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

(11) PI 0919158-5 B1

BRPI0919158B1

(22) Data do Depósito: 17/09/2009

(45) Data de Concessão: 02/06/2020

(54) Título: DISPOSITIVO DE AUTORIZAÇÃO, APARELHO PARA CONTROLE DE OPERAÇÕES DE UM SERVIDOR, SERVIDOR PARA REALIZAÇÃO DE OPERAÇÕES E SISTEMA DE COMUNICAÇÃO DE DADOS

(51) Int.Cl.: G06F 21/00; G06Q 40/00.

(30) Prioridade Unionista: 17/09/2008 EP 08105363.9.

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

(72) Inventor(es): MICHAEL BAENTSCH; PETER BUHLER; THOMAS EIRICH; RETO HERMANN; FRANK HOERING; THORSTEN KRAMP; MICHAEL P KUYPER; THOMAS D WEIGOLD.

(86) Pedido PCT: PCT IB2009054074 de 17/09/2009

(87) Publicação PCT: WO 2010/032207 de 25/03/2010

(85) Data do Início da Fase Nacional: 17/03/2011

(57) Resumo: DISPOSITIVO DE AUTORIZAÇÃO, APARELHO PARA CONTROLE DE OPERAÇÕES DE UM SERVIDOR, SERVIDOR PARA REALIZAÇÃO DE OPERAÇÕES E SISTEMA DE COMUNICAÇÃO DE DADOS Um dispositivo de autorização (5) é fornecido para autorizar as operações de um servidor remoto (2) pedido dos computadores dos usuários (3) através de uma rede de comunicações de dados (4). O dispositivo (5), uma interface de computador (6) para conectar o dispositivo (5) a um computador do usuário local (3) para comunicação com o servidor remoto (2), e uma interface de usuário (7) para apresentar informações ao usuário. Lógica de controle (11) do dispositivo (5) é adaptada para uso de dados de segurança para estabelecer entre o dispositivo (5) e o servidor (2), através do computador do usuário local (3), uma conexão mutuamente autenticada para comunicações extremidade a extremidade criptografada entre o dispositivo e o servidor. A lógica de controle (11) coleta a partir do servidor (2) através dessa conexão informações indicativas de quaisquer operações solicitadas por computadores de usuários através de outras conexões para o servidor (2) e exigindo autorização por um usuário do dispositivo (5). Esta informação é apresentada ao usuário através da interface do usuário (7) para pedir autorização do usuário. Operações do servidor são controladas de acordo com dados de regra (18) que definem as operações que requerem autorização por um ou mais usuários (...).

"DISPOSITIVO DE AUTORIZAÇÃO, APARELHO PARA CONTROLE DE OPERAÇÕES DE UM SERVIDOR, SERVIDOR PARA REALIZAÇÃO DE OPERAÇÕES E SISTEMA DE COMUNICAÇÃO DE DADOS"

[0001] A presente invenção se refere, de modo geral, à autorização de operações de servidor solicitadas a partir de computadores de usuários através de redes de comunicação de dados. São fornecidos dispositivos, sistemas e programas de computador para autorização de operações de servidor remoto e controlar a execução de operações por servidores na dependência de tal autorização.

[0002] Há numerosas situações nas quais os usuários de computadores se comunicam com um servidor remoto através de uma rede de comunicações de dados para solicitar a execução de alguma operação pelo servidor. Tal servidor é, tipicamente, operado pelo provedor de um serviço para acesso on-line por usuários remotos. O termo "servidor" é usado aqui no sentido mais geral, no entanto, e inclui qualquer computador ou sistema que fornece algum serviço ou funcionalidade para os usuários que se conectam. Uma operação executada por um servidor a pedido de um usuário poderia ser simplesmente conceder acesso do usuário a alguns recursos, por exemplo, um banco de dados ou web site restrito, ou poderia ser implementação de alguma transação, tal como uma transação bancária, instruída pelo usuário. Em qualquer caso, a natureza da infraestrutura de comunicação é tal que a segurança é, muitas vezes, uma das principais preocupações, em particular assegurar que as operações do servidor sejam executadas apenas para usuários realmente autorizados. No caso de comércio eletrônico realizado

