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

(11) PI 0819314-2 B1

(22) Data do Depósito: 14/11/2008

(45) Data de Concessão: 01/12/2020

(54) Título: REALIZAÇÃO DE TRANSAÇÕES ELETRÔNICAS SEGURAS

(51) Int.Cl.: G07F 7/10; H04L 29/06; G06F 21/00; G06Q 20/00.

(30) Prioridade Unionista: 19/11/2007 EP 07022419.1.

(73) Titular(es): INTERNATIONAL BUSINESS MACHINES CORPORATION..

(72) Inventor(es): MICHAEL BAENTSCH; PETER BUHLER; THOMAS EIRICH; RETO JOSEF HERMANN; THOMAS D. WEIGOLD; TAMAS VISEGRADY; THORSTEN KRAMP.

(86) Pedido PCT: PCT IB2008054782 de 14/11/2008

(87) Publicação PCT: WO 2009/066217 de 28/05/2009

(85) Data do Início da Fase Nacional: 19/05/2010

(57) Resumo: REALIZAÇÃO DE TRANSAÇÕES ELETRÔNICAS SEGURAS. A invenção refere-se a um método para executar transações eletrônicas entre um computador servidor (HO) e um computador cliente (120), o método compreendendo as etapas de: - executar um primeiro protocolo de comunicação com a transmissão de dados criptografados e autenticação mútua entre o computador servidor (110) e um dispositivo de hardware (130) através de uma rede de comunicação (160); - executar uma descriptografia de respostas do servidor criptografadas recebidas do computador servidor (110) no dispositivo de hardware (130); - encaminhar as respostas do servidor descriptografadas do dispositivo de hardware (130) para o computador cliente (120), - exibir as respostas do servidor descriptografadas em um visor de computador cliente (121) do computador cliente (120); - receber pedidos de clientes para enviar a partir do computador cliente (120) para o computador servidor (110) pelo dispositivo de hardware (130); - analisar os pedidos de clientes por informações de transação predefinida pelo dispositivo de hardware (130); - criptografar e encaminhar solicitações de clientes que não contenham qualquer informação sobre transações predefinidas para o computador servidor (110) pelo dispositivo de hardware (130); - exibir informações sobre a transação predefinida mediante detecção de uma solicitação do cliente em um visor de dispositivo de hardware (210) do dispositivo de hardware (130); - encaminhar e criptografar a solicitação do cliente com as informações de transações predefinidas para o (...).

REALIZAÇÃO DE TRANSAÇÕES ELETRÔNICAS SEGURAS

CAMPO TÉCNICO

[0001] A presente invenção está relacionada com um método para realizar transações eletrônicas seguras. A invenção está ainda relacionada com um sistema correspondente, um computador servidor correspondente, um dispositivo de hardware correspondente, um computador cliente correspondente e um programa de computador correspondente.

ANTECEDENTES DA INVENÇÃO

[0002] Os processos atuais de autenticação da Internet frequentemente utilizam a Infraestrutura de Chave Pública (PKI). Especialmente na presença de software malicioso em um computador pessoal (PC) de um usuário, pode ser incerto se o usuário está conectado ao computador servidor desejado com o qual ele deseja transacionar, por exemplo, um servidor bancário desejado. Um método conhecido para impedir ataques adversários solicita ao usuário verificar os certificados de servidor que foram emitidos por uma entidade confiável para o operador do servidor. Como isso é complicado, muitos usuários se abstêm de executar essa verificação de certificado do servidor. Outra abordagem conhecida usa a tecnologia PKI em combinação com cartões inteligentes. No entanto, o usuário não tem controle total sobre o que o cartão inteligente realmente faz, por exemplo, o que ele sinaliza ou onde ele se conecta. Isso é causado pelo fato de que as conexões com a Internet podem ser comprometidas por ataques *man-in-the-middle*, *worms* ou vírus em execução no PC do usuário. Além disso, software de registro de teclado e software de alteração do visor podem ser usados para enganar o usuário em trabalhar com um site

falso, por exemplo, para transmitir algum dinheiro para uma conta bancária de um adversário.

[0003] As abordagens descritas acima dependem em algum momento do processo de uma etapa em que o servidor apresenta alguma informação confidencial/ secreta no PC e/ ou uma etapa em que o usuário introduz algumas informações confidenciais/ secretas no PC. Isto é verdade mesmo para leitores de cartões inteligentes seguros com uma visor e teclado. As informações que um leitor de cartão inteligente seguro exibe ainda são controladas por software executado no PC.

[0004] O documento US 6895502 B1 descreve um método para exibir com segurança e confirmar de forma segura que uma solicitação de acesso a um recurso num computador servidor foi realmente solicitada pelo usuário cliente. Em resposta à solicitação, o computador servidor envia um desafio criptografado para um ambiente seguro que permite ao usuário do cliente verificar e confirmar que ele fez a solicitação correspondente.

[0005] O documento US 5 596 718 revela uma interface de usuário segura criada pela inserção de um subsistema de percurso confiável entre dispositivos de entrada/ saída de uma estação de trabalho e a própria estação de trabalho. O subsistema de percurso confiável é invocado manualmente pelo usuário e utiliza a exibição da estação de trabalho para exibir uma janela confiável.

[0006] É um objetivo da invenção fornecer outras soluções para realizar transações eletrônicas de uma forma segura.

[0007] É um objetivo adicional da invenção proporcionar soluções para a realização de transações

eletrônicas que podem ser implementadas de uma forma rentável.

[0008] É um objetivo adicional da invenção proporcionar soluções para a realização de transações eletrônicas com uma facilidade de uso melhorada.

[0009] É um objetivo adicional da invenção proporcionar soluções para executar transações eletrônicas de uma forma segura que possa utilizar infraestruturas de servidor existentes sem adaptação significativa dos servidores.

[0010] É um outro objetivo da invenção proporcionar soluções para executar transações eletrônicas de uma forma segura que possa utilizar protocolos de autenticação de fluxo existentes tais como SSL/ TLS.

SUMÁRIO E VANTAGENS DA INVENÇÃO

[0011] A presente invenção é dirigida a métodos, um sistema, um computador servidor, um computador cliente, um dispositivo de hardware e programas de computador como definido nas reivindicações independentes. Outras concretizações da invenção são proporcionadas nas reivindicações dependentes anexas.

[0012] De acordo com um primeiro aspecto da invenção é proporcionado um método para executar transações eletrônicas entre um computador servidor e um computador cliente, o método compreendendo as etapas de:

- executar um primeiro protocolo de comunicação com transmissão de dados criptografados e autenticação mútua entre o computador servidor e um dispositivo de hardware através de uma rede de comunicação,

– executar uma descriptografia de respostas de servidor criptografadas recebidas do computador servidor no dispositivo de hardware,

– encaminhar as respostas de servidor descriptografadas do dispositivo de hardware para o computador cliente,

– exibir as respostas do servidor descriptografadas numa visor de computador cliente do computador cliente,

– receber solicitações do cliente a serem enviadas do computador cliente para o computador servidor pelo dispositivo de hardware,

– analisar as solicitações do cliente para informações de transação predefinidas pelo dispositivo de hardware,

– criptografar e encaminhar solicitações de cliente que não contêm qualquer informação de transação predefinida para o computador servidor pelo dispositivo de hardware,

– exibir as informações de transação predefinidas após a detecção em uma solicitação de cliente em um visor de dispositivo de hardware do dispositivo de hardware,

– encaminhar e criptografar a solicitação de cliente contendo as informações de transação predefinidas para o computador servidor se uma confirmação de usuário for recebida,

– cancelar a transação eletrônica se nenhuma confirmação de usuário for recebida.

[0013] O método de acordo com este aspecto da invenção oferece uma maior segurança das transações eletrônicas. Uma transação eletrônica pode ser, por exemplo, um pagamento eletrônico, uma transferência eletrônica de dinheiro, uma ordem eletrônica ou qualquer outra transferência de informações confidenciais, privadas ou sensíveis quanto à segurança, como informações de logon.

[0014] Além disso, o método de acordo com este aspecto da invenção tem a vantagem de poder ser implementado de uma maneira flexível, eficiente e econômica. Uma vantagem adicional do método é que pode ser adicionado de forma eficiente e econômica a sistemas existentes.

[0015] O dispositivo de hardware funciona como uma interface entre o computador servidor e o computador cliente. Em outras palavras, durante a transação eletrônica somente o dispositivo de hardware se comunica logicamente diretamente com o computador servidor. Isso permite observar, avaliar, analisar e controlar a comunicação entre o computador cliente e o computador servidor. Mensagens ou dados que o computador cliente deseja enviar para o computador servidor são denotados como solicitações do cliente, enquanto mensagens ou dados que o computador servidor envia para o computador cliente são denotados como respostas do servidor. O dispositivo de hardware pode descriptografar as respostas do servidor e pode encaminhá-las para o computador cliente. O computador cliente compreende uma visor de computador cliente que pode apresentar a resposta de servidor descriptografado para um usuário. O usuário pode então interagir com o computador cliente por meio de uma unidade de entrada de computador cliente, por exemplo, por meio de um teclado e/ ou um mouse, e iniciar uma solicitação de cliente. O computador cliente envia a solicitação do cliente para o dispositivo de hardware e o dispositivo de hardware analisa a solicitação do cliente para informações de transação predefinidas. Em outras palavras, o dispositivo de hardware analisa as solicitações do cliente e verifica se ele contém qualquer informação de transação predefinida. Tais informações de transação

predefinidas são, em particular, informações sensíveis a segurança, privadas e/ ou confidenciais, tais como números de cartões de crédito, números de transações (TAN), números de contas bancárias, dados de pagamento, quantidades de pagamento, etc. A predefinição pode ser feita de aplicativo específico e/ ou do cliente específico. Como exemplo, um banco que oferece serviços bancários on-line pode predefinir quais informações a serem transferidas pelo cliente para o banco devem ser consideradas como informações de transação predefinidas. Além disso, o banco pode oferecer serviços bancários online com diferentes níveis de segurança. Para cada nível de segurança, as informações de transação predefinidas podem ser adaptadas.

[0016] O termo computador cliente é entendido num sentido lato. Um computador cliente pode ser, por exemplo, um computador portátil, um PC de secretária, um telefone móvel, um assistente pessoal digital (PDA) ou qualquer outro dispositivo eletrônico através do qual um usuário possa efetuar transações eletrônicas. O termo computador servidor é entendido em um sentido amplo também. Pode ser qualquer dispositivo eletrônico com o qual um computador cliente deseja realizar uma transação eletrônica.

[0017] Se a solicitação do cliente não contiver nenhuma informação de transação predefinida, o dispositivo de hardware pode criptografar e encaminhar a solicitação do cliente para o computador servidor por meio do primeiro protocolo de comunicação. Se a solicitação de cliente contiver informações de transação predefinidas, o dispositivo de hardware pode apresentar as informações de transação predefinidas ao usuário no visor do dispositivo de hardware. Isso permite ao usuário verificar se as informações

de transação predefinidas estão corretas. Além disso, o usuário pode comparar as informações de transação exibidas no visor do computador cliente com as informações de transação exibidas no visor do dispositivo de hardware. Isso facilita a detecção de diferenças que podem ser introduzidas por ataques *man-in-the-middle*. Se o usuário detectar uma diferença entre as informações de transação exibidas no visor do cliente e as informações de transação exibidas no visor do dispositivo de hardware, isso indica que o software malicioso está sendo executado no computador cliente e alterou as informações de transação inseridas pelo usuário via a unidade de entrada do computador cliente.

[0018] O visor do dispositivo de hardware pode ser realizado de várias maneiras. O visor do dispositivo de hardware pode ser incorporado em vários dispositivos ou ferramentas operáveis para apresentar as informações de transação a um usuário. Exemplos para um visor de dispositivo de hardware são Displays de Cristal Líquido (LCD), Displays de diodo emissor de luz (LED), Displays de plasma ou projetores, por exemplo, projetores de LCD ou laser.

[0019] Se as informações de transação predefinidas não estiverem corretas, o usuário pode cancelar ou não confirmar a transação. Em seguida, o dispositivo de hardware cancela a transação. Se o usuário tiver verificado que as informações de transação predefinidas apresentadas no visor do dispositivo de hardware estão corretas, ele pode confirmar a transação. Após a confirmação, o dispositivo de hardware criptografa as informações de transação predefinidas e envia para o computador servidor por meio do primeiro protocolo de comunicação. Existem várias maneiras de implementar a confirmação do usuário ou o cancelamento do usuário. De

acordo com uma concretização da invenção, a confirmação ou o cancelamento podem ser recebidos por meio de uma unidade de entrada de dispositivo de hardware do dispositivo de hardware. Em outras palavras, o usuário pode pressionar um botão de cancelamento ou um botão de confirmação do dispositivo de hardware. Alternativamente, pode ser especificado que o dispositivo de hardware o interpreta como uma confirmação se o usuário não cancelar a transação dentro de um período de tempo predefinido, por exemplo, dentro de 1 minuto. De acordo com outra concretização da invenção, o cancelamento poderia ser realizado puxando o dispositivo de hardware para fora da interface do computador cliente.

[0020] O primeiro protocolo de comunicação é estabelecido e executado como comunicação de ponta a ponta entre o dispositivo de hardware e o computador servidor. O primeiro protocolo de comunicação utiliza a autenticação mútua, ou seja, o computador servidor autentica-se ao dispositivo de hardware e o dispositivo de hardware autentica-se ao computador servidor. A transmissão de dados entre o dispositivo de hardware e o computador servidor é realizada de forma criptografada de modo a proporcionar um elevado grau de confidencialidade.

[0021] De acordo com uma concretização do primeiro aspecto da invenção, o método ainda compreende as etapas de:

- executar num modo de funcionamento normal um segundo protocolo de comunicação entre uma aplicação de navegador do computador cliente e do computador servidor,

- executar num modo de funcionamento seguro o primeiro protocolo de comunicação entre o computador servidor e o dispositivo de hardware,

– rotear no modo seguro de solicitações de cliente de operação da aplicação de navegador através de um aplicativo de proxy para o dispositivo de hardware e do dispositivo de hardware através da aplicação proxy para o computador servidor,

– encaminhar no modo seguro de respostas do servidor de operação do computador servidor através da aplicação proxy para o dispositivo de hardware e do dispositivo de hardware através da aplicação proxy para a aplicação de navegador.

[0022] A aplicação proxy pode ser implementada como um programa de computador em execução no computador cliente e permite uma implementação eficiente do método. Ele executa a função de um switch que é funcionalmente organizado entre o dispositivo de hardware, a aplicação de navegador e o computador servidor.

[0023] No modo de funcionamento normal, o usuário preferencialmente não troca informação de segurança sensível com o computador servidor. No modo de funcionamento normal, o dispositivo de hardware pode ser desligado ou desligado.

[0024] Se durante a sua sessão de navegação o usuário deseja efetuar uma transação eletrônica que pode envolver a troca de informações de segurança sensíveis, o modo de funcionamento seguro é invocado. De acordo com esta concretização da invenção, no modo seguro o primeiro protocolo de comunicação é executado entre o computador servidor e o dispositivo de hardware através da aplicação proxy e da rede de comunicação. Além disso, a comunicação entre a aplicação de navegador e o dispositivo de hardware é realizada através da aplicação proxy.

