O cartão copiado pode então ser usado para fazer compras e saques em dinheiro sem chamar a atenção do portador do cartão ou do banco.

Cartões inteligentes oferecem vantagens significantes de segurança sobre os cartões de tarja magnética no qual todos os dados de autorização, inclusive o PIN, estão armazenados no cartão de forma criptografada. Isso torna praticamente impossível a cópia do cartão durante transações financeiras. Não obstante, se o cartão for roubado é extremamente difícil e

demorado para os criminosos acessar o PIN armazenado no cartão. Apesar disso, a fraude do cartão ainda é possível pela observação do portador do cartão ao inserir seu PIN e subseqüentemente roubando o cartão. Esta forma de fraude de cartão é particularmente relevante para cartões inteligentes nos quais é usado um PIN, ao invés da assinatura, para transações eletrônicas em pontos de venda habituais (EPOS). Em decorrência disso, estão aumentando as chances de observar um PIN de um portador de cartão.

A FR 28119067 descreve um terminal EPOS para uso com um cartão inteligente e compreende um bloco de teclas de tela de toque. Cada vez que um cartão inteligente for inserido no terminal EPOS, um bloco de teclas aleatoriamente disposto é exibido ao portador do cartão na tela de toque do bloco de teclas para inserir seu PIN. Em decorrência disto, um observador fica incapacitado de determinar o PIN do portador do cartão meramente por observar o movimento dos dedos do portador do cartão. Sistemas similares estão descritos na US 5.949.348 e na US 4.479.112.

Como o PIN de um cartão inteligente é armazenado no próprio cartão, as transações EPOS ocorrem sem a necessidade de enviar os dados de autorização completos para o banco de dados ou servidor de autorização. Em particular, em nenhum momento o PIN armazenado no cartão é comunicado além do terminal EPOS. Portanto, estas publicações não referem-se ao problema de outros interceptarem os dados de autorização durante a comunicação entre o terminal EPOS e um servidor de banco de dados remoto.

Enquanto que os cartões inteligentes oferecem uma forma segura de autorização, apesar disso um leitor de cartão deve ser providenciado em cada terminal de cliente com a finalidade de ler o cartão e confirmar a autorização. Em conformidade com isso, os cartões inteligentes são impraticáveis para muitas aplicações, em particular onde o acesso a dados seguros é projetado para ser concedido por meio da Internet. Para aplicações tais como transações bancárias em linha, os dados de autorização continuam a serem enviados entre o terminal do cliente (por exemplo, um computador residencial) e o banco de dados ou servidor de autorização para verificação. Apesar de os dados de autorização, normalmente, serem criptografados, por

exemplo, usando uma criptografia de senha pública, há preocupações de que é somente uma questão de tempo antes de serem desenvolvidos métodos de decodificar tais dados.

SUMÁRIO DA INVENÇÃO

Portanto, há uma necessidade de um processo aperfeiçoado de autorização remota segura entre o terminal do cliente e o servidor, sem a necessidade de prover o terminal de cliente com equipamentos adicionais (por exemplo, leitor de cartões inteligentes). Portanto, um objetivo da presente invenção é proporcionar um processo de autorização no qual os dados enviados pelo terminal de cliente para o servidor, se interceptados, não possam ser usados para extrair os dados completos de autorização do usuário.

Além disso, um truque relativamente novo utilizado pelos criminosos para obter de modo fraudulento os dados de autorização bancária dos clientes do banco ficou conhecido como "phishing" (armadilha para fisgar a senha). Isso envolve o envio de uma mensagem de e.mail ou carta para um cliente bancário de Internet o qual direciona o cliente para um website que tem a aparência de uma página de web do banco o qual solicita ao cliente inserir os seus dados, completos, de autorização – normalmente como um pretexto tal como uma verificação rotineira de segurança. O website, evidentemente, é falso e os criminosos que operam o website estão então habilitados a capturar e usar os dados de autorização do cliente para fazer com que fundos sejam transferidos da conta do cliente.

Portanto, um objetivo adicional separado da presente invenção é apresentar um processo de autorização que reduz a probabilidade dos clientes serem ludibriados por ataques de armadilhas de fisgar as senhas fraudulentamente.

Em conformidade com isso, em um primeiro aspecto, a presente invenção apresenta um processo de comunicação segura entre um servidor e um terminal remoto a partir do servidor, sendo que o terminal inclui um dispositivo de entrada de dados operado pelo usuário, compreendendo o processo de comunicação segura as etapas de: dados codificados de comunicação a partir do servidor para o terminal, sendo os dados codificados es-

pecíficos a um evento de comunicação; gerando dados posicionais a partir dos dados inseridos pelo usuário usando o dispositivo de entrada de dados do terminal no que refere-se aos dados codificados, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário do dispositivo de entrada de dados; comunicando os dados posicionais a partir do terminal ao servidor; e decodificando os dados posicionais recebidos pelo servidor usando os referidos dados de codificação para gerar os dados de entrada do usuário.

Em um segundo aspecto, a presente invenção apresenta um sistema de comunicação segura que compreende um servidor e, pelo menos, um terminal remoto a partir do servidor e em comunicação bidirecional com o servidor, sendo o servidor compreendido de: um codificador para gerar dados codificados específicos para um evento de comunicação; uma interface de comunicações para comunicar os dados codificados para o terminal remoto e para receber dados posicionais a partir do terminal, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário e sendo uma codificação dos dados inseridos pelo usuário; e um decodificador para decodificar os dados posicionais recebidos a partir do terminal, usando o decodificador os dados codificados do codificador para decodificar os dados posicionais e sendo cada terminal compreendido de: um dispositivo de entrada manualmente operado para a entrada de dados do usuário que estão codificados como dados posicionais; e uma interface de comunicações de terminal para receber os dados codificados a partir do servidor e para comunicar os dados posicionais ao servidor.

Em um terceiro aspecto, a presente invenção apresenta um servidor de comunicação segura compreendido de um codificador para gerar dados codificados específicos a um evento de comunicação; uma interface de comunicações para comunicar os dados codificados para um terminal remoto e para receber os dados posicionais a partir do terminal remoto, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário e sendo uma codificação dos dados inseridos pelo usuário; e um decodificador para decodificar os dados posicionais

recebidos a partir do terminal, usando o decodificador dos dados codificados do codificador para decodificar os dados posicionais.

Em um quarto aspecto, a presente invenção apresenta um processo de comunicação segura entre um servidor e um terminal remoto a partir do servidor, incluindo o terminal um dispositivo de entrada e exibição de dados operados pelo usuário, o processo seguro de comunicação segura compreendido de etapas de: emissão de uma solicitação para comunicação ao servidor a partir do terminal remoto e fornecendo ao servidor dados preliminares de identificação de usuário ao usuário do terminal, identificando dados padrão específicos ao usuário e comunicando os dados exibidos a partir do servidor para o terminal com base nos dados padrão identificados; e gerando uma imagem na tela do terminal com base nos dados exibidos recebidos a partir do servidor enquanto os dados susceptíveis adicionais são inseridos por um usuário somente quando a imagem na tela corresponde a uma imagem previamente produzida conhecida ao usuário.

Em um quinto aspecto, a presente invenção apresenta um sistema de comunicação segura compreendendo um servidor e pelo menos um terminal remoto de e em comunicação bidirecional com o servidor, o servidor compreendendo: armazenamento de dados padrão do usuário em que são armazenados dados exibidos específicos de cada usuário; e uma interface de comunicação para comunicar os dados exibidos ao terminal remoto e para receber os dados inseridos pelo usuário a partir do terminal, e cada terminal compreendendo: um dispositivo de entrada da dados operado pelo usuário para a entrada de dados do usuário; um visualizador; e uma interface de comunicação terminal para receber os dados exibidos a partir do servidor e para comunicar os dados inseridos pelo usuário ao servidor.

Em um sexto aspecto, a presente invenção apresenta um servidor de comunicação segura compreendido de: armazenagem de dados padrão do usuário no qual são armazenados os dados exibidos específicos a cada usuário; e uma interface de comunicações para comunicar os dados exibidos para o terminal remoto e para receber os dados inseridos pelo usuário a partir do terminal.

BREVE DESCRIÇÃO DO DESENHOS

Estes e outros objetos, vantagens e novos aspectos da presente invenção serão mais prontamente apreciados a partir da seguinte descrição por menorizada quando efetuada a leitura em conjunto com os desenhos que acompanham, nos quais:

A figura 1 ilustra um sistema de autorização de acordo com a presente invenção.

A figura 2 é um diagrama simplificado das trocas de dados que são efetuadas em conformidade com uma primeira incorporação do processo de comunicação de dados da presente invenção.

A figura 3 ilustra exemplarmente dados de imagem gerados pelo servidor de segurança do sistema de autorização da presente invenção.

A figura 4 ilustra um sistema alternativo de autorização em conformidade com a presente invenção.

A figura 5 é um diagrama simplificado das trocas de dados que são efetuadas em conformidade com uma segunda incorporação do processo de comunicação de dados da presente invenção.

A figura 6 ilustra exemplarmente dados de imagem utilizando caracteres alfanuméricos gerados pelo servidor de segurança do sistema de autorização da figura 4.

A figura 7 ilustra exemplarmente dados de imagem utilizando caracteres não-alfanuméricos gerados pelo servidor de segurança do sistema de autorização da figura 4.

DESCRIÇÃO POR MENORIZADA DAS INCORPORAÇÕES PREFERIDAS

O sistema de autorização da figura 1 compreende um terminal de cliente 1, um servidor de banco de dados 2 e um servidor de segurança 3, dos quais todos os três estão em comunicação bidirecional um com o outro. Com sistemas de autorização convencionais, o servidor de segurança 3 está ausente e o terminal de cliente 1 e o servidor de banco de dados 2 comunicam-se somente um com outro.

O terminal de cliente 1 está adaptado ou no hardware ou no software para acessar dados remotamente armazenados no servidor de

banco de dados 2 e para efetuar trocas e/ou adições aos dados remotamente armazenados. O terminal de cliente 1 inclui uma tela 4 e um dispositivo de entrada 5. Dispositivos apropriados para o terminal de cliente incluem, mas não estão limitados a, computadores pessoais, ATMs, telefones celulares e PDAs. Na verdade, qualquer dispositivo capaz de comunicações externas e que tem uma tela e um dispositivo de entrada pode ser adaptado para funcionar como terminal de cliente 1.