através da Internet, por exemplo, a fraude on-line é uma ameaça em constante crescimento. A prevalência de ataques avançados, tal como o infame "*man-in-the-middle*" (MITM), e vários tipos de softwares maliciosos, tais como vírus ou Trojans, estão aumentando, enquanto que as contramedidas, tais como software antivírus e firewalls, parecem estar sempre um passo atrás dos atacantes. Consequentemente, os computadores dos usuários, tais como computadores pessoais (PCs), bem como a própria Internet, devem ser considerados inerentemente não confiáveis, apresentando riscos significativos de segurança para transações eletrônicas. A título de exemplo, se um usuário se conecta a partir de seu PC a um portal de um provedor de serviços online para iniciar uma transação, ele não pode ter certeza de que a transação não é silenciosamente manipulada por alguns softwares maliciosos ou MITM. Uma dificuldade similar enfrenta o provedor de serviços pelo fato de que ele não pode ter certeza de que está se comunicando com um usuário autorizado genuíno.

[0003] Vários sistemas foram propostos para resolver alguns dos problemas de segurança nas situações acima. Por exemplo, a Patente dos Estados Unidos N° 6.895.502 descreve um dispositivo de segurança o qual pode ser conectado a um PC do usuário e incorpora um leitor para *smart card*. Quando o usuário solicita um recurso a partir de um servidor remoto através de seu PC, o servidor responde ao recuperar a chave pública do usuário e retransmitir um *blob* de dados criptografados que inclui informações sobre a transação junto com um desafio. O

recurso solicitado a partir do PC do usuário é exibido no dispositivo de segurança e o usuário pode confirmar se ele solicitou ou não este recurso ao entrar no dispositivo de segurança, o qual é reenviado para o servidor. Este dispositivo permite que o usuário de um determinado PC forneça uma confirmação simultânea de solicitações de recursos emitidas uma de cada vez a partir do PC. No entanto, o sistema é vulnerável a ataques de "falso-desafio". Ou seja, qualquer pessoa maliciosa poderia gerar um desafio criptografado com a chave pública do usuário e enviá-lo para o PC do usuário, por exemplo, para confundir o usuário quando de resposta. Além disso, alguém pode decifrar a mensagem de resposta do usuário a um desafio com a chave pública do usuário. Este sistema, portanto, é de utilidade limitada e levanta questões de segurança e privacidade em si.

[0004] O Pedido de Patente Europeia Copendente N° 07.022.419,1, depositado em 19 de novembro de 2007, descreve outro dispositivo para conexão ao computador de um usuário. Este dispositivo também é descrito em "*The Zurich Trusted Information Channel - An Efficient Defence Against Man-in-the-Middle and Malicious Software Attacks*", Thomas Weigold *et al*. em P. Lipp, A.-R. Sadeghi e K.-M. Koch (Eds.): TRUST 2008, LNCS 4968, páginas 75-91, Springer-Verlag Berlin Heidelberg 2008. Este dispositivo estabelece uma conexão "*end-to-end*" mutuamente autenticada segura com o servidor quando solicitado por um aplicativo de *proxy* no PC do usuário o qual é contatado pelo navegador para se conectar a uma URL bancária específica (localizador de

recursos universal). A sessão do navegador subsequente é, então, conduzida através da conexão segura e monitorada pelo dispositivo de segurança. Se o dispositivo detecta informações de segurança sensíveis, tais como detalhes de transações bancárias, estas são exibidas no dispositivo e o usuário pode pressionar um botão para indicar sua confirmação. Apenas se o dispositivo de segurança recebe esta confirmação ele manterá a conexão e encaminhará a solicitação de transação para o servidor. Este dispositivo, mais uma vez, permite que o usuário de um determinado PC forneça confirmação simultânea de solicitações emitidas uma de cada vez a partir deste PC embora, neste caso, toda a sessão do servidor seja conduzida através da conexão segura sob o controle do dispositivo de segurança, o qual determina quando a autorização de usuário é necessária.