[0025] De acordo com uma concretização do primeiro aspecto da invenção, o método compreende ainda as etapas de:

– executar no modo normal de funcionamento o segundo protocolo de comunicação entre a aplicação de navegador do computador cliente e o computador servidor através da aplicação proxy do computador cliente,

– análise de solicitações de clientes para um conjunto predefinido de solicitações de cliente pela aplicação proxy,

– iniciar o modo de funcionamento seguro pela aplicação proxy após a detecção de uma solicitação de cliente predefinida.

[0026] Este é um método eficiente para invocar o modo de funcionamento seguro de forma automatizada. A aplicação proxy pode iniciar automaticamente o modo de funcionamento seguro sem qualquer interação do usuário. Como exemplo, o conjunto predefinido de solicitações de cliente pode compreender um conjunto predefinido de Uniform Resource Identifiers (URI) ou Uniform Resource Locators (URL) que identificam recursos do computador servidor. Esses recursos podem ser, por exemplo, um ou mais URLs de bancos onde o usuário tem uma conta e/ ou uma ou mais entidades de comércio eletrônico com quem o usuário deseja realizar comércio eletrônico ou qualquer entidade com a qual o usuário deseja realizar transações eletrônicas. Se o usuário digitar um desses URLs ou URIs predefinidos em seu aplicativo de navegador, a aplicação proxy o detectará e iniciará o modo de funcionamento seguro. O modo de funcionamento seguro pode ser, por exemplo, iniciado por meio do envio de um sinal "iniciar modo seguro" para o dispositivo de hardware.

[0027] No modo de funcionamento normal, a aplicação proxy encaminha ou roteia solicitações de cliente respectivamente e diretamente da aplicação de navegador para o computador servidor através da rede de comunicação. Na

outra direção, as respostas do servidor são enviadas através da rede de comunicação para a aplicação proxy e encaminhadas diretamente da aplicação proxy para a aplicação de navegador.

[0028] De acordo com outra concretização da invenção, o modo seguro poderia ser invocado manualmente pelo usuário, por exemplo, ligando o dispositivo de hardware seguro ao computador cliente.

[0029] De acordo com uma concretização do primeiro aspecto da invenção, o método compreende ainda, antes de encaminhar as respostas do servidor descriptografadas do dispositivo de hardware para o computador cliente, as etapas de:

– analisar as respostas do servidor para informações de transação predefinidas pelo dispositivo de hardware,

– reencaminhar respostas do servidor que não contêm nenhuma informação de transação predefinida para o computador cliente pelo dispositivo de hardware,

– exibir as informações de transação predefinidas pela detecção numa resposta de servidor no visor do dispositivo de hardware do dispositivo de hardware,

– encaminhar a resposta do servidor contendo as informações de transação predefinidas para o computador cliente se uma confirmação de usuário for recebida,

– cancelar a transação eletrônica se não for recebida confirmação de usuário.

[0030] Analisar as respostas do servidor, além de analisar as solicitações do cliente, fornece funcionalidade e aplicações aprimorados. As informações de transação predefinidas das respostas do servidor podem ser exibidas no visor do dispositivo de hardware para a atenção do usuário. As informações de transação predefinidas das respostas do

servidor podem, por exemplo, compreender mensagens de aviso do computador servidor que podem ser apresentadas no visor do dispositivo de hardware. Além disso, as informações de transação predefinidas das respostas do servidor podem ser desafios de servidor para o usuário ou quaisquer outras informações de segurança sensíveis do computador de servidor para o usuário. Isto tem a vantagem de que o usuário pode verificar essas informações de transação predefinidas do servidor mesmo se o software malicioso em execução no computador cliente impede que as informações de transação predefinidas sejam apresentadas na apresentação do computador cliente ou se o software malicioso manipular a vista no visor de computador cliente.

[0031] De acordo com uma outra concretização do primeiro aspecto da invenção, o primeiro protocolo de comunicação compreende uma camada de rede compreendendo um protocolo de acordo com o padrão *Secure Sockets Layer* (SSL) ou de acordo com a *Transport Layer Security* (TLS) e um protocolo de acordo com o padrão Protocolo de Controle de Transmissão/ Protocolo da Internet (TCP/ IP).

[0032] Estes protocolos são amplamente aplicáveis e generalizados. O método de acordo com este aspecto da invenção pode utilizar estes protocolos sem qualquer necessidade de adaptação. Isto permite implementar o método de acordo com este aspecto da invenção de uma maneira rentável. A camada SSL ou TLS é executada acima da camada TCP/ IP e fornece a funcionalidade de autenticação de servidor, autenticação de cliente, bem como transmissão de dados criptografados.

[0033] De acordo com uma outra concretização do primeiro aspecto da invenção, o primeiro protocolo de

comunicação compreende uma camada de aplicação que compreende o Protocolo de Transferência de Hipertexto (*Hyper Text Transfer Protocol* – HTTP).

[0034] Este protocolo é amplamente aplicável e generalizado. Em combinação com um protocolo SSL ou TLS na camada de rede, é possível estabelecer, de preferência, o Protocolo de Transferência de Hipertexto Seguro *(HyperText Transfer Protocol Secure* – HTTPS).

[0035] De acordo com uma outra concretização deste aspecto da invenção, a segunda comunicação compreende uma camada de rede compreendendo o Protocolo de Controle de Transmissão/ Protocolo de Internet (TCP/ IP) e uma camada de aplicação compreendendo o Protocolo de Transferência de Hipertexto (HTTP).

[0036] Estes protocolos são amplamente aplicáveis e generalizados. No modo de funcionamento normal um usuário do computador cliente poderia navegar na internet por meio da aplicação de navegador usando TCP/ IP e HTTP.

[0037] De acordo com uma outra concretização deste aspecto da invenção, o método compreende a etapa de executar uma autenticação de usuário pelo computador servidor.

[0038] Essa autenticação adicional aprimora a segurança do método. Tal autenticação de usuário pode ser realizada, por exemplo, por meio de uma senha ou de um número de identificação pessoal (PIN) do usuário. Como exemplo, o servidor pode enviar uma resposta do servidor para o computador cliente no qual o usuário é solicitado a inserir sua senha ou PIN. A senha ou o PIN é armazenado no computador servidor e, portanto, pode ser verificado pelo computador servidor. Uma autenticação de usuário é entendida como uma autenticação que não pode ser executada automaticamente pelo

próprio dispositivo de hardware, mas precisa de entrada adicional do usuário do sistema. Isso impede que um adversário possa usar um dispositivo de hardware roubado sem conhecer a senha ou o PIN adicionais. Pelo contrário, a autenticação mútua entre o dispositivo de hardware e o computador servidor que é executada durante o primeiro protocolo de comunicação pode ser executada automaticamente sem interação adicional do usuário. De preferência, a autenticação do usuário deve ser realizada antes de qualquer informação de transação predefinida ser enviada do dispositivo de hardware seguro para o computador servidor.

[0039] De acordo com uma outra concretização deste aspecto da invenção, o método compreende a etapa de executar uma autenticação de usuário pelo dispositivo de hardware.

[0040] Essa autenticação adicional aprimora a segurança do método. Tal autenticação de usuário pode ser, por exemplo, executada por meio de uma senha ou um número de identificação pessoal (PIN). Por exemplo, o dispositivo de hardware pode exibir uma mensagem na qual o usuário é solicitado a digitar sua senha ou PIN por meio da unidade de entrada de dispositivo de hardware. A senha ou PIN é armazenado no dispositivo de hardware ou em um cartão inteligente legível pelo dispositivo de hardware e, portanto, pode ser verificado pelo dispositivo de hardware. Isso impede que um adversário possa usar um dispositivo de hardware roubado sem conhecer a senha ou o PIN adicionais. Outros métodos de autenticação de usuários como autenticação biométrica, por exemplo, leitura de impressões digitais, podem ser usados também. Nesta concretização a autenticação do usuário deve ser preferencialmente realizada antes de iniciar ou estabelecer, respectivamente, o primeiro

protocolo de comunicação. De acordo com um segundo aspecto da invenção é proporcionado um sistema para executar transações eletrônicas, compreendendo:

– um computador servidor,

– um computador cliente que compreende uma visor de computador cliente e uma unidade de entrada de computador cliente,

– um dispositivo de hardware que compreende um visor de dispositivo de hardware,

– uma rede de comunicações entre o dispositivo de hardware e o computador servidor, sendo o sistema adaptado para:

– executar um primeiro protocolo de comunicação com transmissão de dados criptografados e autenticação mútua entre o computador servidor e o dispositivo de hardware,

– executar uma descriptografia de respostas de servidor criptografadas recebidas do computador servidor no dispositivo de hardware,

– encaminhar as respostas do servidor descriptografadas do dispositivo de hardware para o computador cliente,

– apresentar as respostas do servidor descriptografadas no visor do computador cliente,

– receber solicitações do cliente para serem enviadas do computador cliente para o computador servidor pelo dispositivo de hardware,

– analisar as solicitações do cliente pelo dispositivo de hardware para informações de transação predefinidas,

– criptografar e encaminhar solicitações de clientes que não contenham nenhuma informação de transação predefinida para o computador servidor,

– exibir as informações de transação predefinidas após a detecção em uma solicitação de cliente no visor do dispositivo de hardware,

– encaminhar e criptografar a solicitação de cliente contendo as informações de transação predefinidas para o computador servidor se uma confirmação de usuário for recebida,

– cancelar a transação eletrônica se nenhuma confirmação do usuário for recebida.

[0041] O segundo aspecto da invenção aborda aspectos do sistema de um sistema no qual o método do primeiro aspecto da invenção pode ser realizado.

[0042] De acordo com um terceiro aspecto da invenção é proporcionado um método para controlar transações eletrônicas entre um computador servidor e um computador cliente por meio de um dispositivo de hardware, o método no dispositivo de hardware compreendendo as etapas de:

– executar um primeiro protocolo de comunicação com transmissão de dados criptografados e autenticação mútua com o computador servidor,

– executar uma descriptografia de respostas de servidor criptografadas recebidas do computador servidor,

– encaminhar as respostas de servidor descriptografadas para o computador cliente,

– receber pedidos do cliente para serem enviados para o computador servidor a partir do computador cliente,

– analisar as solicitações do cliente para informações de transação predefinidas,

– criptografar e encaminhar solicitações de clientes que não contêm quaisquer informações de transação predefinidas para o computador servidor,

– apresentar as informações de transação predefinidas a um usuário após a detecção em uma solicitação de cliente,

– encaminhar e criptografar a solicitação de cliente contendo as informações de transação predefinidas para o computador servidor se uma confirmação de usuário for recebida.

[0043] O terceiro aspecto da invenção refere-se a etapas de método sendo realizadas no dispositivo de hardware. De acordo com uma concretização deste aspecto da invenção, as informações de transação predefinidas são apresentadas numa apresentação do dispositivo de hardware. De acordo com uma concretização deste aspecto da invenção, o método compreende ainda a etapa de cancelar a transação eletrônica se nenhuma confirmação de usuário for recebida.

[0044] De acordo com um quarto aspecto da invenção é proporcionado um dispositivo de hardware para controlar transações eletrônicas, compreendendo:

– uma exibição de dispositivo de hardware e uma unidade de interface de dispositivo de hardware, em que a unidade de interface de dispositivo de hardware é fornecida para acoplar o dispositivo de hardware a um computador cliente, em que o dispositivo de hardware está adaptado para:

– executar um primeiro protocolo de comunicação com transmissão de dados criptografada e autenticação mútua com um computador servidor,

– executar uma descriptografia de respostas de servidor criptografadas recebidas do computador servidor,

– encaminhar as respostas do servidor descriptografado para o computador cliente,

– receber solicitações do cliente para serem enviadas do computador cliente para o computador servidor,

– analisar as solicitações do cliente para informações de transação predefinidas,

– criptografar e encaminhar solicitações de clientes que não contenham nenhuma informação de transação predefinida para o computador servidor,

– apresentar as informações de transação predefinidas após a detecção numa solicitação de cliente no visor do dispositivo de hardware,

– encaminhar e criptografar solicitações de cliente contendo as informações de transação predefinidas para o computador servidor se uma confirmação de usuário for recebida.

[0045] Tal dispositivo de hardware pode ser implementado e utilizado de forma flexível e eficiente para melhorar a segurança das transações eletrônicas. Em particular, pode não haver necessidade de implementar alterações no lado dos computadores servidor se o primeiro protocolo de comunicação é conhecido para o servidor, por exemplo, SSL. O dispositivo de hardware pode trabalhar em conjunto com computadores clientes comuns, como PCs ou laptops. O acoplamento entre o computador cliente e o dispositivo de hardware pode ser implementado ligando a unidade de interface de dispositivo de hardware a uma primeira interface do computador cliente. A unidade de interface do dispositivo de hardware pode ser uma unidade de interface sem fio ou uma unidade de interface cabeada. Por exemplo, a unidade de interface do dispositivo de hardware pode ser uma interface USB (Universal Serial Bus).

[0046] De acordo com uma concretização da invenção, o dispositivo de hardware está adaptado para cancelar a

transação eletrônica se não for recebida nenhuma confirmação do usuário.

[0047] De acordo com uma concretização do quarto aspecto da invenção, o dispositivo de hardware compreende um token de segurança para armazenar dados de segurança sensíveis.

[0048] Um tal token de segurança é uma unidade de hardware, também denotada como token de hardware, que pode armazenar dados sensíveis à segurança, em particular dados de usuário sensíveis à segurança, de uma forma inviolável. Em outras palavras, os dados sensíveis à segurança armazenados no token de segurança não podem ser lidos ou manipulados. O grau ou nível de resistência à violação pode ser adaptado aos requisitos de segurança da respectiva aplicação. O token de segurança pode ser, por exemplo, um componente de hardware compreendendo um chip de cartão inteligente que armazena os dados sensíveis de segurança.

[0049] De acordo com uma concretização do quarto aspecto da invenção, o dispositivo de hardware compreende um leitor de cartões inteligentes para ler dados sensíveis de segurança a partir de um cartão inteligente. De acordo com esta concretização, o chip inteligente do cartão inteligente armazena os dados sensíveis à segurança. O cartão inteligente pode ser mantido pelo usuário em um lugar diferente do dispositivo de hardware. Antes de executar o dispositivo de hardware, o usuário tem de colocar o cartão inteligente no leitor de cartões inteligentes do dispositivo de hardware.

[0050] De acordo com uma concretização do quarto aspecto da invenção, o dispositivo de hardware tem um ou mais níveis predefinidos de resistência à violação.

[0051] Os níveis predefinidos de resistência à violação podem ser adaptados aos requisitos de segurança da respectiva aplicação. Quanto mais altos forem os requisitos de segurança da aplicação, maior será o nível de resistência à violação. De preferência, o nível de resistência à violação é inviolável.

[0052] Os níveis predefinidos de resistência à violação podem abordar diferentes ataques, por exemplo, um nível de resistência contra adulteração contra software malicioso ou um nível de resistência contra adulteração contra a manipulação física do hardware ou um nível de resistência contra a inspeção do dispositivo de hardware, O armazenamento ou a memória, por meio de um microscópio. O software malicioso, também denotado como malware, pode ser entendido como qualquer software que tem a intenção de prejudicar, alterar ou manipular a função correta do dispositivo de hardware. Tal software malicioso pode ser, por exemplo, um vírus, um worm, um cavalo de tróia, spyware ou outro software indesejado. Em outras palavras, software malicioso é um software que é projetado para se infiltrar, danificar ou prejudicar um sistema de computador.