A tela 4 do terminal de cliente 1 pode ser qualquer dispositivo capaz de modificar sua aparência com a finalidade de transmitir várias informações para um usuário. Enquanto é preferido um VDU, a tela 4 pode, alternativamente, consistir em legendas modificáveis em um bloco de teclas ou teclado tal que a tela 4 e o dispositivo de entrada 5 são integrados. Alternativamente, a tela 4 e o dispositivo de entrada 5 podem ser integrados na forma de um tela de toque.

O dispositivo de entrada 5 é usado para inserir os dados de autorização, tal como o nome do usuário, senha e/ou PIN. Estes dados de autorização são, subseqüentemente, usados pelo terminal de cliente 1 para conseguir acesso ao servidor de banco de dados 2. O terminal de cliente 1 pode adicionalmente incluir meios para receber e efetuar a leitura de um cartão, ou outros meios de identificação, portando dados de autorização parciais. Por exemplo, o terminal de cliente 1 pode ser um ATM caso e neste caso o leitor do cartão da ATM recebe um cartão portando os detalhes da conta do portador do cartão, por exemplo, nome, código de classificação de banco e número de conta. No entanto, os dados que constam no cartão representam somente parte dos dados de autorização e o acesso ao servidor de banco de dados 2 somente é concedido quando forem inseridos dados adicionais de autorização pelo usuário no dispositivo de entrada 5 do terminal de cliente 1.

O servidor de banco de dados 2 armazena os dados 10 previstos para serem acessados somente por pessoal autorizado e inclui meios 6 para a verificação da autorização de um usuário que está tentando acessar o servidor de banco de dados 2. Os meios de verificação 6 em sua forma mais

simples compreendem uma tabela de conferência que contém uma lista de dados de autorização válidos. Se os dados de autorização recebidos pelos meios de verificação 6 conferem com os dados de autorização válidos armazenados na tabela de conferência, é concedido ao usuário o acesso aos dados 10 armazenados no servidor de banco de dados 2. De preferência, os meios de verificação 6 são adaptados para determinar a identidade do usuário a partir de dados de autorização recebidos de modo tal que o acesso aos dados armazenados no servidor de banco de dados 2 pode ser adaptado de acordo com a identidade do usuário, por exemplo, de modo tal que um paciente somente esteja habilitado a acessar seus próprios registros médicos, ou um cliente de banco somente está habilitado a acessar seus próprios por menores bancários. Os meios de verificação 6 podem ser parte dos servidor de banco de dados 2 ou podem tomar a forma de um servidor de autorização separado que obtém acesso ao servidor de banco de dados 2 até que sejam recebidos os dados de autorização válidos.

O servidor de segurança 3 compreende um gerador de combinação 7, um gerador de imagem 8 e um decodificador 9. Quando uma solicitação for recebida do servidor de banco de dados 2, o gerador de combinação 7 é adaptado para gerar uma cadeia aleatória e um código de identificação específico àquela cadeia aleatória. A cadeia aleatória que é gerada irá depender do conteúdo dos dados de autorização a ser inserido pelo usuário no dispositivo de entrada 5 do terminal de cliente 1 com a execução aleatória ocorrendo sobre o conjunto de caracteres legitimados. Por exemplo, se os dados de autorização estão na forma de um PIN, por exemplo, se os dados de autorização incluem somente numerais, a cadeira aleatória é composta, de maneira ideal, de 10 caracteres, por exemplo, '7260948135'. Alternativamente, se os dados de autorização incluem ambos, numerais e letras em caixa alta, a cadeia aleatória pode ser compreendida de até 36 caracteres correspondendo a 10 numerais (0-9) e 26 letras (A-Z), por exemplo, '-JR6VSAPKB2G...'. O gerador de combinação 7 comunica ambos, a cadeia aleatória e o código de identificação, ao gerador de imagem 8 e o decodificador 9, e comunica somente o código de identificação de volta ao servidor

de banco de dados 2. A cadeia aleatória também pode ser gerada, por exemplo, por seleção aleatória, por exemplo, usando um gerador de números aleatórios, uma entrada de uma tabela de conferência de cadeias de caracteres, tendo cada cadeia de caracteres uma configuração diferente.

O gerador de imagem 8 usa a cadeia aleatória recebida do gerador de combinação 7 e gera dados de imagem adequados para exibir no terminal de cliente 1. Por exemplo, onde o terminal de cliente 1 é um computador pessoal, os dados de imagem podem consistir em uma imagem de arquivo (por exemplo, JPG, GIF, BMP etc) ou um arquivo HTML. A imagem gerada compreende, pelo menos, um caractere de uma cadeia aleatória, na qual a posição de cada caractere na imagem é determinada pela ordem na qual aquele caractere aparece na cadeia aleatória. Assim, por exemplo, o primeiro caractere da cadeia aleatória pode ser exibido à esquerda superior da imagem enquanto que o último caractere da cadeia é exibido na direita inferior da imagem. A imagem gerada, de preferência, retém o mesmo padrão geral independente da cadeia aleatória de caracteres que são recebidos e é somente a configuração dos caracteres dentro do mesmo padrão geral que muda com cada cadeia aleatória. Por exemplo, o gerador de imagem 8 pode sempre gerar a imagem do bloco de teclas numérico, na qual a disposição dos numerais no bloco de teclas é modificada de acordo com a cadeira aleatória que é recebida. A figura 3 ilustra dados de imagem possíveis gerados pelo gerador de imagem 8 mediante o recebimento da cadeia "35492*0 Nº 6781".

Os dados de imagem gerados pelo gerador de imagem 8 devem ser entendidos como sendo quaisquer dados que o terminal do cliente 1 possa usar para modificar a aparência da tela 4. Por exemplo, onde a tela 4 compreende legendas configuráveis no bloco de teclas, os dados de imagem podem compreender nada mais que a cadeia aleatória recebida do gerador de imagem 7. O terminal de cliente 1 ao receber os dados de imagem então iria modificar a legenda da primeira tecla do bloco de teclas para exibir o primeiro caractere da cadeia aleatória, modificar a legenda da segunda tecla para exibir o segundo caractere da cadeia e assim por diante.

Aos dados de imagem gerados pelo gerador de imagem 8 para uma cadeia aleatória particular é designado o mesmo código de identificação como àquele recebido a partir do gerador de combinação 7 para aquela cadeia aleatória. De acordo com isso, com qualquer solicitação que for recebida do servidor de banco de dados 2, o servidor de segurança 3 gera dados de imagem e designa um código de identificação àqueles dados de imagem. O código de identificação é enviado a partir do servidor de segurança 3 para o servidor de banco de dados que, por sua vez, comunica o código de identificação ao terminal de cliente 1.

O terminal de cliente 1 usa o código de identificação para recuperar os dados de imagem correspondentes gerados pelo gerador de imagem 8 a partir do servidor de segurança 3. O terminal de cliente 1 então usa os dados de imagem recebidos para modificar a aparência da tela 4 de modo a apresentar ao usuário uma multiplicidade de caracteres (por exemplo, numerais, letras e símbolos etc) cujas posições estão aleatoriamente dispostas. Um usuário então insere seus dados de autorização ao selecionar os caracteres individuais formando seus dados de autorização, tal como um PIN, usando o dispositivo de entrada 5. Os dados de autorização inseridos pelo usuário são registrados como dados posicionais pelo terminal de cliente 1. Estes dados posicionais podem então ser convertidos pelo terminal de cliente 1 em dados de caracteres ou alguma outra forma de dados para enviar ao servidor de segurança 3. Por exemplo, se a imagem da figura 3 for exibida no terminal de cliente 1 e o usuário seleciona os numerais "7,9,2,0", então os dados posicionais podem ser "primeira-fila-primeira-coluna, terceira-fila,primeira-coluna, terceira-fila-segunda-coluna, segunda-fila-primeira-coluna'. Estes dados posicionais podem então ser convertidos para "1,7,8,4", o que corresponde à disposição dos numerais em um bloco de teclas numérico convencional. Por conseguinte, os dados posicionais ou os dados de caracteres ao qual podem ser convertidos representam uma forma codificada de dados de autorização. Estes dados de autorização codificados (por exemplo, "1,7,8") somente podem ser decodificados pelo conhecedor dos dados da imagem ou da cadeia aleatória específica àquele código de identi-

ficação e o processo utilizado para gerar os dados de imagem. Após os dados de autorização serem inseridos pelo usuário, os dados de autorização codificados e o código de identificação específico aos dados de imagem exibidos são enviados pelo terminal de cliente 1 ao servidor de segurança 3 onde os mesmos são decodificados pelo decodificador 9.

O decodificador 9 armazena cada cadeia aleatória e código de identificação recebido a partir do gerador de combinação 7. Quando os dados de autorização codificados e o código de identificação são recebidos do terminal de cliente 1, o decodificar 9 decodifica ou extrai os verdadeiros dados de autorização usando a correspondente cadeia aleatória, isto é, a cadeia aleatória que tem o mesmo código de identificação. Os dados de autorização decodificados são então enviados do decodificador 9 do servidor de segurança 3 para o servidor de banco de dados 2.

Em uso, primeiro o terminal de cliente 1 envia uma solicitação (S1) para acesso ao servidor de banco de dados 2. Esta solicitação por ser efetuada ao estabelecer uma conexão entre o terminal de cliente 1 e o servidor de banco de dados 2. Alternativamente, primeiro pode ser solicitado ao usuário a entrada dos dados de autorização parcial, por exemplo, o nome do usuário. Se os dados de autorização parcial forem válidos então isso então constitui uma solicitação de acesso. Uma vez recebida uma solicitação válida de acesso pelo servidor de banco de dados 2, o servidor de banco de dados 2 emite uma solicitação (S2) para um código de identificação de tela de terminal a partir do servidor de segurança 3. O servidor de banco de dados 2 também pode reconhecer a solicitação do terminal do cliente para acesso ao comunicar ao terminal de cliente um código de identificação de transação específico a esta solicitação de acesso. Este código de identificação de transação é diferente daquele código de identificação do servidor de segurança. O gerador de combinação 7 então gera uma cadeia aleatória e um código de identificação de tela de terminal (S3), dos quais ambos são comunicados ao gerador de imagem 8 e ao decodificador 9. O gerador de imagem 8 então gera dados de imagem (S4) adequados para exibir no terminal de cliente 1 e designa aos dados de imagem o mesmo código de iden-

tificação de tela de terminal.