[0053] De acordo com uma concretização do quarto aspecto da invenção, o nível predefinido de resistência à violação do dispositivo de hardware é superior ao nível de resistência à violação do computador cliente.

[0054] Isso significa que é mais difícil para um adversário manipular ou adulterar o dispositivo de hardware do que manipular o computador cliente. Concentração na resistência à violação do dispositivo de hardware é mais eficiente em termos de custos do que melhorar a resistência à violação do computador cliente inteiro. Em particular, é

mais difícil para um adversário colocar software mal-intencionado no dispositivo de hardware do que no computador cliente.

[0055] De acordo com uma concretização do quarto aspecto da invenção, o dispositivo de hardware é concebido de tal modo que não podem ser carregadas aplicações de software no dispositivo de hardware.

[0056] Isso impede que vírus, worms ou outros softwares mal-intencionados possam manipular ou prejudicar o funcionamento do dispositivo de hardware. Esta concretização pode, por exemplo, ser implementada armazenando o programa ou programas do dispositivo de hardware numa memória fundida. Em outras palavras, depois de ter carregado o programa ou os programas na memória de programa do dispositivo de hardware, a memória de programa é fundida. Isso impede que quaisquer outros programas possam ser carregados e executados no dispositivo de hardware.

[0057] De acordo com uma concretização do quarto aspecto da invenção, os dados sensíveis à segurança compreendem uma chave privada e informação de raiz de confiança.

[0058] A chave privada será utilizada para executar o primeiro protocolo de comunicação com o computador servidor, em particular a autenticação mútua.

[0059] As informações de raiz de confiança definem quais autoridades o dispositivo de hardware confia. As informações de raiz de confiança podem incluir, por exemplo, uma ou mais chaves raiz de autoridade de certificação de autoridades de certificação em que o dispositivo de hardware confia. Isso permite usar a tecnologia PKI (*Public Key*

Infrastructure) para executar a autenticação mútua do primeiro protocolo de comunicação.

[0060] De acordo com uma concretização do quarto aspecto da invenção, o dispositivo de hardware compreende uma unidade de entrada de dispositivo de hardware para confirmar e/ ou cancelar uma transação.

[0061] A unidade de entrada do dispositivo de hardware pode ser estabelecida, por exemplo, através de um ou mais botões, por exemplo, através de um botão de confirmação e/ ou um botão de cancelamento. De acordo com um quinto aspecto da invenção é proporcionado um computador cliente que pode ser ligado através de uma primeira interface a uma rede de comunicação e através de uma segunda interface para um dispositivo de hardware, o computador cliente compreendendo:

- um aplicativo de navegador para navegar na rede de comunicação e um aplicativo proxy, sendo a aplicação proxy adaptado para

- encaminhar em um modo seguro de funcionamento solicitações de clientes da aplicação de navegador para o dispositivo de hardware e do dispositivo de hardware através da rede de comunicação a um computador servidor,

- encaminhar no modo seguro de funcionamento respostas do servidor recebidas do computador servidor para o dispositivo de hardware e do dispositivo de hardware para a aplicação de navegador, em que o computador cliente está adaptado para executar no modo de funcionamento seguro das transações eletrônicas com o computador servidor através do dispositivo de hardware e através da rede de comunicação.

[0062] Tal computador cliente pode ser implementado de uma forma eficiente. A aplicação proxy permite a

atualização de computadores clientes comuns e torná-los interoperáveis com o dispositivo de hardware.

[0063] De acordo com uma concretização do quinto aspecto da invenção, a aplicação de proxy está adaptada para:

- encaminhar num modo de funcionamento normal solicitações de clientes recebidas da aplicação de navegador do computador cliente para o computador servidor da rede de comunicações,

- encaminhar no modo de funcionamento normal respostas do servidor recebidas do computador servidor para a aplicação de navegador do computador cliente,

- analisar as solicitações de clientes para um conjunto de solicitações de clientes predefinidas,

- iniciar o modo de funcionamento seguro após a detecção de uma solicitação de cliente predefinida.

[0064] Esta é uma forma eficiente de desencadear o modo seguro de uma maneira automatizada. O usuário não precisa começar ativamente o modo de segurança, mas pode ter certeza que sempre que ele envia um dentre a solicitação do cliente predefinido, o modo de segurança será iniciado automaticamente.

[0065] De acordo com uma concretização do quinto aspecto da invenção, o modo de segurança é iniciado através do envio de um sinal de ativação de modo seguro a partir da aplicação de proxy para o dispositivo de hardware.

[0066] O sinal de ativação de modo seguro indica ao dispositivo de hardware que deve iniciar o modo seguro.

[0067] De acordo com um sexto aspecto da invenção, é fornecido um programa de computador que compreende instruções para realizar as seguintes etapas, quando o

referido programa de computador é executado num computador cliente:

- encaminhar em um modo de funcionamento seguro solicitações de clientes de uma aplicação de navegador de computador cliente para um dispositivo de hardware e do dispositivo de hardware através de uma rede de comunicação para um computador servidor,

- encaminhar no modo de funcionamento seguro respostas do servidor recebidas a partir do computador servidor para o dispositivo de hardware e do dispositivo de hardware para a aplicação de navegador.

[0068] Tal programa de computador incorpora a aplicação proxy e estabelece uma interface eficiente e flexível entre um aplicativo navegador e o dispositivo de hardware. Tal programa de computador faz com que aplicativos de navegador interoperáveis com o dispositivo de hardware de uma forma eficiente.

[0069] De acordo com uma concretização do sexto aspecto da invenção, o programa de computador compreende ainda instruções para realizar os seguintes passos, quando o referido programa de computador é executado no computador cliente:

- encaminhar num modo de funcionamento normal solicitações de clientes recebidas a partir da aplicação de navegador de o computador cliente para o computador do servidor da rede de comunicação,

- encaminhar no modo de funcionamento normal respostas do servidor de operação recebidas do computador servidor para a aplicação de navegador do computador cliente,

- analisar solicitações de clientes para um conjunto predefinido de solicitações de clientes,

– iniciar o modo seguro após a detecção de uma solicitação do cliente predefinida. De acordo com um sétimo aspecto da invenção, é proporcionado um método para controlar as transações eletrônicas entre um computador servidor e um computador cliente por meio de um dispositivo de hardware, o método compreendendo, no dispositivo de hardware, os passos de:

– executar um primeiro protocolo de comunicação com a transmissão de dados criptografados e autenticação mútua com o computador servidor,

– realizar uma descriptografia das respostas do servidor criptografadas recebidas do computador servidor,

– analisar as respostas do servidor para informações de transação predefinidas,

– encaminhar as respostas do servidor que não contém nenhuma informação de transações predefinida para o computador cliente,

– apresentar a informação de transação predefinida para um usuário após a detecção de uma resposta do servidor,

– encaminhar a resposta do servidor que contém a informação de transação predefinida para o computador cliente se uma confirmação de usuário é recebida.

[0070] Este aspecto da invenção refere-se a um método segundo o qual as respostas do servidor são analisadas. As informações de transação predefinida das respostas do servidor podem por exemplo ser desafios de servidor para o usuário ou informações de segurança sensíveis do computador servidor para o usuário.

[0071] Como um exemplo, tal método pode ser usado para realizar um download de software com maior segurança. Antes do dispositivo de hardware encaminhar o software para

o computador cliente, o dispositivo de hardware pode exibir uma mensagem na qual o usuário é perguntado se ele concorda com a transferência. Além disso, o servidor pode enviar alguma informação de verificação de usuário em relação à integridade do software para o dispositivo de hardware. Em seguida, o dispositivo de hardware exibiria as informações de verificação do usuário no visor do dispositivo de hardware e o usuário pode verificar a integridade do software antes de baixá-lo. Isto é particularmente útil para evitar o download de software malicioso.

[0072] De acordo com um oitavo aspecto da invenção é proporcionado um dispositivo de hardware para o controle de transações eletrônicas, que compreende:

- um visorde dispositivo de hardware e uma unidade de interface de dispositivo de hardware, em que a unidade de interface de dispositivo de hardware é fornecida para acoplar o dispositivo de hardware de um computador cliente, em que o dispositivo de hardware é adaptado para:

- executar um primeiro protocolo de comunicação com transmissão de dados criptografados e autenticação mútua com um computador servidor,

- realizar uma descriptografia das respostas do servidor criptografadas recebidas do computador servidor,

- analisar as respostas do servidor para obter informações de transação predefinidas,

- encaminhar respostas do servidor que não contêm qualquer informação de transação predefinida para o computador cliente,

- mostrar as informações de transação predefinidas após a detecção de uma solicitação do cliente no visor do dispositivo de hardware,

- encaminhar as respostas do servidor contendo as informações de transação predefinidas para o computador cliente se uma confirmação de usuário é recebida.

[0073] O oitavo aspecto da invenção refere-se a um dispositivo de hardware, em que o método do sétimo aspecto da invenção pode ser realizado.

[0074] De acordo com um nono aspecto da invenção, é proporcionado um dispositivo de hardware para o controle de transações eletrônicas, que compreende um meio de apresentação para apresentar informação a um usuário e uma unidade de interface de dispositivo de hardware, em que a unidade de hardware de interface de dispositivo é fornecida para acoplar o dispositivo de hardware um computador cliente, em que o dispositivo de hardware é adaptado para:

- executar um primeiro protocolo de comunicação com transmissão de dados criptografados e autenticação mútua com um computador servidor,

- realizar uma descriptografia das respostas do servidor criptografadas recebidas do computador servidor,

- encaminhar as respostas do servidor descriptografadas para o computador cliente,

- receber solicitações de cliente a serem enviadas a partir do computador cliente para o computador servidor,

- analisar as solicitações de clientes para informações de transação predefinidas,

-criptografar e encaminhar solicitações do cliente que não contém nenhuma informação de transação predefinida para o computador servidor,

- apresentar as informações de transação predefinida após a detecção em uma solicitação do cliente pelo meio de apresentação,

– encaminhar e criptografar as solicitações de cliente que contêm as informações de transação predefinida para o computador servidor, se uma confirmação do usuário é recebida.

[0075] De acordo com este aspecto da invenção um meio de apresentação é fornecido para apresentar a informação de transação predefinida para o usuário. De acordo com uma concretização deste aspecto da invenção, o meio de apresentação pode ser um visor.

[0076] De acordo com um décimo aspecto da invenção é proporcionado um dispositivo de hardware para o controle de transações eletrônicas, compreendendo uma interface de usuário e uma unidade de interface de dispositivo de hardware, em que a unidade de interface de dispositivo de hardware é fornecida para acoplar o dispositivo de hardware de um computador cliente, em que o dispositivo de hardware é adaptado para:

– executar um primeiro protocolo de comunicação com transmissão de dados criptografados e autenticação mútua com um computador servidor,

– realizar uma descriptografia das respostas do servidor criptografadas recebidas do computador servidor,

– encaminhar as respostas do servidor descriptografadas para o computador cliente,

– receber solicitações de cliente a serem enviadas a partir do computador cliente para o computador servidor,

– analisar as solicitações de cliente para informações de transações predefinidas,

– criptografar e encaminhar as solicitações de cliente que não contêm qualquer informação de transação predefinida para o computador servidor,

– apresentar as informações de transação predefinidas pela interface do usuário após a detecção de uma solicitação do cliente,

– encaminhar e criptografar solicitações de clientes contendo as informações de transação predefinidas para o computador servidor, se uma confirmação do usuário é recebida.

[0077] De acordo com este aspecto da invenção uma interface de usuário geral é fornecida para apresentar a informação de transação predefinida para o usuário. Essa interface de usuário em geral pode apresentar as informações de transação para o usuário de várias maneiras. De acordo com uma concretização da invenção, a interface de usuário pode ser um visor. De acordo com uma outra concretização da invenção, a interface de usuário pode ser uma interface acústica, tal como um alto-falante.

[0078] As etapas dos diferentes aspectos da invenção podem ser realizadas em diferentes ordens. Além disso, as etapas também podem ser combinadas, isto é, por exemplo, duas ou mais etapas são realizadas em conjunto.

[0079] Qualquer um dos recursos do dispositivo pode ser aplicado ao aspecto do método da invenção e vice-versa. Vantagens dos recursos do dispositivo se aplicam a recursos de método e vice-versa correspondente.

DESCRIÇÃO DOS DESENHOS

[0080] As concretizações preferidas da invenção são descritas em detalhes abaixo, para fins de exemplo apenas, com referência aos seguintes desenhos esquemáticos.

[0081] Os desenhos são fornecidos apenas para fins ilustrativos e não representam necessariamente exemplos práticos da presente invenção em escala. Nas figuras, os

mesmos sinais de referência são usados para indicar as mesmas partes ou semelhantes.

[0082] A Figura 1 é um diagrama de blocos de um sistema de acordo com uma concretização da presente invenção;

[0083] A Figura 2 é um diagrama de blocos de um dispositivo de hardware de acordo com uma concretização da presente invenção;

[0084] A Figura 3 é um diagrama de blocos de um dispositivo de hardware de acordo com outra concretização da presente invenção;

[0085] A Figura 4 ilustra o fluxo de comunicação entre uma aplicação de navegador, uma aplicação proxy, o dispositivo de hardware e um computador servidor de acordo com uma concretização da presente invenção;

[0086] A Figura 5 mostra uma ilustração esquemática de um fluxo de mensagens de um método de acordo com uma concretização da invenção, num modo de funcionamento normal;

[0087] A Figura 6 até a Figura 8 mostra ilustrações esquemáticas de fluxos de mensagens de um método de acordo com uma concretização da invenção, em um modo de funcionamento seguro.

[0088] A Figura 1 mostra um sistema 100 de acordo com uma concretização da presente invenção. O sistema 100 compreende um computador do servidor 110, um computador cliente 120 e um dispositivo de hardware 130. O computador cliente 120 compreende um visor de computador do cliente 121 e uma unidade de entrada de computador cliente 122. A unidade de entrada de computador de cliente 122 compreende um teclado 123 e um mouse 124. O computador cliente 120 compreende além disso uma unidade de processamento 150, memória 151 (por exemplo, um dispositivo de memória volátil) e de

armazenamento 152 acoplada por meio de um sistema de barramento 153 e disposta numa carcaça do computador 154. O armazenamento 152 pode incluir um dispositivo de memória não-volátil (por exemplo, EEPROM, ROM, PROM, memória RAM, DRAM, SRAM, flash, firmware, lógica programável, etc.), unidade de disco magnético, unidade de disco óptico, unidade de fita, etc. O armazenamento 152 pode compreender um dispositivo de armazenamento interno, um dispositivo de armazenamento acoplado e/ ou um dispositivo de armazenamento acessível em rede. O computador cliente 120 pode incluir uma lógica de programa 157 incluindo código de programa 158, que pode ser carregado na memória 151 e executado pela unidade de processamento 150. Em certas concretizações, a lógica do programa 157, incluindo o código de programa 158 pode ser armazenado no armazenamento 152. Portanto, enquanto que a Figura 1 mostra a lógica do programa 157 em separado dos elementos restantes, a lógica de programa 157 pode ser implementada no armazenamento 152.