O código de identificação de tela de terminal é enviado a partir do servidor de segurança 3 para o servidor de segurança 2 que, por sua vez, envia o código de identificação ao terminal de cliente 1(S5). De acordo com isso, o terminal de cliente 1 recebe a partir do servidor de banco de dados 2 um código único de identificação de transação específico à transação em andamento e também um código de identificação de tela de terminal. O terminal de cliente 1 então usa o código de identificação de tela de terminal para solicitar dados de imagem do servidor de segurança 3 (S6). Os dados de imagem gerados pelo gerador de imagem 8 específicos àquele código de identificação particular são então retornados pelo servidor de segurança 3 para o terminal de cliente 1 onde é exibido.

Então o usuário insere seus dados de autorização (S7) usando os dados de imagem apresentados no terminal de cliente 1. Devido à disposição aleatória dos caracteres exibidos no terminal de cliente 1, os dados de autorização inseridos pelo usuário são codificados. Os dados de autorização codificados e o código de identificação de tela de terminal são então enviados (S8) do terminal de cliente 1 ao servidor de segurança 3 onde são recebidos pelo decodificador 9. O decodificador 9 decodifica os dados de autorização codificados (S9) usando o código de identificação de tela de terminal para identificar a correspondente cadeia aleatória que foi usada para codificar os dados de autorização. Uma vez decodificados, os verdadeiros dados de autorização são comunicados (S10) a partir do servidor de segurança 3 para o servidor de banco de dados 2. Os dados de autorização verdadeiros são então verificados pelos meios de comunicação 6 (S11) e se os meios de verificação 6 determinam que os dados de autorização recebidos do servidor de segurança 3 são válidos, é concedido o acesso ao usuário ao servidor de banco de dados 2 (S12). Caso contrário, o servidor de banco de dados 2 comunica ao terminal de cliente 1 que os dados de autorização são inválidos (S13) e, de acordo com isso, a prática bancária atual convida o usuário a inserir novamente o seu PIN até o máximo de três tentativas. Se forem inválidas, o servidor de banco de dados 2 pode adicionalmente solicitar um novo

código de identificação de tela de terminal a partir do servidor de segurança 3 o qual também resultará, por sua vez, com novos dados de imagem sendo entregues ao terminal de cliente 1, de modo a iniciar um novo processo.

Os dados de imagem recuperados do servidor de segurança 3 pelo terminal de cliente 1 servem como o código para codificar os dados de autorização inseridos pelo usuário. Ao exibir os dados codificados no terminal 1 e usar os dados exibidos para inserir os dados de autorização do usuário, os dados inseridos pelo usuário são imediatamente codificados, isto é, o usuário na verdade insere dados de autorização codificados. Para isso, o terminal de cliente 1 não necessita separadamente codificar os dados inseridos pelo usuário. Em particular, o terminal de cliente 1 não recebe e então codifica os dados de autorização verdadeiros inseridos pelo usuário. Ao invés disso, o usuário, sem saber, insere os dados de autorização codificados. Em decorrência disso, não há necessidade para o terminal de cliente 1 incluir os meios de processamento para codificar a autorização a não ser que seja separadamente exigida para os propósitos de comunicação com o servidor de banco de dados e/ou o servidor de segurança. Na verdade, os dados de autorização codificados podem ser obtidos através do uso de um terminal burro, isto é, um terminal 1 compreendido de nada mais que meios de exibição 4 e meios de entrada 5.

Onde os meios de entrada 5 do terminal de cliente 1 tem uma multiplicidade de botões ou teclas que podem ser individualmente operadas que estão em posições fixas em relação umas com as outras e cada uma das quais é alocada a um respectivo caractere, o servidor de segurança 3 pode emitir ao terminal de cliente um 'mapa virtual' no qual as posições de teclas específicas do teclado, por exemplo, a seqüência alfanumérica, são todas alocadas para seus próprios identificadores. Cada identificador de posição é selecionado para ser diferente ao caractere real de tal tecla no teclado. Sendo assim, onde os identificadores são símbolos alfanuméricos, na verdade o mapa virtual troca quase todos caracteres pelas teclas individuais do teclado. Ao utilizar o mapa virtual para comunicar os toques de teclas do usuário ao servidor de segurança, apesar do teclado do usuário permanecer

o mesmo e os dados de autorização sejam inseridos da maneira usual, os dados de autorização inseridos pelo usuário que são comunicados de volta ao servidor de segurança 3 são codificados na forma de dados posicionais com relação ao mapa virtual. Este sistema é particularmente adequado, por exemplo, a circunstâncias tais como o uso de um PC residencial ao efetuar transações bancárias em linha.

O uso de códigos de identificação possibilita o acesso de múltiplos terminais de cliente 1 ao servidor de banco de dados 2 e ao servidor de segurança 3 simultaneamente. No entanto, o uso de códigos de identificação pode ser omitido caso o sistema de autorização seja configurado que somente um usuário, ou terminal de cliente 1, seja capaz de acessar o servidor de banco de dados 2 em qualquer única ocasião. Neste caso, os códigos de identificação não são necessários visto que somente uma cadeia aleatória é gerada e usada pelo servidor de segurança 3 em qualquer única ocasião.

Cada código de identificação pode consistir, ou incluir, um URL para um website. Os dados de imagem gerados pelo gerador de imagem 8 são então armazenados na forma de um documento web, por exemplo, arquivo HTML ou XML ou programa Java etc. Por conseguinte, um URL único e temporário é retornado ao terminal de cliente 1 em resposta a uma solicitação do terminal de cliente 1 para acesso ao servidor de banco de dados 2. O terminal de cliente 1 utiliza o URL para carregar o conteúdo do website relevante para exibir os dados de imagem. O URL, de preferência, não inclui dados que poderiam possibilitar uma falsificação.

Uma vez que o decodificador 9 tenha decodificado os dados de autorização codificados recebidos do terminal de cliente 1, a correspondente cadeia aleatória armazenada no decodificador 9 é, de preferência, excluída do servidor de segurança 3. Ao excluir a cadeia aleatória do servidor de segurança 3, uma pessoa que estiver interceptando os dados de autorização codificados fica impossibilitada de reenviar estes dados codificados ao servidor de segurança 3 com a finalidade de obter acesso ao servidor de banco de dados 2. Caso o decodificador 9 receba dados codificados que tem um código de identificação não existente, o servidor de segurança 3 pode ser

configurado para emitir um alerta de uma violação de segurança em potencial. Similarmente, os dados de imagem gerados pelo gerador de imagem 8 são também, de preferência, excluídos após o servidor de segurança 3 receber os dados de autorização codificados. Isso então impede outros, que tenham interceptado os dados de autorização codificados enviados a partir do terminal de cliente 1, de extrair o código de identificação de tela de terminal e solicitar os dados de imagem correspondentes a partir do servidor de segurança 3. Alternativamente, ou na verdade adicionalmente, os dados de imagem e/ou cadeia aleatória podem ter uma vida útil limitada, por exemplo 5 minutos, que é suficiente para a maioria das transações ATM. Em decorrência disso, o usuário pode ser interrompido caso consuma muito tempo em inserir seus dados de autorização.

Com o sistema de autorização descrito acima, os dados de autorização nunca são enviados sem codificação a partir do terminal de cliente 1. Não obstante, como os dados de autorização codificados enviados pelo terminal de cliente 1 são codificados usando uma cadeia aleatória, é extremamente difícil, senão impossível, para outros interceptarem somente os dados codificados para extrair os dados de autorização. Adicionalmente, como os dados de autorização são inseridos por seleção de caracteres que tem uma configuração aleatória, é significativamente mais difícil para uma pessoa observar o usuário para visualmente obter os dados de autorização do usuário.

A intenção é que a conexão de comunicação entre o servidor de banco de dados 2 e o servidor de segurança 3 seja segura por si própria, por exemplo, por meio de uma linha interna ou reservada que não é externamente acessível. Conseqüentemente, não há necessidade de codificar os dados de autorização enviados entre o servidor de segurança 3 e o servidor de banco de dados 2. No entanto, onde as comunicações entre o servidor de banco de dados 2 e o servidor de segurança 3 não são seguros, o decodificador 9 do servidor de segurança 3, de preferência, recodifica os dados de autorização decodificados usando um algoritmo de verificação de uma via antes de enviar os dados de autorização verificados ao servidor de banco de dados 2. Em vez de armazenar uma lista de dados de autorização reais, os

meios de verificação 6 do servidor de banco de dados 6, ao invés armazena somente dados de autorização verificados (hashed). Esta etapa adicional de verificação dos dados de autorização nunca é armazenada em uma forma não codificada tanto no servidor de banco de dados 2 quanto no servidor de segurança 3. Conseqüentemente, qualquer um que estiver comprometendo a segurança de qualquer um dos servidores 2,3 está impossibilitado de extrair os dados de autorização.

Com a finalidade de aperfeiçoar adicionalmente a segurança, todas as comunicações dentro do sistema de autorização, por exemplo, entre servidores 2,3 e com o terminal de cliente 1, de preferência, são criptografadas usando o protocolo SSL de 128 bit, por exemplo.

Importante, ao separar as diversas partes da informação de identificação do usuário e dados de autorização, a segurança inerente do sistema é muito intensificada. Com a finalidade de colocar em risco a conta do cliente, um observador deve capturar e decodificar as comunicações (i) entre o terminal de cliente 1 e o servidor de banco de dados 2; (ii) entre o terminal de cliente 1 e o servidor de segurança 3; e (iii) entre o servidor de segurança 3 e o servidor de banco de dados 2. Ao separar os fluxos de dados em três trajetórias distintas e separadas e com cada trajetória de dados portando significantemente menos dados, torna-se muito mais difícil, senão impossível, para um observador violar a segurança do sistema. Por conseguinte, mesmo que um observador seja bem-sucedido em decodificar um dos fluxos de dados, sem as informações contidas nos outros dois fluxos relacionados à mesma transação, as informações decodificadas são inúteis. Não obstante, como os dados de comunicação são comunicados ao servidor de banco de dados 2 em associação com o código de identificação de uma transação enquanto os dados de autorização são comunicados ao servidor de segurança 3 em associação com um código de identificação de tela de terminal, os dois fluxos de dados não tem dados em comum para possibilitar um observador determinar se os fluxos de dados estão relacionados à mesma conta.

A aquisição ilícita de dados de autorização pela interceptação de

ambos os dados de imagem e os dados de autorização codificados enviados entre o terminal de cliente 1 e o servidor de segurança 3 podem ser solapados pelo aperfeiçoamento adicional da segurança do sistema de autorização com a criptografia dos dados de imagem e os dados de autorização codificados com diferentes chaves de criptografia. Ao utilizar diferentes chaves de criptografia, a tarefa de decriptografia dos dados para obter os dados de autorização é mais do que duplicada. Isso é em razão da tarefa de decriptografia tornar-se muito mais difícil à medida que o tamanho dos dados criptografados decrescem. Como os dados de imagem compreendem um pouco mais que uma cadeia aleatória de caracteres (por exemplo, numerais de 0-9) e os dados de autorização codificados podem compreender um pouco mais que alguns caracteres selecionados (por exemplo, um PIN), o tamanho dos dados a serem criptografados é extremamente resistente aos processos de força bruta da decriptografia.

Chaves separadas de criptografia para os dados de imagem e dados de autorização codificados é possível ao utilizar duas trajetórias de comunicação entre o terminal de cliente 1 e o servidor de segurança 3, com cada trajetória de comunicação utilizando uma chave diferente de criptografia. Por exemplo, o servidor de segurança 3 pode incluir dois servidores, o primeiro servidor armazenando os dados de imagem gerados pelo gerador de imagem 8 e o segundo servidor armazenando os dados de autorização codificados recebidos do terminal de cliente 1. O terminal de cliente 1 então solicita os dados de imagem do primeiro servidor, que estão criptografados usando uma primeira chave e envia os dados de autorização codificados ao segundo servidor usando uma segunda chave de criptografia.

Apesar do sistema de autorização, de preferência, incluir um servidor de banco de dados 2 separado e um servidor de segurança 3, o gerador de combinação 7, o gerador de imagem 8 e o decodificador 9 podem todos formar parte do servidor de banco de dados 2. Neste caso, o servidor de segurança 3 é omitido e o terminal de cliente 1 somente se comunica com o servidor de banco de dados 2. O servidor de banco de dados 2, mediante o recebimento de uma solicitação de acesso do terminal de cliente

1, retorna um código de identificação e dados de imagem ao terminal de cliente 1. O terminal de cliente 1 então envia os dados de autorização codificados e o código de identificação ao servidor de banco de dados 2, por meio do qual os dados de autorização codificados são decodificados e sua validade verificada. Conforme descrito acima, para o servidor de segurança 3, o servidor de banco de dados 2 pode incluir dois servidores utilizando duas chaves de criptografia diferentes para separadamente comunicar os dados de imagem e os dados de autorização codificados. O primeiro servidor é responsável pelo recebimento de uma solicitação para acesso do terminal de cliente 1 e retorno do código de identificação e dos dados de imagem, enquanto que o segundo servidor é responsável pelo recebimento da autorização codificada e do código de identificação do terminal de cliente 1.

Enquanto até então foi feita referência a um sistema de autorização para obter o acesso aos dados armazenados no servidor de banco de dados 2, o sistema de autorização pode ser utilizado em qualquer situação na qual há necessidade de autorização a ser remotamente verificada. Por exemplo, o sistema de autorização pode ser usado para obter acesso a um edifício seguro. Neste caso, o terminal de cliente 1 pode ser um bloco de teclas adjacente à porta e o servidor de banco de dados 2 mediante o recebimento de dados de autorização válidos a partir do servidor de segurança 3 envia um sinal para que a porta seja aberta.

Com o sistema de autorização e o processo da presente invenção, a autorização de um usuário pode ser remotamente verificada, através de comunicações potencialmente não seguras, de um modo mais seguro do que atualmente possível. Em particular, a autorização do usuário pode ser verificada sem dados sendo enviados pelo usuário que, se interceptado, podem ser usados para extrair os dados de autorização do usuário.

Um outro desenvolvimento do sistema de autorização e processo descrito acima está ilustrado na figura 4; o sistema é similar ao do sistema ilustrado na figura 1 e do mesmo modo, onde apropriados, foram usados numerais de referência. Este desenvolvimento adicional é particularmente adequado para a utilização com um terminal de cliente 1 que tem uma tela

tal como um tela de LCD, plasma ou CRT. O servidor de banco de dados 2, adicionalmente, inclui uma tabela de conferência 11 na qual é armazenada uma relação de usuários ou clientes com cada usuário designado a um código padrão tal como um cadeia alfanumérica que é, de preferência, mas não necessariamente, única a um usuário individual. No servidor de segurança 3, está provido adicionalmente um decodificador de dados de tela 12. O decodificador de dados de tela 12 é programado para decodificar os códigos padrão de cada usuário e a comunicar os dados padrão ao gerador de imagem 8.

Os dados padrão definem aspectos da imagem a ser exibida por um terminal de cliente quando o usuário do terminal está sendo solicitado a inserir seus dados de autorização tal como um número PIN. Subseqüentemente, a página web que é apresentada é adequada e, de preferência, é única para cada usuário. Além disso, o mesmo usuário é apresentado à mesma página web, porém o padrão da página web varia entre os usuários. Exemplos do que os dados padrão podem definir são: o tamanho da fonte de cada página web; a cor das teclas a serem selecionadas individualmente; a coloração da borda em torno das teclas; bem como quaisquer detalhes decorativos tais como imagens padrão ou adicionais.

A figura 5 ilustra uma página web com uma borda padronizada retilínea para um bloco de teclas eletrônico alfanumérico. Sem dúvida, é óbvio que as variações de projetos de página web não estão limitadas aos exemplos apresentados acima e que há um número extremamente amplo de características de projeto que podem variar sem se afastar da função da página web que é a de possibilitar ao usuário a inserir os seus dados de autorização.

Com o sistema de autorização ilustrado na figura 4, o processo de autorização é conforme se segue. O terminal remoto 1 solicita o acesso (S20) ao servidor de banco de dados 2. Em resposta o servidor de banco de dados 2 informa o terminal remoto da sessão de identidade para esta sessão de comunicação e solicita ao terminal remoto a identificação preliminar do usuário que está pedindo o acesso. Isso pode ser o nome do usuário ou seu

número de conta, por exemplo. Uma vez que o usuário tenha inserido sua identificação preliminar, o terminal remoto 1 comunica as informações de identificação com a sessão de identificação para o servidor de banco de dados 1. O servidor de banco de dados 2 identifica, a partir da tabela de conferência 11, o código padrão daquele usuário (21) e comunica o código padrão ao servidor de segurança 3 com a solicitação de uma nova sessão (S22). O servidor de segurança 3 determina a partir do código padrão (23) os aspectos padrão para a página de registro específica para aquele usuário. Opcionalmente, uma disposição aleatória do botão individual do bloco de teclas é gerada (24), conforme descrito acima com referência à figura 2. O gerador de imagem 8 então cria uma página de identificação de usuário (S25) utilizando os aspectos padrão do usuário e comunica à URL para aquela página de identificação de usuário com uma sessão separada de identificação à sessão de comunicação com relação àquele usuário entre o servidor de banco de dados e o servidor de segurança (S26). O servidor de banco de dados 2 então comunica a URL ao terminal remoto 1 que acessa a URL (S27) e exibe a página web de registro de identificação para aquele usuário. Presumindo que a página web de registro de identificação seja familiar ao usuário, os dados de autorização do usuário são então inseridos (S28) e comunicados pelo terminal remoto 1 em sua forma codificada em decorrência do rearranjo do bloco de teclas ao servidor de segurança 3 (S29). O servidor de segurança 3, subseqüentemente, decodifica os dados da chave posicional (S30) para identificar os dados de autorização verdadeiros do usuário que então são comunicados ao servidor de banco de dados 2 (S31) usando a sessão de identificação única para a sessão de comunicação entre o servidor de banco de dados e o servidor de segurança. O servidor de banco de dados 2 então confere (S32) os dados de autorização recebidos do servidor de segurança 3 com os dados de autorização que já foram registrados para aquele usuário. Presumindo que os dados de autorização estejam corretos, o servidor de banco de dados 2 então concede o acesso (S33) para o sistema seguro solicitado pelo usuário no terminal remoto 1 ou recusa o acesso (S34) onde os dados de autorização estão incorretos.

Conseqüentemente, ficará óbvio a partir do acima mencionado que, similares ao processo de autorização da figura 2, a informação necessária de autorização é fragmentada em segmentos e diferentes segmentos são trocados entre diferentes combinações de comunicação do terminal remoto, do servidor de banco de dados e do servidor de segurança. Nenhuma das comunicações individuais contém todos os dados de identificação e de autorização. Além disso, os pacotes de dados individuais, cada um dos quais é, de preferência, criptografado, não são suficientemente grandes para possibilitar alguém a violar o criptografia usando técnicas atuais de violação de códigos. Os dados de identificação e de autorização são fragmentados em, pelo menos, dois segmentos utilizando uma sessão diferente de identificação e uma conexão diferente de comunicação.

Está previsto que um usuário possa ter a oportunidade de selecionar suas próprias variações de padrão que então são armazenadas na tabela de conferência 11 do servidor de banco de dados 2. No entanto, isso iria exigir uma ampla faixa de variações de padrão a ficar disponíveis publicamente. Por isso, é preferível que as variações de padrão sejam selecionadas pelo banco de modo que as permutações disponíveis sejam mantidas confidenciais.

Com este sistema os usuários são encorajados a se familiarizarem com o padrão da página web que é apresentada aos mesmos toda vez que forem solicitados os seus dados de autorização. Esta familiarização com a sua própria página web, de preferência única, significa que se for efetuada uma tentativa para obter dados de autorização de usuário por fraude, o usuário será apresentado a uma página de web que não inclui os por menores de padrão com os quais o usuário se tornou familiarizado. Isso possibilita um usuário a distinguir entre uma página web válida emitida pelo banco e uma página web falsificada.

Evidentemente, será óbvio que este sistema que apresenta cada usuário com sua própria página web personalizada registrada não envolve, adicionalmente, a reorganização da disposição das teclas ou botões individuais. Isso quer dizer que o gerador de combinação 7 é opcional na figura 4.

No entanto, mesmo com a reorganização de teclas ou botões, o sistema ainda oferece uma segurança aperfeiçoada sobre os sistemas conhecidos na medida que os dados de autorização inseridos pelo usuário são comunicados ao servidor de segurança 3 sob uma identidade de comunicação única à transação entre o terminal remoto e o servidor de segurança e é separada da identidade de comunicação designada à comunicação entre o terminal de cliente 1 e o servidor de banco de dados 2. Por conseguinte, a identidade do usuário que é comunicada ao servidor de banco de dados 2 permanece separada dos dados de autorização que são comunicados ao servidor de segurança 3. Portanto, a comunicação de três vias descrita acima no que refere-se ao sistema de autorização da figura 1 também é apresentada com o sistema de autorização da figura 4.

Sem dúvida, onde o gerador de combinação 7 é adicionalmente executado no sistema de autorização em um nível até superior de segurança pode ser obtido e remete totalmente a preocupações sobre riscos de roubo de senhas bem como as preocupações que cartões podem ser roubados uma vez que o número PIN tenha sido monitorado.