[0089] O computador cliente 120 é acoplado a uma rede de comunicação 160 através de uma primeira interface 156. A primeira interface 156 pode ser uma interface sem fio ou cabeada, em particular uma interface de Barramento Serial Universal (USB). A rede de comunicações 160 pode ser a Internet. O computador cliente 120 é acoplado ao dispositivo de hardware 130 através de uma segunda interface 155. A segunda interface 155 pode ser sem fio ou uma interface com fios, em especial, uma interface USB. O computador cliente 120 pode ser um computador pessoal (PC). O computador servidor 110 é acoplado à rede de comunicação 160 também. O computador servidor 110 pode ser, por exemplo, o computador do servidor de um banco, uma companhia de seguros ou de uma

entidade que oferece transações eletrônicas via rede de comunicação 160, em particular a Internet.

[0090] A Figura 2 mostra uma concretização de hardware do dispositivo 130 da Figura 1 em maiores detalhes. O dispositivo de hardware 130 compreende uma unidade de processamento 200, um dispositivo de hardware visor 210, a memória 220 (por exemplo, um dispositivo de memória volátil) e de armazenamento 230. A armazenagem 230 pode incluir um dispositivo de memória não volátil (por exemplo, EEPROM, ROM, PROM, RAM, DRAM, SRAM, flash, firmware, lógica programável, etc.). O dispositivo de hardware 130 pode incluir uma lógica de programa 240 inclui código de programa 241 que pode ser carregado na memória 220 e executado pela unidade de processamento 200. Em certas concretizações, a lógica do programa 240, incluindo o código de programa 241 pode ser armazenado no armazenamento 230. Portanto, enquanto que a Figura 2 mostra a lógica do programa 240 em separado dos restantes elementos, a lógica do programa 240 pode ser implementado no armazenamento 230. O dispositivo 130 compreende, além disso, o hardware de um leitor de cartão inteligente 250, uma unidade de interface do dispositivo de hardware 270, também denotada como unidade de E/S 270, e uma unidade de entrada de dispositivo de hardware 280. A unidade de interface de dispositivo de hardware 270 pode ser uma interface sem fio ou com fio, em particular uma –interface de Barramento Serial Universal (*Universal Serial Bus* – USB). A unidade de interface do dispositivo de hardware 270 pode ser usada para ligar ou acoplar o dispositivo de hardware 130 ao computador cliente 120. A unidade de entrada de dispositivo de hardware 280 é fornecida para a entrada de usuário e pode compreender um ou mais botões ou um teclado

completo. Como exemplo, a unidade de entrada de dispositivo de hardware 280 pode consistir de apenas dois botões, um cancelar botão para cancelar uma transação e um botão de confirmação para confirmar uma transação. O dispositivo de hardware 130 é coberto por uma carcaça 290, por exemplo, por um alojamento de plástico.

[0091] O leitor de cartão inteligente 250 pode ler a partir de cartões inteligentes 260 de dados de segurança sensíveis, em particular os dados do usuário de segurança sensíveis, como uma chave privada e informação de raiz de confiança.

[0092] A Figura 3 mostra uma outra concretização do dispositivo de hardware 130 da Figura 1 em maiores detalhes. O dispositivo de hardware 130 de acordo com a concretização da figura 3 compreende a unidade de processamento 200, o visor do dispositivo de hardware 210, a memória 220, o armazenamento 230, a lógica de programa 240, incluindo o código de programa 241, a unidade de interface de dispositivo de hardware 270, a unidade de entrada do dispositivo de hardware 280 e o alojamento 290, tal como descrito com referência à figura 2.

[0093] Além disso, dispõe de um token de segurança integrado 310 para armazenar dados de segurança sensíveis, tais como as chaves privadas e informações de raiz de confiança. O token de segurança 310 pode ser, por exemplo, um chip de cartão inteligente.

[0094] O dispositivo de hardware 130 é, de preferência inicializado em um ambiente confiável e seguro, por exemplo, em um site seguro de um banco. Tal inicialização compreende por exemplo, o carregamento de informações de segurança sensíveis no token de segurança 310 ou no cartão

inteligente 260. O dispositivo de hardware 130 pode ser, por exemplo implementado como um dispositivo USB.

[0095] A Figura 4 ilustra o fluxo de comunicação entre uma aplicação de navegador 410 executada no computador cliente 120, uma aplicação proxy 420 em execução no computador cliente 120, o dispositivo de hardware 130, a rede de comunicação 160 e o computador servidor 110.

[0096] De acordo com uma concretização da invenção a aplicação de navegador 410 e a aplicação proxy 420 estão implementadas como código de programa 158 da lógica de programa 157 do computador cliente 120, tal como descrito com referência à Figura 1. A aplicação de navegador 420 pode ser, em particular, um navegador web que permite que um usuário exiba e interaja com texto, imagens, vídeos, música e outras informações que podem estar localizados em uma página web ou site da Internet. Em particular, a aplicação de navegador 420 permite a um usuário exibir e interagir com texto, imagens, vídeos, música e outras informações que é acessível através da rede de comunicação 160 a partir do computador servidor 110. A aplicação de navegador 410 pode se comunicar com o computador servidor 110 através da aplicação proxy 420 e pela rede de comunicação 160, por exemplo, por meio do protocolo HTTP na camada de aplicação e o Protocolo de Controle de Transmissão/ Protocolo de Internet (TCP/ IP) na camada de rede.

[0097] Em um modo de funcionamento normal, a aplicação de navegador 410 se conecta através da aplicação de proxy 420 à rede de comunicação 160. No modo de funcionamento normal, a aplicação de navegador 410 executa um segundo protocolo de comunicação e pode enviar solicitações de clientes, por exemplo, solicitações get

HTTP, através da aplicação proxy 420 e a rede de comunicação 160 para o computador servidor 110. Na outra direção, o computador servidor 110 pode enviar no modo de operação normal respostas do servidor, por exemplo, respostas http, via rede de comunicação 160 e a aplicação proxy 420 para a aplicação de navegador 410. No modo de funcionamento normal, a aplicação proxy 420 trabalha como remetente entre a aplicação de navegador 410 e a rede de comunicação 160 e, simultaneamente, observa e analisa, respectivamente, as solicitações do cliente para um conjunto predefinido de solicitações de clientes. O conjunto predefinido de solicitações de clientes pode ser, por exemplo, um conjunto de *Uniform Resource Locator* (URL). O conjunto predefinido de solicitações de clientes representam um conjunto de recursos para o qual o usuário do computador cliente 120 tem predefinidos que uma comunicação com este recurso deve ser controlada pelo dispositivo de hardware 130. Como um exemplo, o usuário do computador cliente 120 pode definir o URL do seu banco como uma solicitação predefinida na aplicação proxy 420. Em seguida, a aplicação proxy 420 observaria se o usuário digita a URL correspondente deste banco na aplicação de navegador 410. Em outras palavras, a aplicação proxy 420 observa se o usuário envia uma solicitação do cliente para acessar a URL predefinida pela rede de comunicação 160 para o computador servidor 110. Após a detecção de uma das solicitações de cliente predefinidas, a aplicação proxy 420 muda para e inicia um modo de funcionamento seguro. No modo de funcionamento seguro, a aplicação proxy 420 altera as solicitações de fluxo de dados e as rotas de clientes recebidos a partir da aplicação de navegador 410 para o dispositivo de hardware 130. Além disso, a aplicação proxy

420 inicia o modo de operação seguro, enviando um sinal apropriado, por exemplo, um sinal de ativação de modo seguro, para o dispositivo de hardware 130. Em seguida, o dispositivo de hardware 130 inicia e executa um primeiro protocolo de comunicação com a transmissão de dados criptografados e autenticação mútua entre o computador servidor 110 e o dispositivo de hardware 130. A seguir, o dispositivo de hardware 130 trabalha como uma interface inteligente entre o computador servidor 110 e a aplicação de navegador 410 do computador cliente 120. Em outras palavras, o dispositivo de hardware 130 controla e observa a comunicação de dados entre o computador servidor 110 e a aplicação de navegador 410. No modo de operação seguro, a aplicação proxy 420 funciona como uma espécie de interruptor. Por um lado, a aplicação proxy 420 encaminha no modo de funcionamento seguro, solicitações de clientes recebidas do dispositivo de hardware 130 para a rede de comunicação 160 e respostas de servidor recebidas a partir da rede de comunicação 160 para o dispositivo de hardware 130. Por outro lado, a aplicação proxy 420 encaminha no modo de funcionamento seguro solicitações de clientes recebidas da aplicação de navegador 410 para o dispositivo de hardware 130 e respostas do servidor recebidas do dispositivo de hardware 130 para a aplicação de navegador 410.

[0098] Após o primeiro protocolo de comunicação ter sido estabelecido, o dispositivo de hardware 130 analisa solicitações de clientes recebidas do computador cliente 120 ou da aplicação de navegador 410, respectivamente, para informações sobre a transação predefinida. Em outras palavras, o dispositivo de hardware 130 observa se o tráfego de dados que recebe do computador cliente 120 contém qualquer

informação de transação predefinida. Tais informações de transação predefinidas podem ser informações seguras sensíveis por exemplo, tais como detalhes de pagamento, valores de pagamento etc. A informação de transação predefinida pode ser, por exemplo predefinida pelo proprietário do respectivo URL, por exemplo, o banco que o usuário deseja realizar uma transação. As informações de transação predefinidas podem ser, por exemplo, enviadas por meio de uma solicitação HTTP POST. Após a detecção de informações de transações predefinidas o dispositivo de hardware 130 interrompe a solicitação do cliente correspondente e exibe as informações de transação predefinidas detectadas no visor do dispositivo de hardware 210 do dispositivo de hardware 130. O usuário que quer realizar a transação pode então verificar no visor do dispositivo de hardware 210 se as informações respectivas sobre a transação estão corretas. Como exemplo, se as informações de transação predefinidas se referem ao valor da transferência de um pagamento eletrônico, o dispositivo de hardware 130 iria exibir no visor do dispositivo de hardware 210 o respectivo valor da transferência. O usuário pode verificar no visor do dispositivo de hardware 210 se o valor da transferência está correto. O dispositivo de hardware 130 se limita a continuar com a transação se o usuário confirma a transação através da unidade de entrada de dispositivo de hardware 280, por exemplo, pressionando um botão de confirmação. Se o dispositivo de hardware 130 recebe uma tal confirmação, ele continua com a transação e encaminha as informações de transação por meio da aplicação proxy 420 e a rede de comunicação 160 para o computador servidor 110. Se o dispositivo de hardware 130 recebe nenhuma confirmação ou

um sinal de cancelamento, ele cancela a transação e não encaminha as informações de transação para a aplicação proxy 420.

[0099] De preferência, o dispositivo de hardware 130 envia, após a detecção de informações de transações predefinidas, uma mensagem de interrupção, também denotada como a mensagem de solicitação de confirmação, de volta para a aplicação de navegador 410. Tal mensagem de interrupção pode indicar à aplicação de navegador 410 que o dispositivo de hardware 130 identificou informações de transação predefinidas e está aguardando uma confirmação do usuário antes de continuar com a transação. A aplicação de navegador 410 apresenta de preferência uma mensagem de interrupção correspondente, também denotada como a mensagem de solicitação de confirmação, para o usuário no visor do computador cliente 121. Tal mensagem de interrupção por exemplo, poderia informar ao usuário que ele deve verificar no visor do dispositivo de hardware 210 se a informação de transação está correta e que ele deve confirmar isso através da unidade de entrada de dispositivo de hardware 280.

[0100] O dispositivo de hardware 130 compreende um programa de análise para analisar as solicitações do cliente. O programa de análise compreende as informações de transação predefinidas e pode ser de aplicação específica. Como um exemplo, os bancos podem emitir um dispositivo de hardware específico do banco 130 no qual um programa de análise específico do banco é carregado. O respectivo banco poderia adaptar o programa de análise para o seu processo de banco on-line específica e suas necessidades e requisitos de segurança específicos. De preferência, o programa de análise é inicializado em um ambiente confiável e seguro, por

exemplo, em um site seguro do banco. O programa de análise é de preferência carregado e armazenado no token de segurança 310 ou no cartão inteligente 260 do dispositivo de hardware 130. No entanto, de acordo com outra concretização da invenção, o programa de análise pode ser armazenado no armazenamento 230 do dispositivo de hardware 130.

[0101] De acordo para uma concretização da invenção, o dispositivo de hardware 130 analisa as respostas do servidor recebidas a partir do computador servidor 110 para informações sobre a transação predefinida. Em outras palavras, além de analisar a solicitação do cliente, o dispositivo de hardware 130 analisa também as respostas do servidor para informações sobre a transação predefinida.

[0102] O processo de análise realizado pelo dispositivo de hardware 130 para solicitações do cliente e respostas do servidor é indicado na Figura 4 por meio das linhas em tracejado.

[0103] A figura 5, 6, 7 e 8 mostram uma ilustração esquemática de um fluxo de mensagens de um método de acordo com uma concretização da invenção. Nesse sentido, o fluxo de mensagens entre o computador servidor 110, a aplicação proxy 420, a aplicação de navegador 410 e o dispositivo de hardware 130 é representado com setas rotuladas as quais respectivos números de referência são atribuídos. Outras etapas ou sub-etapas são indicadas por números de referência em um círculo. O fluxo é entendido como sendo realizado sequencialmente a partir de cima para baixo, como indicado pelos números de referência crescentes.

[0104] A figura 5 ilustra o fluxo de mensagens de um modo de funcionamento normal.

[0105] Numa etapa 510, o usuário do computador cliente 120 insere uma solicitação de cliente, por exemplo um URL de um site, por meio da unidade de entrada do computador cliente 122. Numa etapa 520, a aplicação de navegador 410 envia a solicitação de cliente, por exemplo, uma solicitação Get HTTP que compreende o URL de um site, para a aplicação proxy 420. Numa etapa 530 a aplicação proxy 420 analisa a solicitação do cliente para um conjunto predefinido de solicitações, por exemplo, para um conjunto predefinido de URLs. Neste exemplo é assumido que a solicitação do cliente enviada na etapa 520 não pertence ou corresponde ao conjunto predefinido de solicitações de clientes. Assim, a aplicação proxy 420 encaminha a solicitação do cliente na etapa 540 através da rede de comunicação 160 para o computador servidor 110. Na etapa 550, o computador servidor 110 responde ao enviar de volta uma resposta do servidor, por exemplo, uma resposta de servidor HTTP que compreende um arquivo HTML do URL solicitado. Em seguida, na etapa 560 a resposta do servidor, por exemplo, o arquivo HTML do URL solicitado, é exibido no visor do computador cliente 121.

[0106] As etapas 510, 520, 530, 540, 550 e 560 representam um modo de funcionamento normal da aplicação de navegador 410 e da aplicação proxy 420. O modo de funcionamento normal pode ser executado sem o dispositivo de hardware 130. No modo de funcionamento normal, um segundo protocolo de comunicação é executado entre a aplicação de navegador 410 e o computador servidor 110.