O sistema de autorização da figura 1 foi descrito com relação à necessidade de uma série de chaves ou botões numérica e individualmente rotulados a serem exibidos. No entanto, com a finalidade de oferecer um nível adicional de segurança, a presente invenção considera a opção de que as teclas ou botões sejam individualmente rotulados com uma mistura de números e letras a serem ilustradas na figura 6. Com este aspecto adicional, a página web registrada iria apresentar uma disposição de uma multiplicidade de teclas, paro exemplo, uma ordenação de 3 x 4, que não inclui uma tecla para cada possível número ou letra. No entanto, conforme determinado pelo código padrão armazenado na tabela de conferência 11, a página web irá incluir os números e letras que o usuário necessita para inserir seu código de autorização. De modo que se alguém deseja efetuar uma cópia da página registrada para os propósitos de obtenção ilícita de senha precisa não somente adivinhar o conjunto correto de aspectos padrão para cada usuário a partir de uma ampla faixa de permutações padrão possíveis, porém

agora precisa também selecionar de uma faixa de dez números e vinte e seis letras (presumindo o alfabeto inglês) o subgrupo correto de letras e números que compõe os dados de autorização para aquele usuário.

Um desenvolvimento adicional do mesmo projeto envolve o uso de gráficos não alfanuméricos para cada tecla. Conforme ilustrado na figura 7, desenhos ou imagens concisos de qualquer caractere distinguível podem ser utilizados com o sistema de autorização. Deste modo, as teclas na figura 7 abrangem imagens de desenhos de veículo, uma nuvem, uma flor um copo etc. Estes caracteres são, além do padrão distinto do bloco de teclas como um todo o qual, neste caso, abrange uma borda de círculos adjacentes. O usuário então seleciona as três ou quatro teclas do conjunto de teclas que constituem os seus dados de autorização. Na figura 7, os dados de autorização compreendem 1) um carro, 2) uma nuvem de chuva, 3) um sol e 4) um vaso de flores.

Com um conjunto de, por exemplo, 256 caracteres ou símbolos diferentes e uma ordenação de 12 teclas, há $6,1 \times 10^{28}$ combinações possíveis que podem ser exibidos para um usuário. Da mesma forma, com os mesmos 256 caracteres diferentes há 4,2 bilhões de PINs de 4 caracteres diferentes. Em decorrência disso, a chance de um usuário ser capaz de inserir um PIN, se for efetuada uma tentativa de obtenção ilegal de senha, é 1 em 3,4 milhões.

Além disso, acredita-se que este desenvolvimento adicional do sistema de autorização pode oferecer vantagens adicionais aos usuários. Isso é devido ao fato de que muitos usuários sentem dificuldades em lembrar seus dados de autorização tais como o seu número PIN. Acredita-se que os usuários irão achar estas imagens mais fáceis de relembrar individualmente e em sua ordem correta à medida que as mesmas são mais adequadas para reunir por meio de uma seqüência ou história cognitiva.

Um benefício adicional do sistema seguro da figura 4 é que, pelo padrão do teclado exibido a um usuário, o mesmo pode ser selecionado para ajustar deficiências de visão. Por exemplo, as imagens exibidas poderiam ser apresentadas com um contraste superior ao normal ou maior que o nor-

mal para aqueles com visão restrita. O que também está previsto é que os dados padrão poderiam incorporar características de áudio para usuários que tenham uma acuidade visual extremamente limitada ou nenhuma acuidade visual. Particularmente nestes casos onde o terminal remoto é um computador residencial, cada uma das teclas individuais da tela podem ser alocadas a um som separado, de preferência uma breve descrição do caractere da tecla. Será então permitido a um usuário passar através das teclas para ouvir os diferentes sons sem que as teclas sejam selecionadas. Ao ouvir uma tecla específica ao código de autorização do usuário, um usuário então será capaz de selecionar a tecla ao pressionar a tecla Enter em seu teclado, por exemplo. Alternativamente, o sistema pode ser adaptado de modo que as teclas somente sejam selecionadas se a mesma tecla for selecionada duas vezes sucessivamente. De modo que a primeira seleção da tecla pelo usuário somente desencadeia uma descrição de áudio da tecla, repetindo a seleção depois disso iria então tratar a tecla como selecionada para os propósitos do código de autorização do usuário. Sem dúvida, será entendido que está invenção pretende abranger procedimentos alternativos para possibilitar um usuário ouvir os diferentes sons associados com as teclas sem selecionar as teclas para propósitos de inserir a código de autorização do usuário. Deste modo, a presente invenção adicionalmente oferece aos usuários portadores de deficiências visuais o benefício de acesso eletrônico a dados seguros, tais como transações bancárias residenciais, previamente não disponíveis aos mesmos.

Enquanto que os sistemas de comunicação seguros acima descritos estão relacionados com dados de autorização de comunicação, isso será, sem dúvida óbvio que o processo seguro de comunicações incorporado nestes sistemas é adequado para a comunicação de qualquer informação susceptível e, em particular, a etapa de verificação da validade dos dados de autorização inseridos pelo usuário não é uma característica essencial da invenção.

Os sistemas de autorização da presente invenção, por conseguinte, oferecem segurança significativamente aperfeiçoada sobre os siste-

mas de registro eletrônico à medida que os mesmos podem violar a identificação e os dados de autorização em uma multiplicidade de segmentos com, pelo menos, um dos segmentos sendo comunicado sob um código diferente de sessão de identificação àquele de um outro segmento e/ou uma conexão diferente de comunicações. O sistema de autorização da figura 4 adicionalmente oferece um risco significativamente reduzido de um cliente ou usuário possa ser induzido a erro ao inserir seus dados de autorização em um site falsificado. Acredita-se que como as fraudes de roubo de senhas representam custos bancários e perdas para empresas de cartões de crédito em torno de $10 bilhões em 2003, atualmente, a necessidade de recorrer a este seguro de risco é acentuada.

Apesar de somente algumas poucas incorporações exemplares ou a presente invenção ter sido acima descrita em por menores, aqueles versados na técnica prontamente irão considerar que são possíveis muitas modificações nas incorporações apresentadas exemplares sem distanciar-se materialmente dos recentes ensinamentos e vantagens da presente invenção. Em conformidade com isso, todas tais modificações tencionam serem incluídas na área da presente invenção conforme definido nas reivindicações que se seguem.

REIVINDICAÇÕES

1. Processo de comunicação segura entre um servidor e um terminal remoto a partir do servidor, sendo que o terminal inclui um dispositivo de entrada de dados operado pelo usuário, compreendendo o processo de comunicação segura as etapas de:

dados codificados de comunicação a partir do servidor para o terminal, sendo os dados codificados específicos a um evento de comunicação; gerando dados posicionais a partir dos dados inseridos pelo usuário usando o dispositivo de entrada de dados do terminal no que refere-se aos dados codificados, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário do dispositivo de entrada de dados;

comunicando os dados posicionais a partir do terminal ao servidor; e decodificando os dados posicionais recebidos pelo servidor usando os referidos dados de codificação para gerar os dados de entrada do usuário.

2. Processo de acordo com a reivindicação 1, em que o terminal inclui um tela e o processo adicionalmente compreende a etapa de exibição de uma multiplicidade de caracteres na tela, sendo a disposição de cada um dos caracteres na tela determinada com relação aos referidos dados codificados.

3. Processo de acordo com as reivindicações 1 ou 2, compreendendo adicionalmente a etapa de geração dos referidos dados codificados em resposta a uma solicitação do referido terminal para um evento de comunicação.

4. Processo de acordo com as reivindicações 2 ou 3, em que os dados codificados identificam a disposição dos caracteres exibidos.

5. Processo de acordo com a reivindicação 4, em que a multiplicidade de caracteres exibidos inclui as séries numéricas 0,1,2,3,4,5,6,7,8,9.

6. Processo de acordo com a reivindicação 4, em que a multiplicidade de caracteres exibidos compreendem um sub-conjunto de um conjunto completo de caracteres alfanuméricos.

7. Processo de acordo com a reivindicação 4, em que a multipli

cidade de caracteres exibidos compreendem caracteres não-alfanuméricos que podem ser distinguidos pelo usuário.

8. Processo de acordo com a reivindicação 7, em que os dados codificados incluem um sub-conjunto de caracteres não-alfanuméricos extraídos de um conjunto mais amplo de caracteres não-alfanuméricos.

9. Processo de acordo com a reivindicação 8, em que o sub-conjunto de caracteres a ser exibido é selecionado a partir de um conjunto de caracteres alfanuméricos e não-alfanuméricos.

10. Processo de acordo com a reivindicação 5, em que os referidos dados codificados compreendem uma cadeia de numerais em ordem aleatória.

11. Processo de acordo com a reivindicação 10, em que a referida etapa de geração de dados codificados compreende a seleção aleatória de uma cadeia de caracteres a partir de uma tabela de cadeias de caracteres, tendo cada cadeia de caracteres na referida tabela uma ordem diferente.

12. Processo de acordo com qualquer uma das reivindicações de 2 até 9, em que os referidos dados codificados compreendem dados de imagem capazes de serem exibidos em uma tela de um terminal.

13. Processo de acordo com a reivindicação 12, compreendendo adicionalmente a etapa de comunicação ao terminal a URL de um website no qual os dados codificados são incorporados no referido website e a etapa de exibição de uma multiplicidade de caracteres na tela compreender a exibição do conteúdo do website na tela.

14. Processo de acordo com a reivindicação 1, em que o referido dispositivo de entrada é um teclado e os referidos dados codificados compreendem uma mapa virtual designando identificadores únicos a cada das posições de um grupo selecionado de teclas no teclado.

15. Processo de acordo com qualquer uma das reivindicações precedentes, em que os referidos dados codificados e referidos dados posicionais são comunicados através de trajetórias de comunicação diferentes.

16. Processo de acordo com qualquer uma das reivindicações

precedentes, em que os dados comunicados entre o servidor e o terminal são criptografados usando criptografia de chave pública.

17. Processo de acordo com a reivindicação 16, em que os referidos dados codificados e os referidos dados posicionais são comunicados através de trajetórias de comunicação diferentes e cada um é criptografado usando uma chave de criptografia diferente.

18. Processo de acordo com qualquer uma das reivindicações de 15 até 17, em que os dados codificados são gerados por um servidor de segurança que está comunicado ao referido servidor e a partir do referido servidor ao referido terminal remoto e os referidos dados posicionais estão comunicados pelo terminal ao referido servidor de segurança onde os dados posicionais são decodificados para os dados inseridos pelo usuário a ser comunicados a partir do servidor de segurança ao referido servidor.

19. Processo de comunicação segura entre um servidor e um terminal remoto a partir do servidor, o terminal incluindo um dispositivo de entrada de dados operada pelo usuário e uma tela, sendo o processo de comunicação segura composto das etapas de:

a emissão de uma solicitação para comunicação ao servidor a partir do terminal remoto e fornecimento de dados de identificação de usuário preliminares específicos ao usuário do terminal;

da identificação de dados padrão específicos ao usuário e comunicação de dados exibidos a partir do servidor ao terminal com base nos dados padrão identificados; e

da geração de uma imagem na tela do terminal com base nos dados de tela exibidos recebidos a partir do servidor

em que são inseridos dados susceptíveis adicionais pelo usuário somente quando a imagem na tela corresponde à imagem previamente produzida conhecida do usuário.

20. Processo de acordo com a reivindicação 19, compreendendo adicionalmente etapas de:

de comunicação de dados codificados do servidor para o terminal, sendo os dados codificados específicos ao evento de comunicação;

de geração de dados posicionais a partir de dados subseqüentemente inseridos por um usuário usando um dispositivo de entrada de dados do terminal no que refere-se aos dados codificados, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionáveis pelo usuário do dispositivo de entrada de dados;

de comunicação de dados posicionais a partir do terminal ao servidor; e

de decodificação dos dados posicionais recebidos do servidor usando os referidos dados codificados para gerar os dados inseridos pelo usuário.

21. Processo de acordo com uma das reivindicações 19 ou 20, em que os dados exibidos incluem dados em um ou mais de: um modelo de borda pré-selecionada; uma ou mais colorações pré-selecionadas e uma forma de botão pré-selecionada.

22. Processo de acordo com a reivindicação 21, em que para usuários com deficiência visual os dados exibidos incluem dados de um ou mais dos seguintes itens: colorações de alto contraste pré-selecionáveis e caracteres selecionáveis maiores que os normais.

23. Processo de acordo com qualquer uma das reivindicações de 19 a 22, em que dados de áudio relacionados aos dados exibidos são comunicados ao terminal a partir do servidor.

24. Processo de acordo com a reivindicação 23, em que os dados de áudio incluem sons identificáveis para cada caractere a ser selecionado pelo usuário dos dados exibidos.

25. Sistema de comunicação segura que compreende um servidor e, pelo menos, um terminal remoto a partir do servidor e em comunicação bidirecional com o servidor, sendo o servidor compreendido de: um codificador para gerar dados codificados específicos para um evento de comunicação; uma interface de comunicações para comunicar os dados codificados para o terminal remoto e para receber dados posicionais a partir do terminal, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário e sendo uma codificação dos dados

inseridos pelo usuário; e um decodificador para decodificar os dados posicionais recebidos a partir do terminal, usando o decodificador os dados codificados do codificador para decodificar os dados posicionais e sendo cada terminal compreendido de: um dispositivo de entrada manualmente operado para a entrada de dados do usuário que estão codificados como dados posicionais; e uma interface de comunicações terminal para receber dados codificados a partir do servidor e para comunicar os dados posicionais ao servidor.

26. Sistema de comunicações seguras de acordo com a reivindicação 25, em que o terminal adicionalmente compreende uma tela na qual uma multiplicidade de caracteres são exibidos, sendo a posição de cada um dos caracteres na tela determinados com relação aos referidos dados codificados.

27. Sistema de comunicações seguras de acordo com qualquer uma das reivindicações 25 ou 26, em que os dados inseridos pelo usuário compreendem os dados de autorização e o servidor adicionalmente inclui a armazenagem de dados na qual os dados de autorização válidos estão armazenados em comparação com os quais os dados de autorização decodificados são validados.

28. Sistema de comunicações seguras de acordo com qualquer uma das reivindicações de 25 até 27, em que o codificador inclui uma armazenagem de dados codificados na qual está armazenada uma tabela de cadeia de caracteres, tendo cada cadeia de caracteres uma ordem diferente, por meio da qual o codificador gera os dados codificados pela seleção aleatória de uma cadeia de caracteres a partir da tabela de cadeias de caracteres.

29. Sistema de comunicações seguras de acordo com as reivindicações de 26 até 27, em que o servidor inclui uma armazenagem de dados padrão de tela de usuário na qual são armazenados dados padrão específicos a cada usuário, ordenando os dados padrão características de uma imagem a ser exibida na tela do terminal.

30. Sistema de comunicações seguras de acordo com qualquer

uma das reivindicações de 25 até 29, em que o servidor e, pelo menos, cada terminal remoto compreender meios de criptografia de chave pública para criptografar comunicações entre o servidor e o terminal.

31. Sistema de comunicações seguras de acordo com qualquer uma das reivindicações de 25 até 30, em que o servidor tem meios de comunicação separados para comunicar os dados codificados para o terminal e para receber dados posicionais a partir do terminal de modo tal que os dados codificados e os dados posicionais são comunicados entre o terminal e o servidor através de trajetórias de comunicação diferentes.

32. Servidor de comunicação segura compreendido de um codificador para gerar dados codificados específicos a um evento de comunicação; uma interface de comunicações para comunicar os dados codificados para um terminal remoto e para receber dados posicionais do terminal remoto, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário e sendo uma codificação de dados inseridos pelo usuário; e um decodificador para decodificar dados posicionais recebidos do terminal, usando o decodificador os dados codificados do codificador para decodificar os dados posicionais.

33. Sistema de comunicação segura compreendido de um servidor e, pelo menos, um terminal remoto a partir do servidor e em comunicação bidirecional com o servidor, o servidor compreendido de: armazenagem de dados padrão de usuário no qual são armazenados dados exibidos específicos a cada usuário; e uma interface de comunicações para comunicar os dados exibidos para o terminal remoto e para receber os dados inseridos pelo usuário a partir do terminal, e cada terminal compreendido de: um dispositivo de entrada de dados, operado pelo usuário para a entrada de dados do usuário; uma tela e uma interface de comunicações de terminal para receber os dados exibidos a partir do servidor e para comunicar os dados inseridos pelo usuário ao servidor.

34. Sistema de comunicação segura de acordo com a reivindicação 33, em que os dados inseridos pelo usuário compreendem os dados de autorização e o servidor adicionalmente inclui a armazenagem de dados na

qual os dados de autorização válida estão armazenados contra o qual são comparados os dados de autorização inseridos pelo usuário.

35. Sistema de comunicação segura de acordo com qualquer uma das reivindicações 33 ou 34, em que cada terminal remoto inclui um ou mais microfones e os dados exibidos comunicados ao terminal a partir do servidor incluem dados de áudio.

36. Sistema de comunicação segura de acordo com qualquer uma das reivindicações de 33 até 35, em que o servidor ainda inclui um codificador para gerar dados codificados específicos a um evento de comunicação e um decodificador para decodificar dados posicionais recebidos do terminal, consistindo nos dados posicionais de identificadores para as posições dos caracteres selecionados pelo usuário e sendo uma codificação de dados inseridos pelo usuário, usando o decodificador os dados codificados do codificador para decodificar os dados posicionais e caracterizado pelo fato de que a interface de comunicações está adaptada para comunicar os dados codificados ao terminal remoto e para receber os dados posicionais a partir do terminal.

37. Sistema de comunicações seguras de acordo com a reivindicação 36, em que o codificador inclui uma armazenagem de dados codificados na qual é armazenada uma tabela de cadeia de caracteres, tendo os caracteres em cada cadeia de caracteres uma ordem diferente, por meio da qual o codificador gera os dados codificados pela seleção aleatória de uma cadeia de caracteres a partir da tabela de cadeias de caracteres.

38. Sistema de comunicações seguras de acordo com qualquer uma das reivindicações de 33 até 37, em que o servidor e, pelo menos, um terminal remoto cada adicionalmente compreende meios de criptografia de chave pública para criptografar as comunicações entre o servidor e o terminal.

39. Sistema de comunicações seguras de acordo com a reivindicação 38, em que o servidor tem meios de comunicação separados para comunicar os dados exibidos para o terminal e para receber os dados inseridos pelo usuário a partir do terminal de modo tal que os dados exibidos e os

dados inseridos pelo usuário são comunicados entre o terminal e o servidor através de trajetórias diferentes de comunicação.

40. Servidor de comunicação segura compreendido de: armazenagem de dados padrão de usuário na qual são armazenados dados exibidos específicos a cada usuário; e uma interface de comunicações para comunicar os dados exibidos para o terminal remoto e para receber os dados inseridos a partir do terminal.

41. Processo de comunicação segura entre o servidor e um terminal remoto a partir do servidor substancialmente como aqui descrito anteriormente com referência aos desenhos anexos.