[0107] Numa etapa 570, o usuário do computador cliente 120 insere outra solicitação de cliente, por exemplo um URL de um site, por meio da unidade de entrada de

computador do cliente 122. Na etapa 580, a solicitação do navegador 410 envia uma solicitação de cliente correspondente à solicitação proxy 420. Neste exemplo é assumido que a solicitação do cliente enviada na etapa 580 pertence ou corresponde ao conjunto predefinido de solicitações de clientes. Como um exemplo, a solictação de cliente enviada na etapa 580 pode ser uma solicitação GET HTTP para um URL que pertence ao conjunto predefinido de URLs. Isso pode ser, por exemplo, a URL do site do banco do usuário. Numa etapa 590, a aplicação proxy 420 analisa a solicitação do cliente para o conjunto predefinido de solicitações e detecta que a solicitação do cliente enviada na etapa 580 pertence ou corresponde ao conjunto predefinido de solicitações de clientes. Assim, a aplicação proxy 420 muda para um modo de funcionamento seguro e inicia na etapa 595 o modo de funcionamento seguro do dispositivo de hardware 130 através do envio de um sinal de ativação de modo seguro para o dispositivo de hardware 130. O sinal de ativação de modo seguro pode ser, por exemplo implementado como "iniciar o modo seguro" – comando que é entendido pelo dispositivo de hardware 130. O sinal de ativação de modo seguro indica ao dispositivo de hardware 130 que deve iniciar o modo de funcionamento seguro para a comunicação subsequente entre a aplicação de navegador 410 e o computador servidor 110.

[0108] Com referência às Figuras 6, 7 e 8, o fluxo de mensagens no modo de funcionamento seguro é ilustrado.

[0109] Depois de ter recebido o sinal de ativação de modo seguro na etapa 595, o dispositivo de hardware 130 envia na etapa 605 uma mensagem de solicitação de confirmação (CRM) por meio da aplicação proxy 420 da aplicação de navegador 410. Em seguida, na etapa 610 a aplicação de navegador 410

exibe a mensagem de solicitação de confirmação para o usuário no visor do computador cliente 121. A mensagem de solicitação de confirmação solicita ao usuário para confirmar que o modo de funcionamento seguro deve ser realizado. Pode, por exemplo ler o seguinte: "O site que você solicitou requer a inicialização de um modo de funcionamento seguro. Por favor, confirme se você concorda, ao pressionar o botão de confirmação do seu dispositivo de hardware". Na etapa 615 uma mensagem correspondente, em particular numa forma abreviada como "Confirmar modo seguro?" é apresentada no visor do dispositivo de hardware 210 do dispositivo de hardware 130. A resposta de confirmação do usuário pode ser recebida na etapa 620 através da unidade de entrada do dispositivo de hardware 280.

[0110] Após a confirmação do usuário na etapa 620 o dispositivo de hardware 130 envia na etapa 625 uma mensagem de olá através da aplicação proxy 420 e a rede de comunicação 160 para o computador servidor 110. Na etapa 630, o computador servidor 110 envia uma mensagem de Olá de volta pela rede de comunicação 160 e a aplicação proxy 420 para o dispositivo de hardware 130. Na etapa 635, o computador servidor 110 autentica-se ao dispositivo de hardware 130. Isto pode incluir o envio de um certificado de servidor (certificado de chave pública) para o dispositivo de hardware 130. Além disso, pode incluir uma solicitação de certificado para um certificado de cliente. Na etapa 640, o computador cliente 120 autentica-se ao computador servidor 110. Isto pode incluir o envio de um certificado de cliente (certificado de chave pública) para o computador servidor 110. Em resumo, o computador servidor 110 e o dispositivo de

hardware 130 executam nas etapas 635 e 640 uma autenticação mútua.

[0111] Nas etapas 645 e 650 o servidor de computador 110 e o dispositivo de hardware 130 trocam uma chave criptográfica simétrica SK, também denotada como chave de sessão.

[0112] As etapas 625 a 650 podem ser, por exemplo implementadas por meio do protocolo de reconhecimento de SSL/ TLS.

[0113] A seguir, a transmissão de dados entre o dispositivo de hardware 130 e o computador servidor 110 é executada de uma forma criptografada por meio da chave de sessão SK. Isto pode ser, por exemplo implementado por meio do protocolo de registro SSL/ TLS.

[0114] Na etapa 655 o computador servidor 110 envia uma resposta de autenticação do usuário para o dispositivo de hardware 130. Tal resposta autenticação do usuário pode, por exemplo compreender um formulário HTML com um campo de usuário e um campo de senha em que o usuário insere seu nome e sua senha.

[0115] A resposta de autenticação de usuário é descriptografado na etapa 657 pelo dispositivo de hardware 130 e, em seguida, encaminhados em uma etapa 660 através da aplicação proxy 420 para a aplicação de navegador 410. Na etapa 662 a resposta de autenticação de usuário é exibida no visor do computador cliente 121. Na etapa 665 o usuário insere seus dados pessoais de autenticação, por exemplo, o seu nome de usuário e sua senha, para o formulário HTML correspondente por meio da unidade de entrada do computador cliente 122. Em seguida, na etapa 670 a aplicação de navegador 410 envia uma solicitação HTTP POST compreendendo

os dados de autenticação do usuário para o dispositivo de hardware 130. Na etapa 675 o dispositivo de hardware analisa a solicitação HTTP POST para informações sobre a transação predefinida. Neste exemplo, assume-se que uma solicitação HTTP POST com informações para autenticação do usuário não é informação predefinida sobre a transação. Assim, na etapa 677 a solicitação HTTP POST é criptografada por meio da chave de sessão simétrica SK e enviada na etapa 680 para o computador servidor 110. O computador servidor 110 decifra a solicitação HTTP POST por meio da chave de sessão simétrica SK e, se os dados de autenticação do usuário forem válidos, autentica o usuário na etapa 695. Caso contrário, o computador servidor 110 pode cancelar a transação.

[0116] As etapas 655-695 ilustram uma autenticação de usuário adicional pelo computador servidor 110 que podem ser implementadas para aumentar a segurança no caso em que o dispositivo de hardware 130 é roubado ou perdido. De acordo com uma outra concretização exemplar a autenticação do usuário adicional descrita com referência nas etapas 655-695 é substituída por uma autenticação do usuário executada pelo dispositivo de hardware 130.

[0117] A ilustração do fluxo de mensagens no modo de funcionamento seguro após a autenticação do usuário é continuada com referência a Figura 7.

[0118] Na etapa 705 o computador servidor 110 envia como resposta do servidor uma resposta de transação através da aplicação proxy 420 para o dispositivo de hardware 130. Tal resposta de transação poderia, por exemplo, compreender um arquivo HTML com conta bancária de dados do usuário que foi autenticado nas etapas anteriores. Numa etapa 710, o dispositivo de hardware 130 descriptografa a resposta do

servidor por meio da chave de sessão simétrica SK. Na etapa 715, o dispositivo de hardware 130 pode analisar a resposta do servidor para informações sobre a transação predefinida. Neste exemplo é assumido que a resposta do servidor recebida na etapa 705 não inclui informação de transação predefinida. Em seguida, na etapa 720, a resposta do servidor descriptografada é enviada do dispositivo de hardware 130 via a aplicação proxy 420 para a aplicação de navegador 410. Na etapa 725, a aplicação de navegador 410 exibe a resposta do servidor no visor do computador cliente 121 do computador cliente 120.

[0119] Segundo com um outro exemplo, como ilustrado com linhas em tracejado, assume-se que a resposta do servidor recebida na etapa 705 não compreendem informação de transação predefinida. Em seguida, o dispositivo de hardware 130 detecta na etapa de análise 715 que a resposta do servidor compreende informações de transação predefinida. Assim, o dispositivo de hardware 130 exibe na etapa 717, as informações de transação predefinidas de resposta do servidor no visor do dispositivo hardware 210. Se o usuário confirma em uma etapa 718 as informações de transação da resposta do servidor exibido no visor do dispositivo de hardware 210, por meio da unidade de entrada de dispositivo de hardware 280, o método continua com a etapa 720. Se o usuário não confirma as informações de transação da resposta do servidor, o dispositivo de hardware 130 cancela a transação.

[0120] Na etapa 730, o usuário insere uma solicitação de cliente que não inclui informações sobre a transação predefinida. Isto poderia ser, por exemplo, uma solicitação de cliente para obter dados específicos da conta bancária do

usuário, para mostrar mais detalhes da conta bancária ou para executar uma verificação inicial de uma transação eletrônica planejada, por exemplo, de uma transferência de dinheiro. Na etapa 735 a aplicação de navegador 410 envia a solicitação do cliente por meio da aplicação proxy 420 para o dispositivo de hardware 130. Na etapa 740 o dispositivo de hardware 130 analisa a solicitação do cliente recebida para informações de transações predefinidas e detecta que a solicitação do cliente não inclui informações sobre a transação predefinida. Em seguida, na etapa 745 o dispositivo de hardware 130 criptografa a solicitação do cliente, por meio da chave de sessão simétrica SK e envia a solicitação de cliente criptografada na etapa 750 para a aplicação proxy 420. A aplicação proxy 420 envia a solicitação do cliente criptografada na etapa 750 através da rede de comunicações 160 para o computador servidor 110. Na etapa 755, o computador servidor 110 descriptografa a solicitação criptografada recebida do cliente por meio da chave de sessão simétrica SK e processa a solicitação do cliente descriptografada. Na etapa 760 o computador servidor 110 envia uma resposta do servidor no que diz respeito à solicitação do cliente recebida através da aplicação proxy 420 de volta para o dispositivo de hardware 130. Numa etapa 765 o dispositivo de hardware 130 descriptografa a resposta do servidor por meio da chave de sessão simétrica SK. Na etapa 770, o dispositivo de hardware 130 pode analisar a resposta do servidor para informações sobre a transação predefinida. Neste exemplo é assumido que a resposta do servidor recebida na etapa 760 não inclui informação de transação predefinida. Assim, na etapa 775 a resposta do servidor descriptografada é enviada do dispositivo de

hardware 130 via a aplicação proxy 420 para a aplicação de navegador 410 e na etapa 780 a aplicação de navegador 410 exibe a resposta do servidor no visor do computador cliente 121 do computador cliente 120.

[0121] A figura 8 ilustra o fluxo de mensagens no modo de funcionamento seguro de uma solicitação de cliente que compreende informações de transação predefinidas.

[0122] Na etapa 805, o usuário insere uma solicitação de cliente que não compreende informações de transação predefinidas. As informações de transação predefinidas podem ser, por exemplo, uma ordem final para realizar uma transação eletrônica. Tal ordem final pode ser, por exemplo, uma ordem de transferência de dinheiro com detalhes de pagamento, como o montante da transferência de dinheiro. As informações de transação predefinidas podem ser, por exemplo digitadas pelo usuário em um formulário HTML correspondente por meio da unidade de entrada de computador cliente 122. Na etapa 810 a aplicação de navegador 410 envia uma solicitação do cliente, compreendendo as informações de transação predefinidas através da aplicação proxy 420 ao dispositivo de hardware 130. Isso poderia ser, por exemplo, uma solicitação HTTP post. Na etapa 815 o dispositivo de hardware 130 analisa a solicitação do cliente recebida para informações de transações predefinidas e detecta que a solicitação do cliente compreende informações de transação predefinidas, por exemplo, os detalhes de pagamento finais mencionados acima de uma transferência de dinheiro. Em seguida, na etapa 820 o dispositivo de hardware 130 envia uma mensagem de solicitação de confirmação (CRM) por meio da aplicação proxy 420 da aplicação de navegador 410. A aplicação de navegador 410 exibe na etapa 825 a mensagem de

solicitação de confirmação no visor do computador cliente 121 do computador cliente 120. A mensagem de solicitação de confirmação indica ao usuário que o dispositivo de hardware 130 detectou informações de transação predefinidas e que o usuário deve verificar e confirmar a exatidão das informações de transação no visor do dispositivo de hardware 210 de hardware do dispositivo 130. A mensagem de solicitação de confirmação poderia por exemplo, ter a seguinte redação: "Por favor, verifique o valor da transferência no visor do seu token de segurança. Se o montante da transferência estiver correto, confirme a operação pressionando o botão de confirmação do token de segurança.".

[0123] Na etapa 830, o dispositivo de hardware 130 exibido no visor do dispositivo de hardware 210 as informações de transação predefinida (PTI), por exemplo, a quantidade de dinheiro a ser transferido e a conta de destino. Além disso, algumas mensagens de confirmação poderiam ser exibidas no visor do dispositivo de hardware 210 também. Como o visor do dispositivo de hardware 210 pode ser bastante pequeno, de tal mensagem de confirmação é de preferência bastante curta, como "Por favor, confirme a transferência de uma quantidade X de explicar Y". O usuário pode então verificar no visor do dispositivo de hardware 210 se a informação da transação está correta. Além disso, ele pode comparar a informação de transação mostrada no visor do dispositivo de hardware 210 com a informação de transação exibida no visor do computador cliente 121. Se o usuário confirma, numa etapa 835 de confirmação de que a informação de transação mostrada no visor do dispositivo de hardware 210 está correta, por exemplo, pressionando um botão de confirmação da unidade de entrada de dispositivo de hardware

280, a transação será continuada. Em seguida, na etapa 840 o dispositivo de hardware 130 criptografa a solicitação do cliente, compreendendo as informações de transação por meio da chave de sessão simétrica SK e envia a solicitação do cliente criptografada na etapa 845 para a aplicação proxy 420. A aplicação proxy 420 encaminha a solicitação do cliente criptografada via rede de comunicação 160 para o computador servidor 110. O computador servidor 110 descriptografa na etapa 850 a solicitação do cliente criptografada recebida pela chave de sessão simétrica SK. Em seguida, na etapa 855 o computador servidor 110 executa a operação. No exemplo de transferência de dinheiro o computador servidor 110 transferiria na etapa 855 o dinheiro para a conta de destino.

[0124] Se o usuário não confirmar que a informação de transação mostrada no visor do dispositivo de hardware 210 está correta, o método continua com a etapa 870. Isto é indicado pela linha em tracejado. A não confirmação da transação pode ser invocada ativamente pelo usuário, por exemplo pressionando um botão de cancelamento da unidade de entrada de dispositivo de hardware 280 ou passivamente, por exemplo, se o dispositivo de hardware 130 não recebendo uma confirmação dentro de um período de tempo limite predefinido. Em seguida, na etapa 875 o dispositivo de hardware 130 cancela a transação e não encaminha as informações de transação para o computador servidor 110. Além disso, na etapa 880 o hardware do dispositivo 130 pode enviar uma mensagem de cancelamento (CM) por meio da aplicação proxy 420 para a aplicação de navegador 410. A aplicação de navegador 410 é exibida na etapa 885 a mensagem de cancelamento no visor do computador cliente 121 do computador cliente 120. A mensagem de cancelamento indica ao usuário

que o dispositivo de hardware 130 cancelou a transação. A mensagem de cancelamento poderia, por exemplo ter a seguinte redação: "A operação foi cancelada devido a não confirmação. Se você observou uma discrepância entre as informações de transação que você inseriu através do teclado do seu PC e as informações de transação mostradas no visor de seu token de segurança, o seu PC pode ser comprometido por software malicioso". Além disso, a mensagem de cancelamento poderia ser exibida na etapa 890 no visor do dispositivo de hardware 210 também.

[0125] Qualquer concretização descrita pode ser combinada com uma ou várias das outras concretizações mostradas e/ ou descritas. Isto também é possível para uma ou mais características de concretizações.

Detalhes de Concretização adicional

[0126] As técnicas descritas podem ser implementadas como método, dispositivo ou artigo de fabricação que envolve o software, firmware, microcódigo, hardware e/ ou qualquer combinação dos mesmos. O termo "artigo de fabricação", como aqui utilizado refere-se a código ou lógica implementados em um meio, em que tal meio pode compreender lógica de hardware [por exemplo, um chip de circuito integrado, arranjo de portas programáveis em campo (*Programmable Gate Array* – PGA), Circuito Integrado de Aplicação Específica (ASIC), etc.] ou de um meio legível por computador, como meio de armazenamento magnético (por exemplo, unidades de disco rígido, disquetes, fitas, etc.), de armazenamento óptico (CD-ROMs, discos ópticos, etc.), dispositivos de memória volátil e não volátil [por exemplo, memória somente de leitura programável eletricamente apagável (*Electrically Erasable Programmable Read Only Memory* – EEPROM), memória somente de leitura (*Read*

Only Memory – ROM), memória somente de leitura programável (*Programmable Read Only Memory* – PROM), memória de acesso aleatório (RAM), memória de acesso aleatório dinâmica (DRAM), memória de acesso aleatório estática (SRAM), flash, firmware, lógica programável, etc.]. Código no meio legível por computador é acessado e executado por um processador. O meio no qual o código ou lógica é codificado pode também compreender sinais de transmissão que se propagam através do espaço ou de um meio de transmissão, tal como uma fibra óptica, fio de cobre, etc. O sinal de transmissão, no qual o código ou lógica é codificado pode ainda compreender um sinal sem fio, transmissão por satélite, ondas de rádio, sinais infravermelhos, Bluetooth, etc. O sinal de transmissão, na qual o código ou lógica é codificado é capaz de ser transmitido por uma estação de transmissão e recebido por uma estação de recepção, onde o código ou lógica codificado no sinal de transmissão podem ser decodificados e armazenados em hardware ou um meio legível por computador nas estações ou dispositivos de recepção e transmissão. Além disso, o "artigo de fabricação" pode compreender uma combinação de componentes de hardware e software no qual o código é incorporado, processado e executado. É claro, os versados na técnica reconhecerão que muitas modificações podem ser feitas sem se afastar do escopo das concretizações, e que o artigo de fabricação pode compreender qualquer meio de armazenamento de informação. Por exemplo, o artigo de fabricação compreende um meio de armazenamento que tem nele armazenadas instruções que, quando executadas por uma máquina resultam em operações sendo executadas.

[0127] Certas concretizações podem ter a forma de uma concretização totalmente de hardware, uma concretização

totalmente software ou uma concretização contendo ambos os elementos de hardware e de software. Numa concretização preferida, a invenção é implementada em software, que inclui, mas não está limitada a firmware, software residente, microcódigo, etc.

[0128] Além disso, certas concretizações podem ter a forma de um produto de programa de computador acessível a partir de um meio legível por computador utilizável ou computador proporcionando código de programa para o uso por ou em ligação com um computador ou qualquer sistema de execução de instruções. Para os fins desta descrição, um meio legível por computador ou computador utilizável pode ser qualquer aparelho que pode conter, armazenar, comunicar, propagar ou transportar o programa para uso por ou em conexão com o sistema de execução de instruções, aparelho ou dispositivo. O meio pode ser um sistema eletrônico, magnético, óptico, eletromagnético, infravermelho ou semicondutor (ou aparelho ou dispositivo) ou um meio de propagação. Exemplos de um meio legível por computador incluem um semicondutor ou memória de estado sólido, uma fita magnética, um disquete de computador removível, uma memória de acesso aleatório (RAM), uma memória somente de leitura (ROM), um disco rígido magnético e um disco óptico. Exemplos atuais de discos ópticos incluem disco compacto de memória somente de leitura (CD-ROM), disco compacto – leitura/ gravação (CD-RAV) e DVD. Os termos "certas concretizações", "Uma concretização", "incorporação", "concretizações", "a incorporação", "as concretizações", "uma ou mais concretizações", "algumas concretizações", e "uma concretização" significam uma ou mais (mas não todos) concretizações, a menos que expressamente especificado de

outra forma. Os termos "incluindo", "compreendendo", "tendo" e as suas variantes significam "incluindo mas não limitado a", a menos que expressamente especificado em contrário. O perfil enumerado de itens não implica que qualquer um ou todos os itens são mutuamente exclusivos, a menos que expressamente especificado em contrário. Os termos "um", "uma" e "a" significa "um ou mais", a menos que expressamente especificado ao contrário. Os dispositivos que estão em comunicação uns com os outros não precisam estar em comunicação permanente com o outro, a menos que expressamente especificado em contrário. Além disso, os dispositivos que estão em comunicação uns com os outros podem se comunicar diretamente ou indiretamente através de um ou mais intermediários. Além disso, a descrição de uma concretização com vários componentes em comunicação um com o outro não implica que todos estes componentes são necessários. Ao contrário, uma variedade de componentes opcionais é descrita para ilustrar a grande variedade de concretizações possíveis.

[0129] Além disso, embora as etapas do processo, as etapas do método, algoritmos ou semelhantes podem ser descritos por uma ordem sequencial, tais processos, métodos e algoritmos pode ser configurado para funcionar em ordens alternativas. Em outras palavras, qualquer sequência ou ordem das etapas que pode ser descrito não indica necessariamente um requisito de que as etapas sejam realizadas nesta ordem. As etapas de processo aqui descritas podem ser realizadas em qualquer ordem prática. Além disso, algumas etapas podem ser realizadas simultaneamente, em paralelo, ou em simultâneo.

[0130] Quando um único dispositivo ou artigo é aqui descrito, será evidente que mais do que um dispositivo/ artigo (quer sejam ou não cooperar) pode ser usado em lugar de um único dispositivo/ artigo. Do mesmo modo, em que mais do que um dispositivo ou artigo está aqui descritos (estejam ou não cooperem), será evidente que um único dispositivo/ artigo pode ser usado no lugar da mais do que um dispositivo ou artigo. A funcionalidade e/ ou as características de um dispositivo pode ser alternativamente incorporada com um ou mais outros dispositivos que não estão explicitamente descritos como tendo tais características/ funcionalidade. Assim, outras concretizações não precisam incluir o próprio dispositivo.

[0131] O meio de programa de computador ou programa de computador no presente contexto, significa qualquer expressão, em qualquer linguagem, código ou notação, de um conjunto de instruções destinado a fazer com que um sistema tendo uma capacidade de processamento de informação realize uma função específica, quer diretamente ou depois de qualquer um ou ambos o seguinte a) conversão para outra linguagem, código ou notação; b) reprodução de uma forma material diferente.

REIVINDICAÇÕES

1. Método para executar transações eletrônicas entre um computador servidor (110) e um computador cliente (120) por meio de um dispositivo de hardware (130), compreendendo, no dispositivo de hardware (130), as etapas de:

- executar um primeiro protocolo de comunicação com a transmissão de dados criptografados e autenticação mútua entre o computador servidor (110);

- executar uma descriptografia de respostas do servidor criptografadas recebidas do computador servidor (110);

- encaminhar as respostas do servidor descriptografadas para o computador servido (110) a partir do computador cliente (120),

caracterizado pelo fato de

- analisar as solicitações de clientes por informações de transação predefinida que foram inseridas por um usuário por meio de uma unidade de entrada de computador cliente;

- criptografar e encaminhar solicitações de clientes que não contenham qualquer informação sobre transações predefinidas para o computador servidor (110);

- exibir as informações sobre a transação predefinida para confirmação de usuário para um usuário mediante detecção de uma solicitação do cliente;

- encaminhar e criptografar a solicitação do cliente com as informações de transações predefinidas para o computador servidor (110) se uma confirmação do usuário é recebida, em que o dispositivo de hardware interpreta como uma confirmação se o usuário não cancelar a transação dentro de um período de tempo predefinido.

2. Dispositivo de hardware (130) para controlar transações eletrônicas, compreendendo uma unidade de interface de dispositivo de hardware (270), em que a unidade de interface do dispositivo de hardware (270) é fornecida para o acoplamento do dispositivo de hardware (130) com um computador cliente (120), em que o dispositivo de hardware (130) é adaptado para:

- executar um primeiro protocolo de comunicação com a transmissão de dados criptografados e autenticação mútua entre o computador servidor (110);

- executar uma descriptografia de respostas do servidor criptografadas recebidas do computador servidor (110);

- encaminhar as respostas do servidor descriptografadas para o computador cliente (120),

- receber solicitações de clientes para enviar a partir do computador cliente (120) para o computador servidor (110),

caracterizado pelo fato de que compreende um dispositivo de exibição de hardware (210), e em que o dispositivo de hardware (130) é adaptado para:

- analisar as solicitações de clientes por informações de transação predefinidas que foram inseridas por um usuário por meio de uma unidade de entrada de computador cliente;

- criptografar e encaminhar solicitações de clientes que não contenham qualquer informação sobre transações predefinidas para o computador servidor (110);

- exibir as informações sobre a transação predefinida mediante detecção de uma solicitação do cliente para

confirmação de usuário no dispositivo de exibição de hardware (210);

- encaminhar e criptografar a solicitação do cliente com as informações de transações predefinidas para o computador servidor (110) se uma confirmação do usuário é recebida;

interpretar como uma confirmação se o usuário não cancelar a transação dentro de um período de tempo predefinido.

3. Dispositivo de hardware (130), de acordo com a reivindicação 2, **caracterizado pelo** fato de que o dispositivo de hardware (130) compreende um token de segurança (310) para armazenar dados sensíveis à segurança.

4. Dispositivo de hardware (130), de acordo com a reivindicação 2, **caracterizado pelo** fato de que o dispositivo de hardware (130) inclui uma leitora de cartão inteligente (250) para a leitura de dados sensíveis à segurança a partir de um cartão inteligente (260).

5. Dispositivo de hardware (130), de acordo com qualquer uma das reivindicações 2 a 4, **caracterizado pelo** fato de que o dispositivo de hardware (130) tem um nível predefinido de resistência à adulteração.

6. Dispositivo de hardware (130), de acordo com a reivindicação 5, **caracterizado pelo** fato de que o nível predefinido de resistência à adulteração do dispositivo de hardware (130) é maior do que o nível de resistência à adulteração do computador cliente (120).

7. Dispositivo de hardware (130), de acordo com qualquer uma das reivindicações 2 a 6, **caracterizado pelo** fato de que o dispositivo de hardware (130) é projetado de

tal forma que nenhuma aplicação de software pode ser carregada no dispositivo de hardware (130).

8. Dispositivo de hardware (130), de acordo com a reivindicação 3 ou 4, **caracterizado pelo** fato de que os dados sensíveis à segurança compreendem uma chave privada e informações de raiz confiável.

9. Dispositivo de hardware (130), de acordo com qualquer uma das reivindicações 2 a 8, **caracterizado pelo** fato de que o dispositivo de hardware (130) compreende uma unidade de entrada do dispositivo de hardware (280) para confirmar e/ou cancelar uma transação.

10. Dispositivo de hardware (130), de acordo com a reivindicação 2, **caracterizado pelo** fato de que o primeiro protocolo de comunicação compreende uma camada de rede que inclui um protocolo de acordo com o padrão SSL (*Secure Sockets Layer*) ou de acordo com o padrão TSL (*Transport Layer* Security) e um protocolo de acordo com o padrão TCP-IP (*Transmission Control Protocol/Internet Protocol*).

11. Dispositivo de hardware (130), de acordo com a reivindicação 2, **caracterizado pelo** fato de que as informações de transação predefinida são números de conta bancária e um valor de pagamento.

12. Método para executar transações eletrônicas entre um computador servidor (110) e um computador cliente (120) por meio de um dispositivo de hardware (130), compreendendo, no dispositivo de hardware (130), as etapas de:

- executar um primeiro protocolo de comunicação com a transmissão de dados criptografados recebidos do computador servidor (110);

- executar uma descriptografia de respostas do servidor criptografadas recebidas do computador servidor (110), **caracterizado pelo** fato de;

- analisar as respostas de servidor para informações de transação predefinida;

- encaminhar solicitações de clientes que não contenham qualquer informação sobre transações predefinidas para o computador cliente (120);

- exibir as informações sobre a transação predefinida para confirmação de usuário para um usuário mediante detecção de uma resposta de servidor;

- encaminhar a resposta de servidor contendo as informações de transações predefinidas para o computador cliente (120) se uma confirmação do usuário é recebida,

em que o dispositivo de hardware interpreta isso como uma confirmação se o usuário não cancelar a transação dentro de um período de tempo predefinido.

13. Dispositivo de hardware (130) para controlar transações eletrônicas, compreendendo um dispositivo de exibição de hardware (210) e uma unidade de interface de dispositivo de hardware (270), em que a unidade de interface do dispositivo de hardware (270) é fornecida para o acoplamento do dispositivo de hardware (130) com um computador cliente (120), em que o dispositivo de hardware (130) é adaptado para:

- executar um primeiro protocolo de comunicação com a transmissão de dados criptografados e autenticação mútua com o computador servidor (110);

- executar uma descriptografia de respostas do servidor criptografadas recebidas do computador servidor (110);

caracterizado pelo fato de que compreende um dispositivo de exibição de hardware (210), e em que o dispositivo de hardware (130) é adaptado para:

- analisar as respostas de servidor para informações de transação predefinida;

- encaminhar respostas de servidor que não contenham qualquer informação sobre transações predefinidas para o computador cliente (120);

- exibir as informações sobre a transação predefinida para confirmação de usuário mediante detecção em uma resposta de servidor no dispositivo de exibição de hardware (210);

- encaminhar as respostas de servidor contendo as informações de transações predefinidas para o computador cliente (120) se uma confirmação do usuário é recebida,

- interpretar como uma confirmação se o usuário não cancelar a transação dentro de um período de tempo predefinido.