42. Sistema de comunicação segura substancialmente como aqui descrito anteriormente com referência aos desenhos anexos

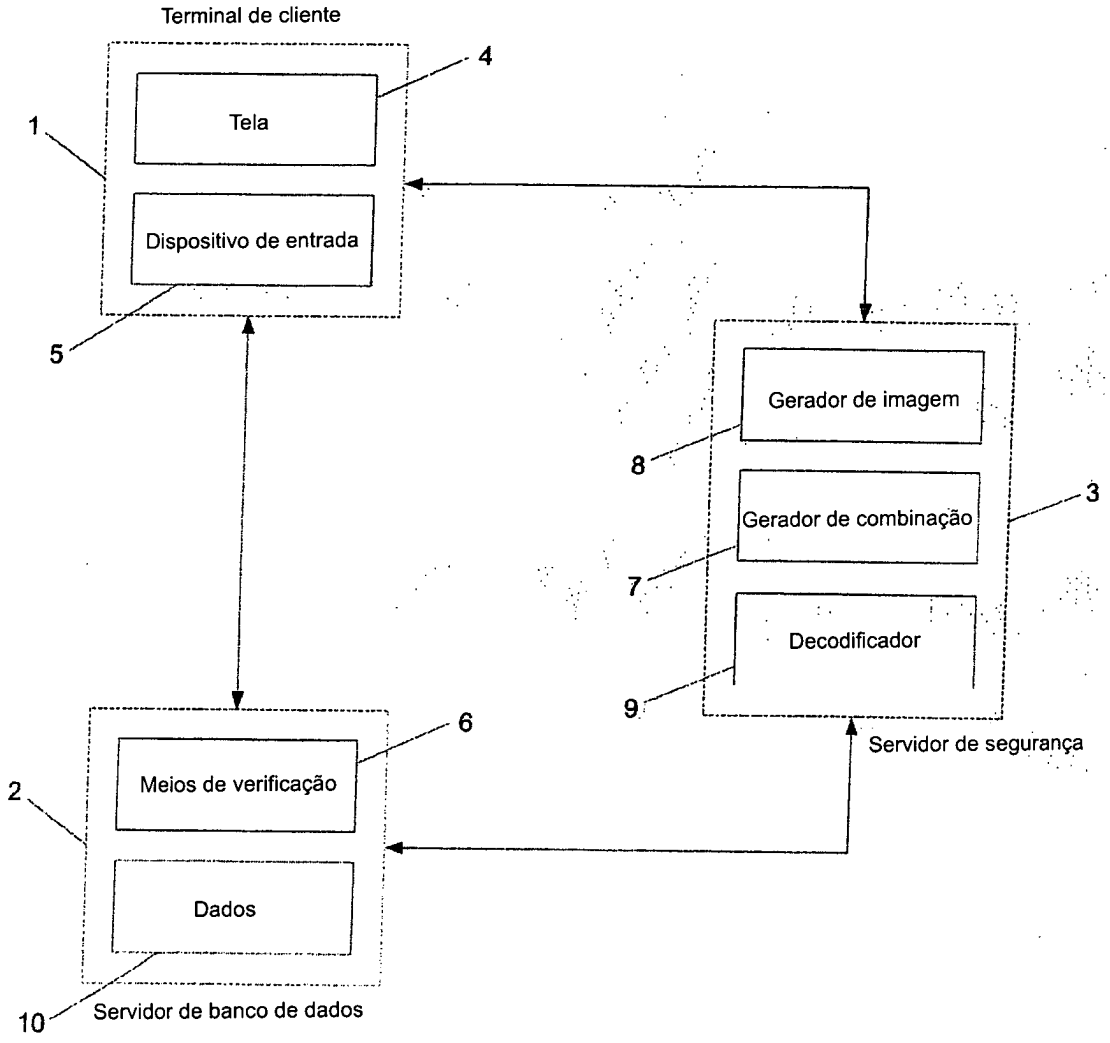

Terminal de cliente
4
Tela
1
Dispositivo de entrada
5
Gerador de imagem
8
Gerador de combinação
3
7
Decodificador
9
Servidor de segurança
6
Meios de verificação
2
Dados
10
Servidor de banco de dados

Fig.1

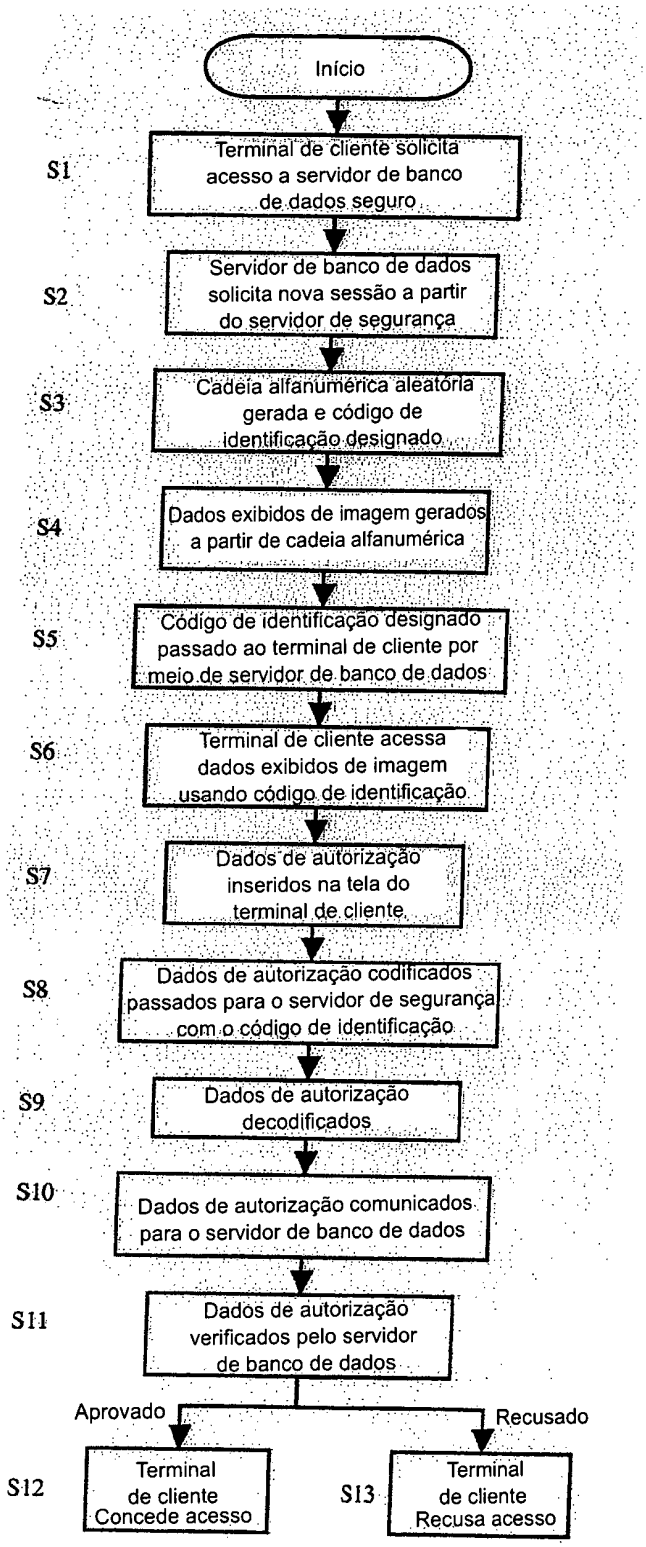

Início
S1
Terminal de cliente solicita acesso a servidor de banco de dados seguro
S2
Servidor de banco de dados solicita nova sessão a partir do servidor de segurança
S3
Cadeia alfanumérica aleatória gerada e código de identificação designado
S4
Dados exibidos de imagem gerados a partir de cadeia alfanumérica
S5
Código de identificação designado passado ao terminal de cliente por meio de servidor de banco de dados
S6
Terminal de cliente acessa dados exibidos de imagem usando código de identificação
S7
Dados de autorização inseridos na tela do terminal de cliente
S8
Dados de autorização codificados passados para o servidor de segurança com o código de identificação
S9
Dados de autorização decodificados
S10
Dados de autorização comunicados para o servidor de banco de dados
S11
Dados de autorização verificados pelo servidor de banco de dados
Aprovado
Recusado
S12
Terminal de cliente Concede acesso
S13
Terminal de cliente Recusa acesso

Fig.2

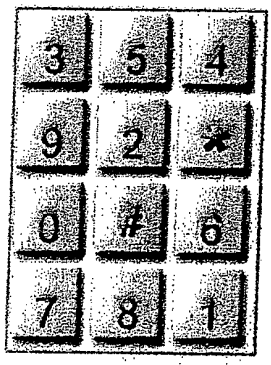


Fig.3

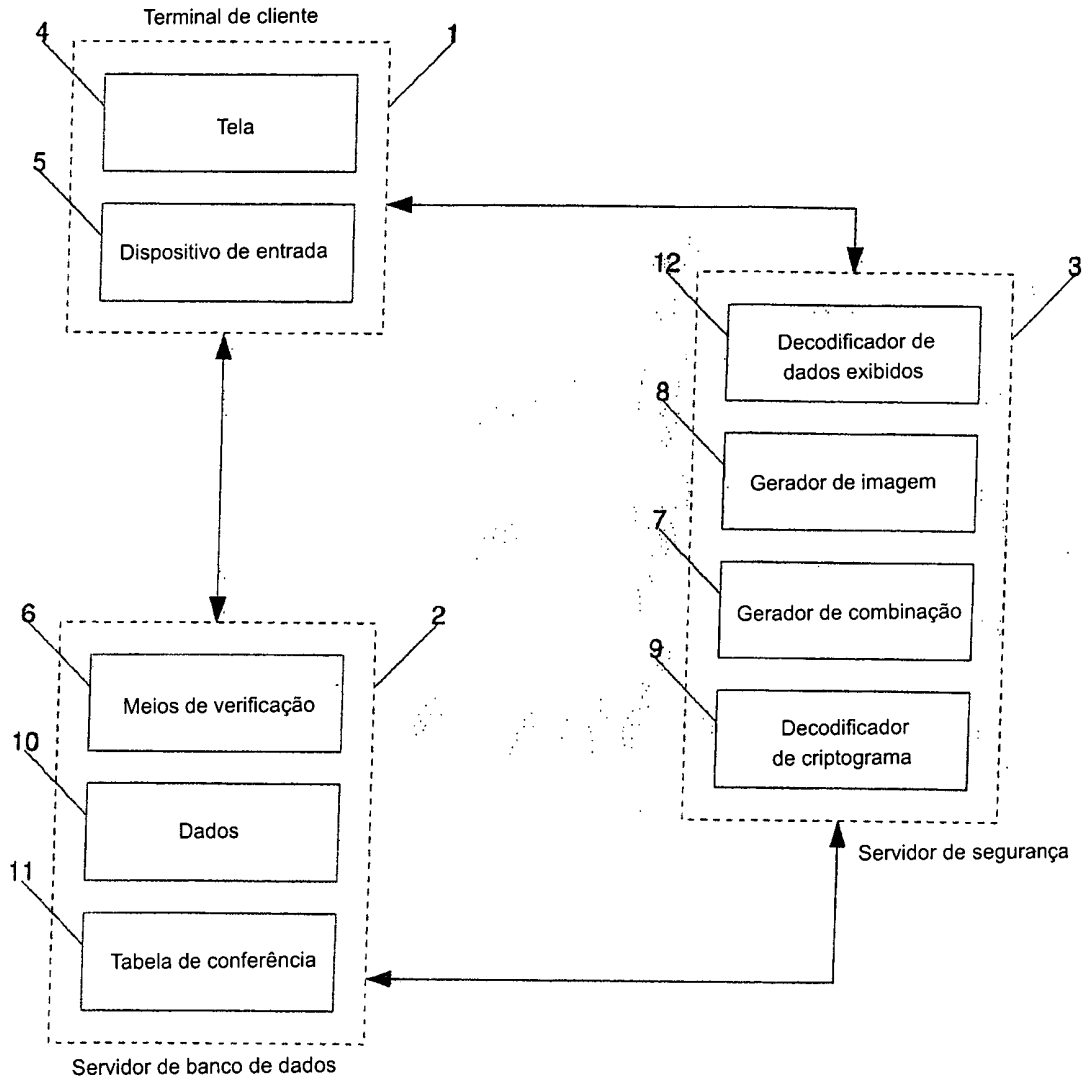

Terminal de cliente
4
1
Tela
5
Dispositivo de entrada
12
3
Decodificador de dados exibidos
8
Gerador de imagem
7
Gerador de combinação
9
Decodificador de criptograma
Servidor de segurança
6
2
Meios de verificação
10
Dados
11
Tabela de conferência
Servidor de banco de dados

Fig.4

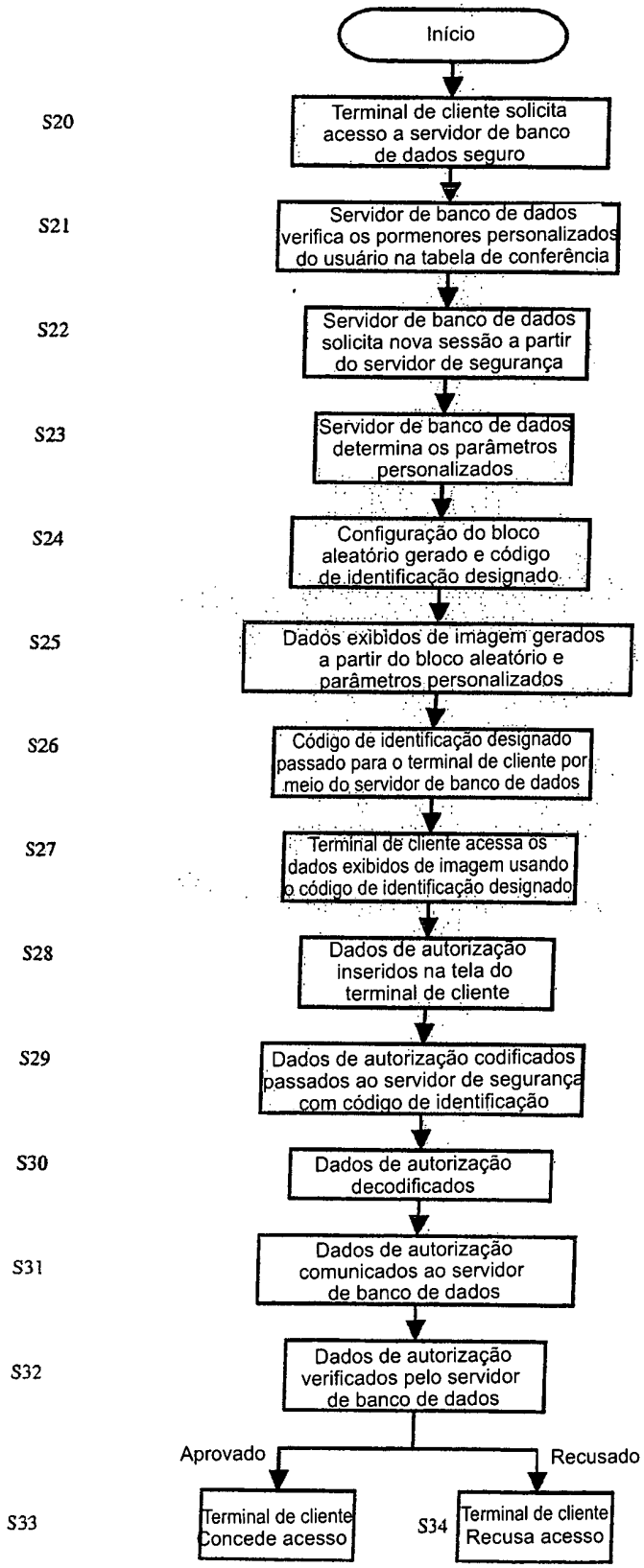

Início
S20
Terminal de cliente solicita acesso a servidor de banco de dados seguro
S21
Servidor de banco de dados verifica os pormenores personalizados do usuário na tabela de conferência
S22
Servidor de banco de dados solicita nova sessão a partir do servidor de segurança
S23
Servidor de banco de dados determina os parâmetros personalizados
S24
Configuração do bloco aleatório gerado e código de identificação designado
S25
Dados exibidos de imagem gerados a partir do bloco aleatório e parâmetros personalizados
S26
Código de identificação designado passado para o terminal de cliente por meio do servidor de banco de dados
S27
Terminal de cliente acessa os dados exibidos de imagem usando o código de identificação designado
S28
Dados de autorização inseridos na tela do terminal de cliente
S29
Dados de autorização codificados passados ao servidor de segurança com código de identificação
S30
Dados de autorização decodificados
S31
Dados de autorização comunicados ao servidor de banco de dados
S32
Dados de autorização verificados pelo servidor de banco de dados
Aprovado
Recusado
S33
Terminal de cliente Concede acesso
S34
Terminal de cliente Recusa acesso

Fig.5

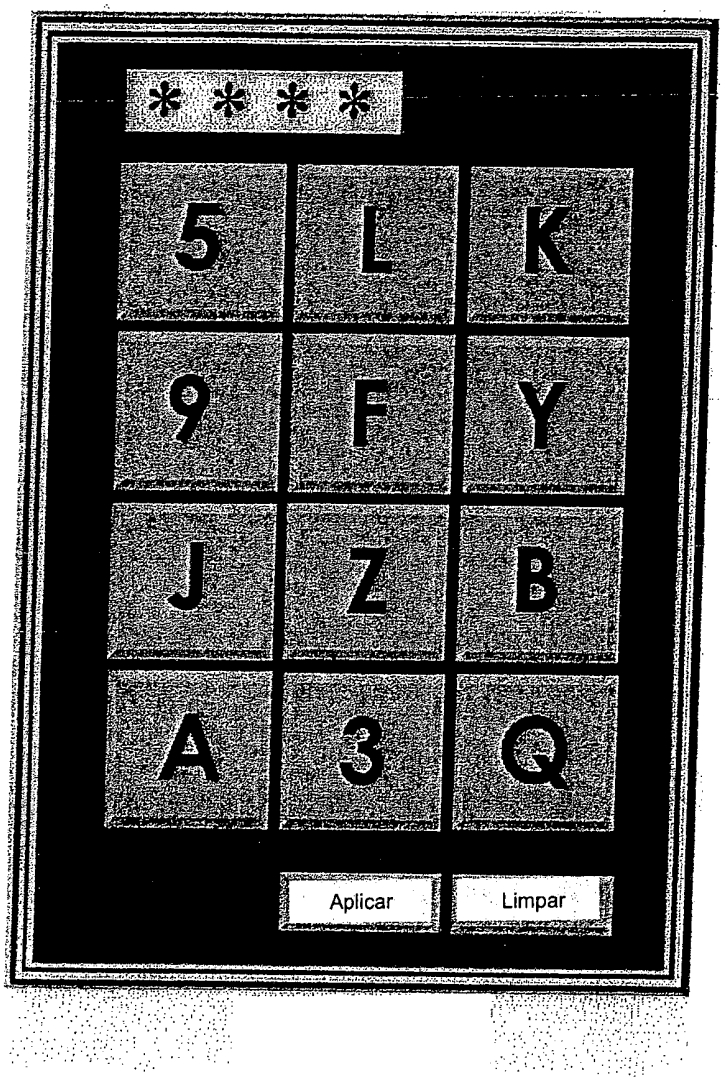


Fig.6

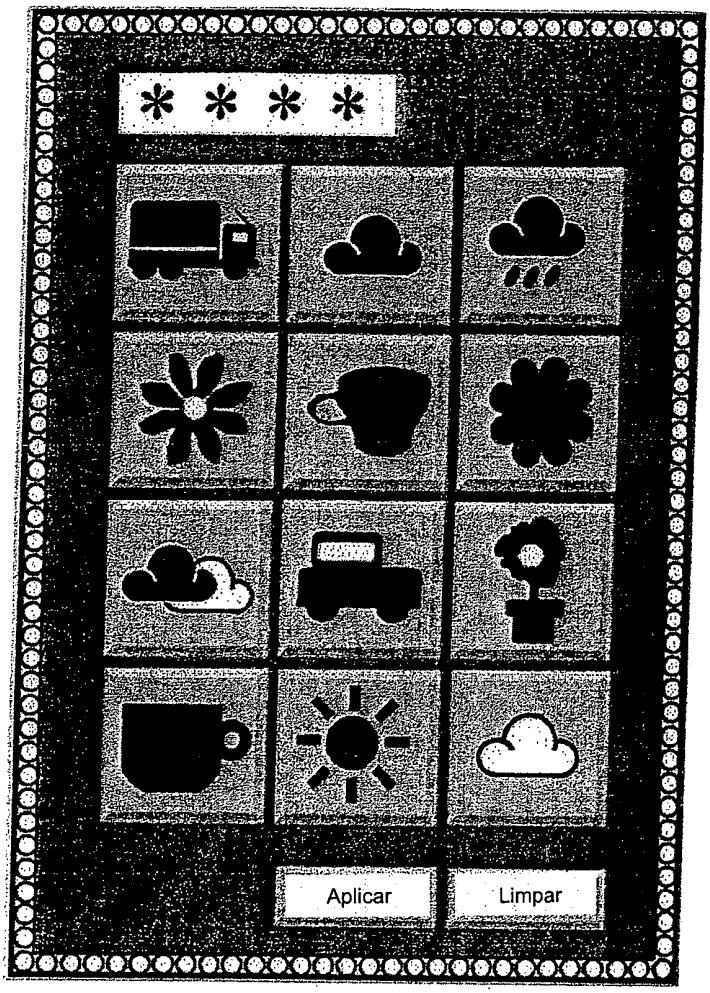


Fig.7

PI0608576-8

RESUMO

Patente de Invenção: **"PROCESSO PARA COMUNICAÇÃO DE DADOS SEGURA".**

A presente invenção refere-se a uma troca de dados entre um cliente terminal (1) e um servidor de banco de dados seguro (2) os dados são codificados usando uma informação posicional gerada por um gerador de combinação (7) em um servidor de segurança separado (3). A informação posicional é usada para produzir uma imagem específica para uma ocorrência de comunicação que é acessada por um cliente terminal (1) e é a base para a entrada de dados sensíveis no terminal do cliente (1). A conexão de comunicação de três vias entre o cliente terminal, o servidor de banco de dados e o servidor de segurança aumenta imensamente a dificuldade de interceptação bem-sucedida e a decodificação dos dados que foram inseridos no terminal do cliente. Este processo de comunicação de dados seguro é particularmente adequado para a comunicação de dados de senhas, por exemplo, em uma instituição bancária.