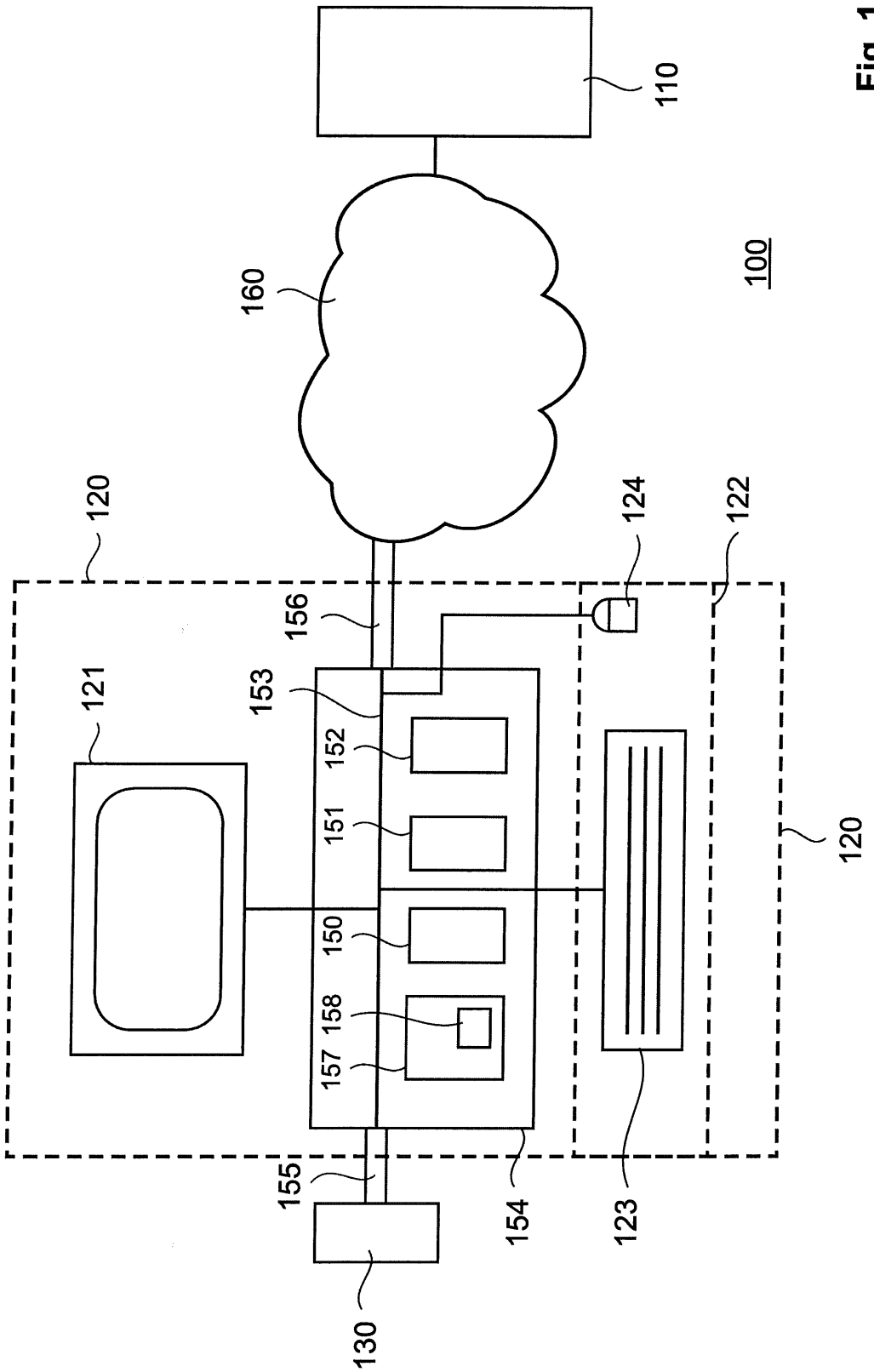

110
160
100
120
124
122
156
153
121
152
151
150
158
157
120
155
154
123
130

Fig. 1

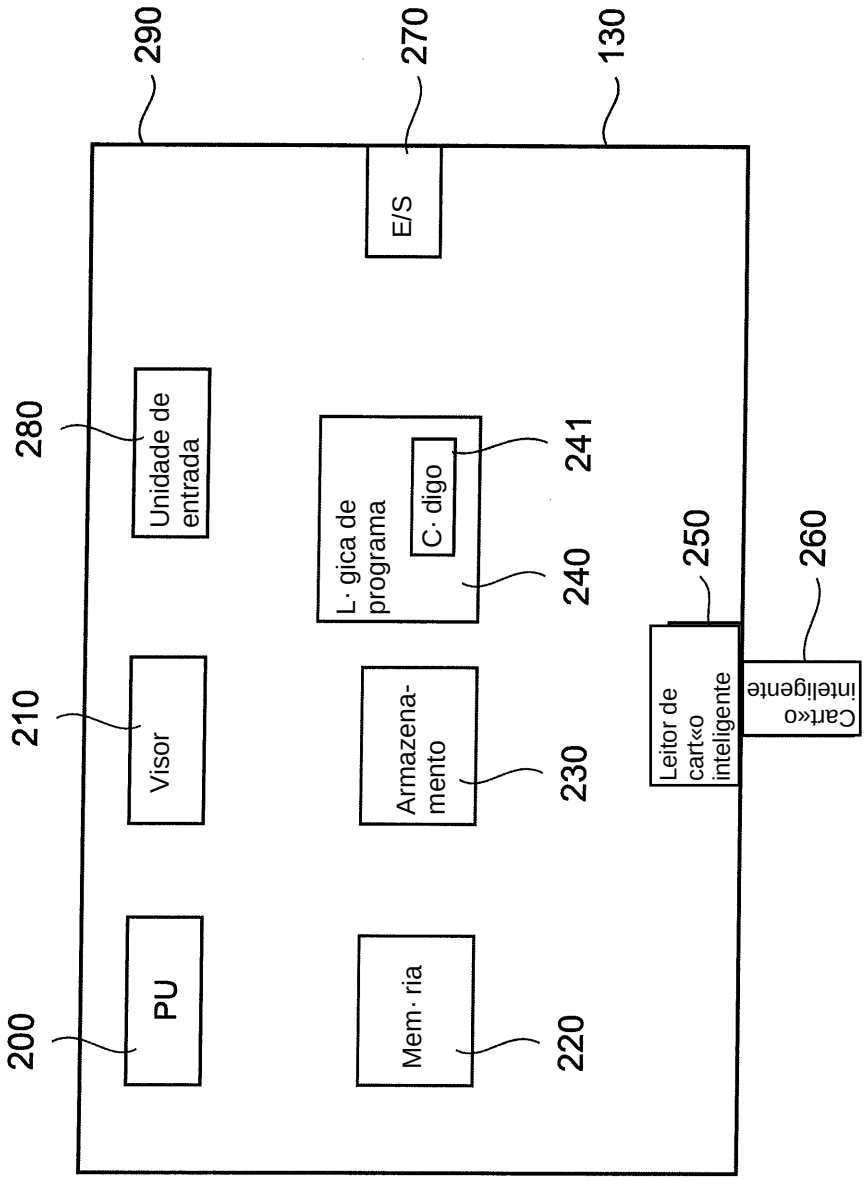

290
270
130
E/S
280
Unidade de entrada
L· gica de programa
C· digo
241
240
250
260
210
Visor
Armazena-mento
230
Leitor de cart«o inteligente
Cart«o inteligente
200
PU
Mem· ria
220

Fig. 2

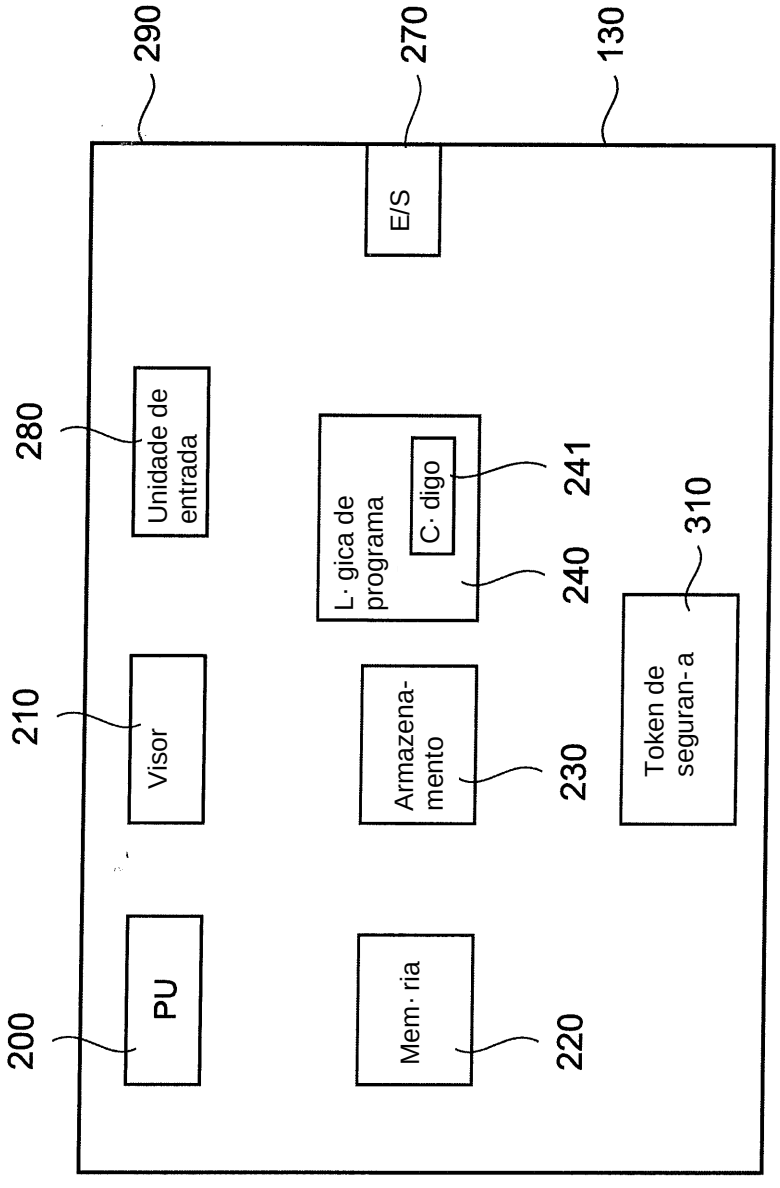

290
270
130
E/S
280
Unidade de entrada
L· gica de programa
C· digo
241
240
310
210
Visor
Armazena-mento
230
Token de seguran-a
200
PU
Mem· ria
220

Fig. 3

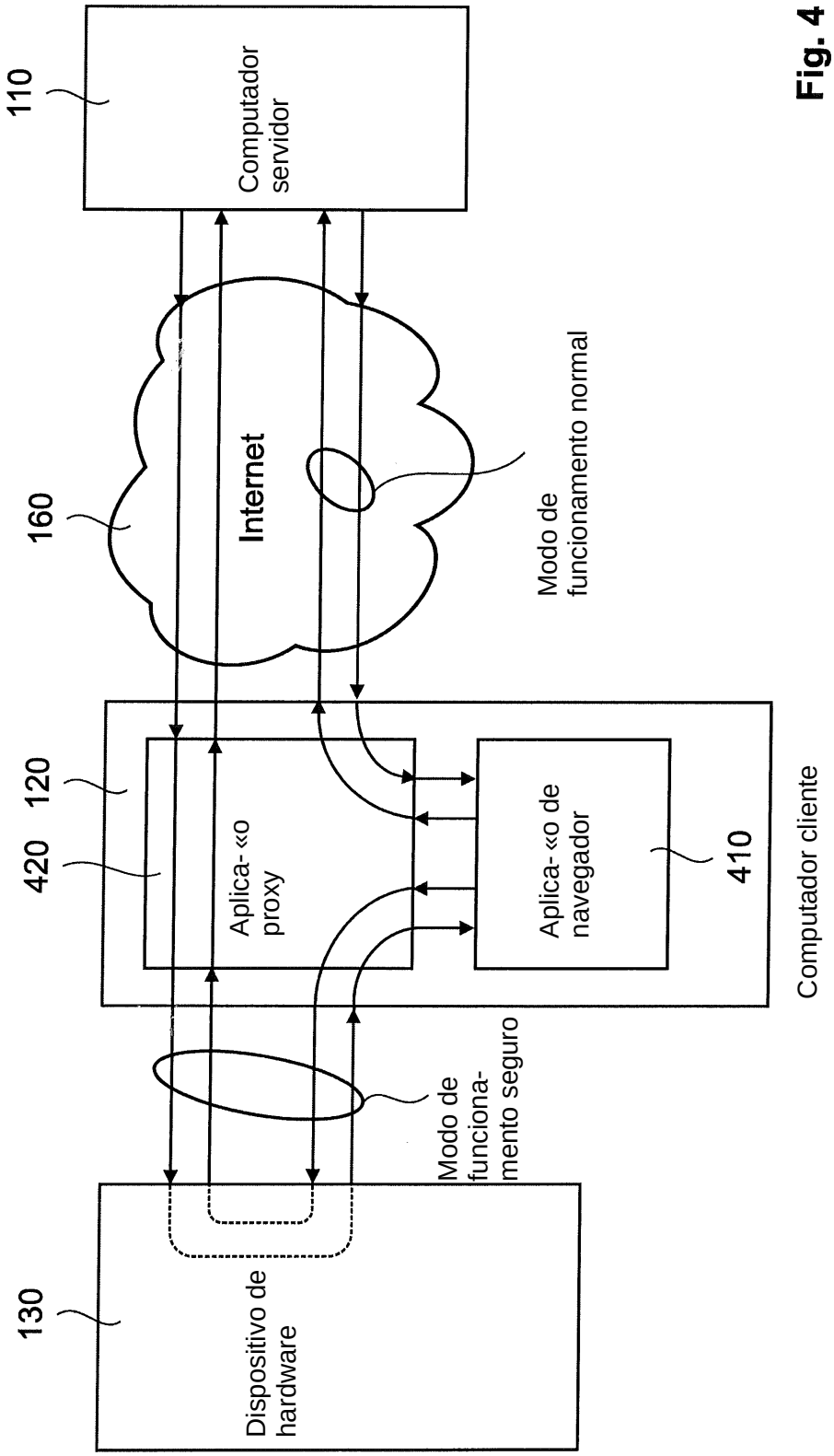

110
Computador servidor
160
Internet
Modo de funcionamento normal
120
420
Aplica-«o proxy
Aplica-«o de navegador
410
Computador cliente
Modo de funciona-mento seguro
130
Dispositivo de hardware

Fig. 4

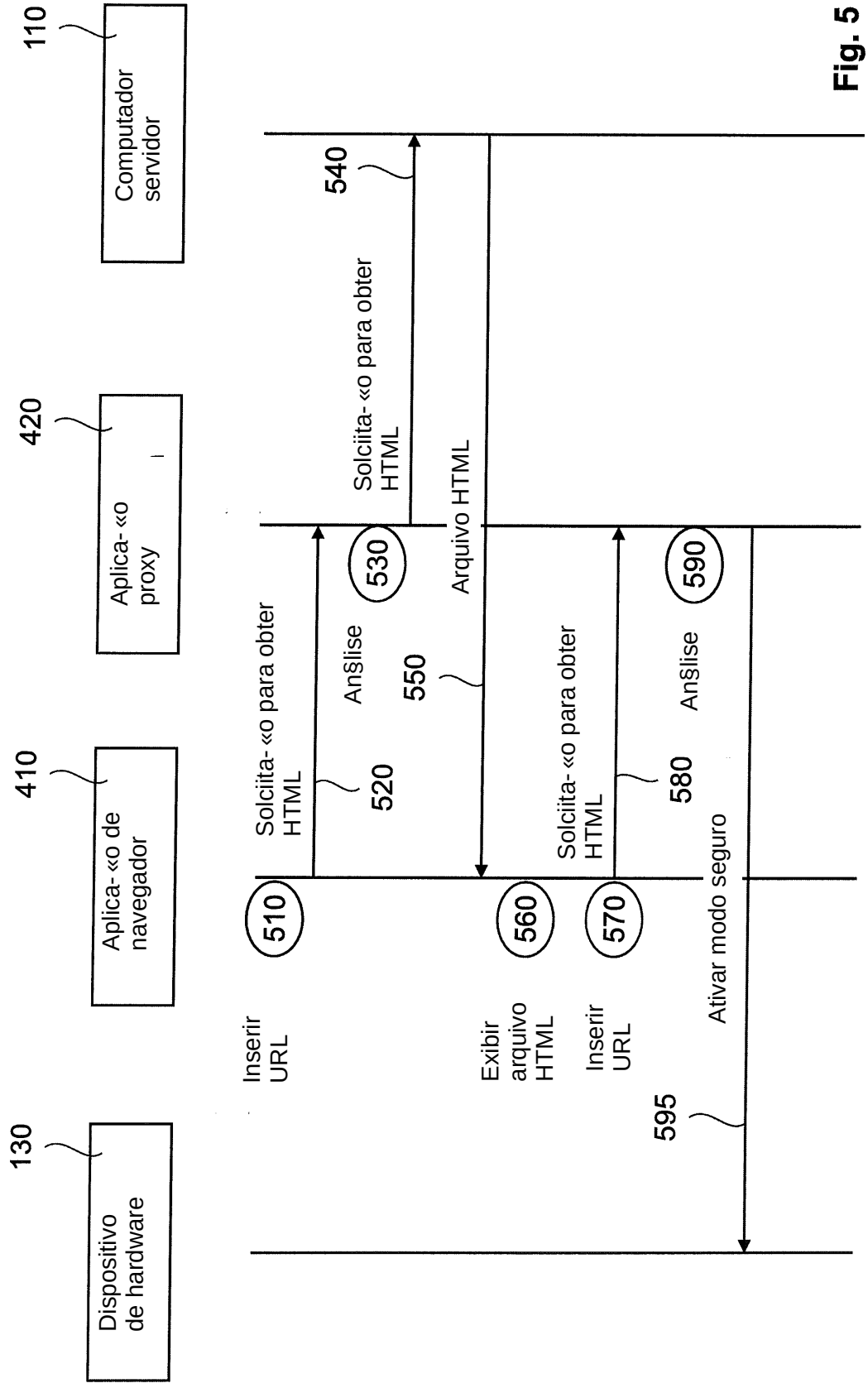
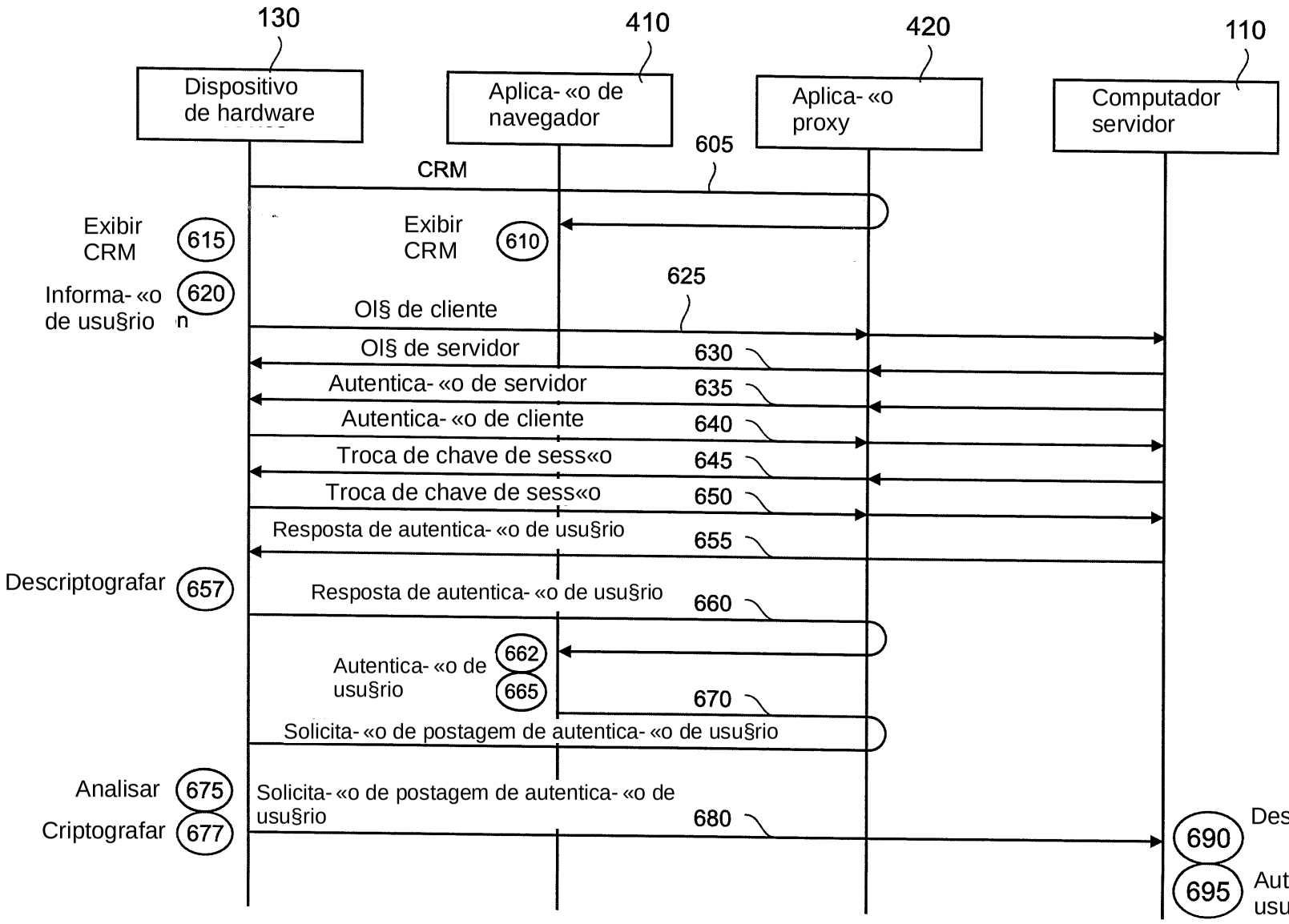

110
Computador servidor
420
Aplica-«o proxy
410
Aplica-«o de navegador
130
Dispositivo de hardware
Inserir URL
510
Solciita-«o para obter HTML
520
An§lise
530
Solciita-«o para obter HTML
540
Arquivo HTML
550
Exibir arquivo HTML
560
Solciita-«o para obter HTML
570
An§lise
580
590
Inserir URL
Ativar modo seguro
595

Fig. 5


130
Dispositivo de hardware
410
Aplica- «o de navegador
420
Aplica- «o proxy
110
Computador servidor
605
CRM
Exibir CRM
615
Exibir CRM
610
Informa- «o de usu§rio
620
625
Ol§ de cliente
Ol§ de servidor
630
Autentica- «o de servidor
635
Autentica- «o de cliente
640
Troca de chave de sess«o
645
Troca de chave de sess«o
650
Resposta de autentica- «o de usu§rio
655
Descriptografar
657
Resposta de autentica- «o de usu§rio
660
662
Autentica- «o de usu§rio
665
670
Solicita- «o de postagem de autentica- «o de usu§rio
Analisar
675
Criptografar
677
Solicita- «o de postagem de autentica- «o de usu§rio
680
Descriptografar
690
695
Autenticar usu§rio

6/8

Fig. 6

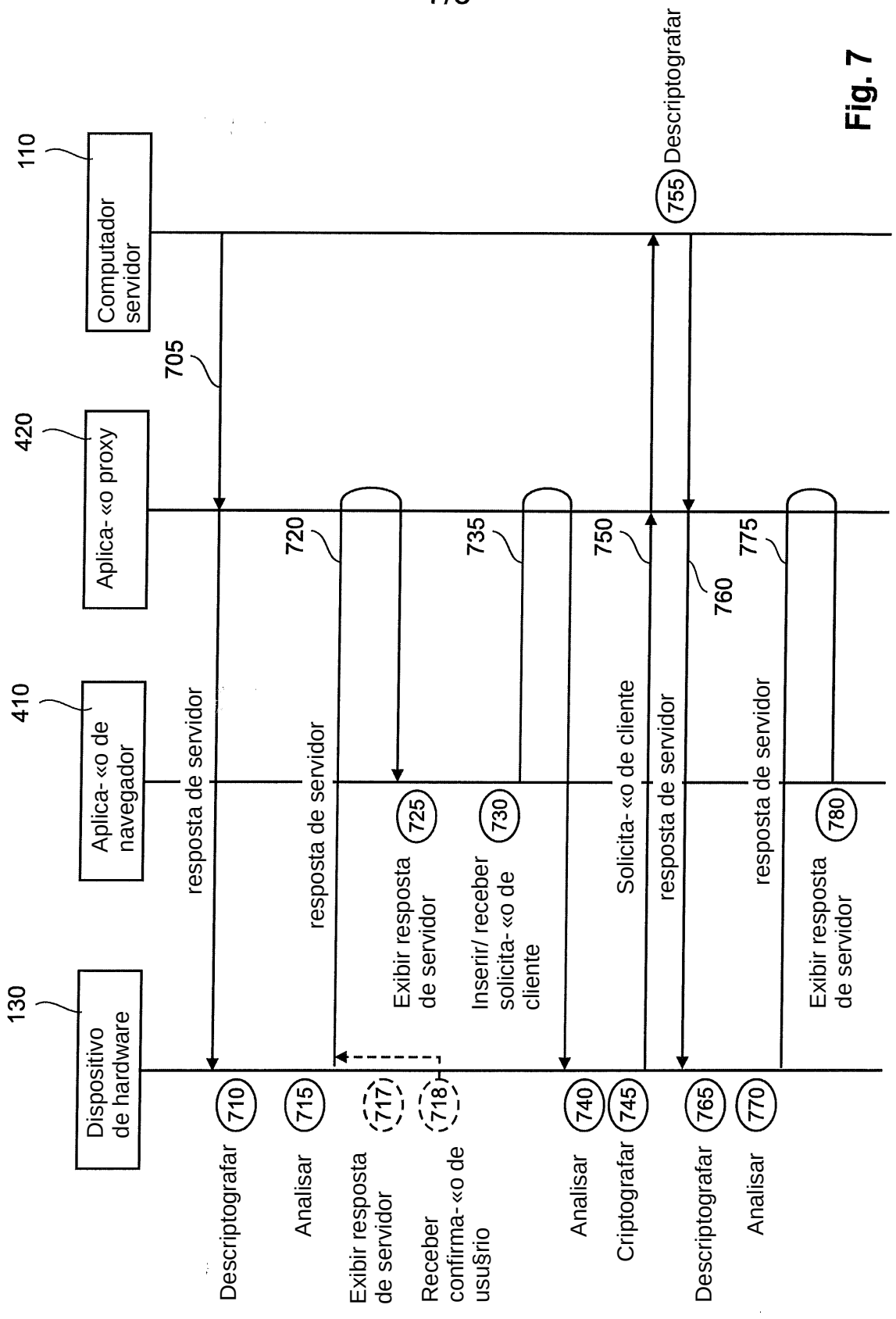
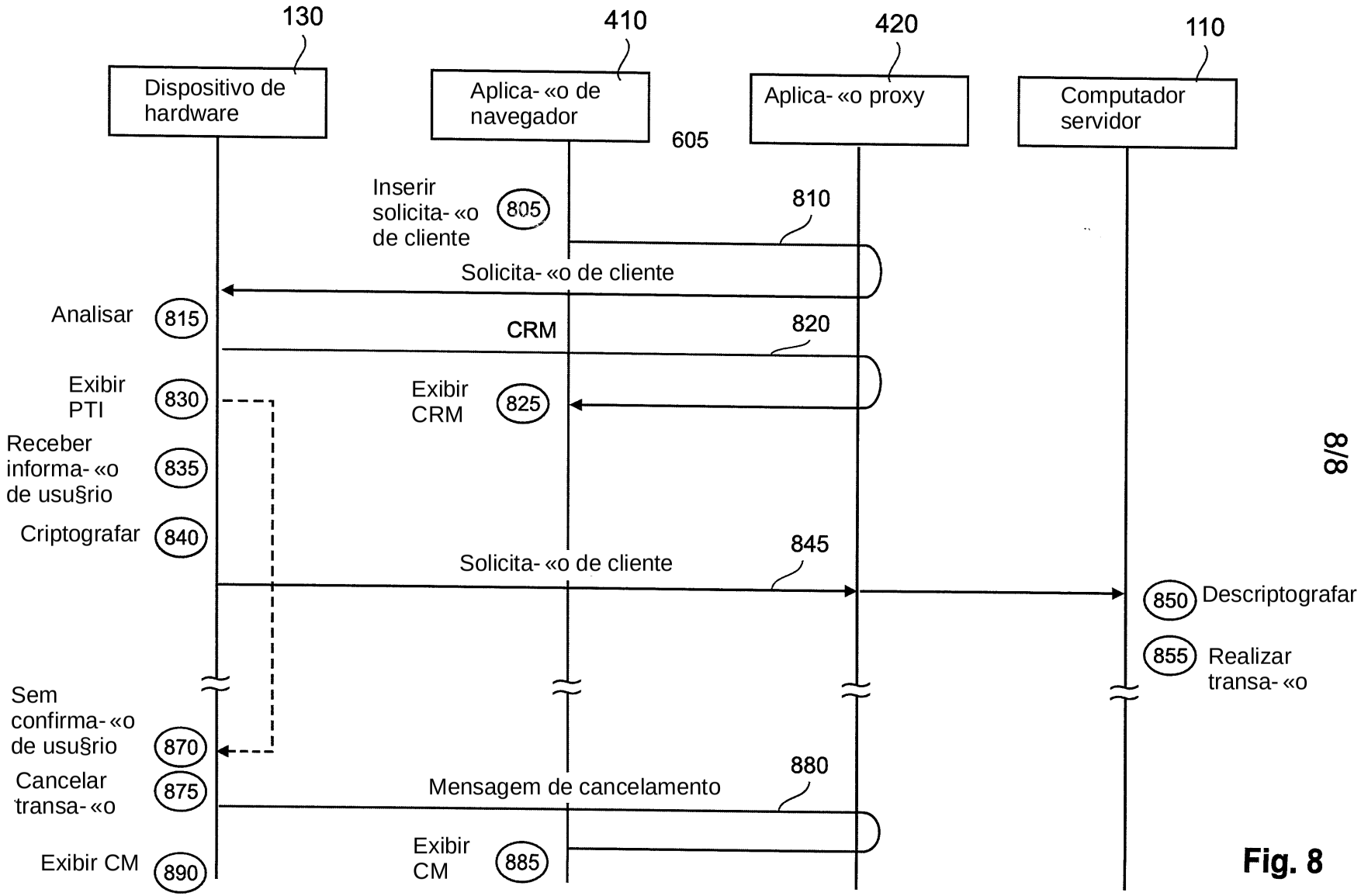

110
Computador servidor
420
Aplica-«o proxy
410
Aplica-«o de navegador
130
Dispositivo de hardware
705
resposta de servidor
720
resposta de servidor
735
750
760
775
755 Descriptografar
725
Exibir resposta de servidor
730
Inserir/ receber solicita-«o de cliente
Solicita-«o de cliente
resposta de servidor
resposta de servidor
780
Exibir resposta de servidor
710 Descriptografar
715 Analisar
717 Exibir resposta de servidor
718 Receber confirma-«o de usu§rio
740 Analisar
745 Criptografar
765 Descriptografar
770 Analisar

Fig. 7


130
Dispositivo de hardware
410
Aplica-«o de navegador
420
Aplica-«o proxy
110
Computador servidor
605
Inserir solicita-«o de cliente
805
810
Solicita-«o de cliente
Analisar
815
CRM
820
Exibir PTI
830
Exibir CRM
825
Receber informa-«o de usu§rio
835
Criptografar
840
Solicita-«o de cliente
845
850
Descriptografar
855
Realizar transa-«o
Sem confirma-«o de usu§rio
870
Cancelar transa-«o
875
Mensagem de cancelamento
880
Exibir CM
890
Exibir CM
885

8/8

Fig. 8