[0005] Um aspecto da presente invenção fornece um dispositivo de autorização para autorizar operações de um servidor remoto solicitadas a partir de computadores de usuários através de uma rede de comunicações de dados. O dispositivo compreende:

uma interface de computador para conexão do dispositivo a um computador de usuário local para comunicação com o servidor remoto através de uma rede de comunicação de dados,

uma interface de usuário para apresentação de informações a um usuário e

lógica de controle adaptada para:

usar dados de segurança acessíveis à lógica de controle em uso para estabelecer entre o dispositivo e o

servidor, através do computador de usuário local, uma conexão mutuamente autenticada para comunicações criptografadas "*end-to-end*" entre o dispositivo e o servidor;

coletar, a partir do servidor por meio da dita conexão, informação indicativa de qualquer operação solicitada através de uma conexão diferente ao servidor e que requer autorização por um usuário do dispositivo; e

apresentar a dita informação a um usuário através da dita interface de usuário para solicitar autorização para a dita operação.

[0006] Assim, um dispositivo de autorização que incorpora a presente invenção pode ser conectado a um computador de usuário através de sua interface de computador e estabelecer uma conexão "*end-to-end*" mutuamente autenticada segura com o servidor. Além disso, a lógica de controle do dispositivo coleta, a partir do servidor por meio desta conexão, informação indicativa de qualquer operação solicitada através de uma conexão diferente ao servidor que requer autorização por um usuário do dispositivo. Assim, a aquisição de informação sobre solicitações de operação que requerem autorização pelo usuário é iniciada pela ação da lógica de controle e as solicitações de operação sobre as quais a informação é recebida são aquelas enviadas através de uma ou mais conexões ao servidor diferentes. O dispositivo pode, assim, coletar detalhes sobre qualquer número de solicitações de operação enviadas para o servidor a qualquer momento, antes ou após o estabelecimento da conexão segura, e enviadas por

qualquer usuário de qualquer computador de usuário, seja aquele ao qual o dispositivo está conectado e/ou um ou mais de outros computadores que, em algum momento, estabeleceram uma conexão de rede com o servidor. Desta forma, os dispositivos de autorização que incorporam a presente invenção constituem a base para autorização segura de operações de servidor solicitadas a partir de computadores de usuários não confiáveis em um ambiente de computação móvel, bem como para autorização de solicitações por múltiplas partes em tais ambientes. Em particular, as operações de servidor podem ser dependentes de autorização por mais de um usuário de autorização, as autorizações necessárias sendo obtidas de forma assíncrona à medida que diferentes usuários se conectam ao servidor através de dispositivos de autorização e coletam detalhes de solicitações de operações pendentes. Além disso, qualquer outra sessão, por exemplo, uma sessão atual do navegador, entre o computador do usuário e o servidor pode permanecer inalterada pelo procedimento de autorização quando de conexão segura e pode ser inteiramente conduzida como normal. Os dispositivos que incorporam a invenção, assim, oferecem sistemas flexíveis, eficientes e de fácil utilização para autorização de múltiplas partes segura de operações de servidor em relação aos sistemas inseguros em um ambiente de computação móvel.

[0007] Para coletar a informação sobre solicitação de operação a partir do servidor, a lógica de controle do dispositivo emitirá algum tipo de solicitação para o servidor para solicitar o retorno da informação embora, em

geral, esta solicitação possa ser explícita ou implícita. Por exemplo, a solicitação poderia estar implícita no processo de estabelecimento da conexão segura, o servidor respondendo ao estabelecimento bem-sucedido da conexão ao enviar qualquer informação sobre solicitação de operação apropriada a um usuário de autorização associado aos dados de segurança usados para estabelecer a conexão. Alternativamente, a lógica de controle poderia enviar uma solicitação explícita para obter informação sobre as solicitações de operação que requerem autorização pelo usuário do dispositivo. Assim, a lógica de controle pode ser adaptada para enviar a solicitação de informação através de uma conexão segura, por exemplo, em resposta ao estabelecimento da conexão e, de preferência, solicita a informação a partir do servidor periodicamente enquanto a conexão segura persistir. O ponto chave aqui é que a aquisição de informação sobre solicitação de operação a partir do servidor é iniciada pelo dispositivo de autorização, permitindo que o dispositivo obtenha a informação quando e onde exista uma conexão segura com o servidor em um ambiente móvel.

[0008] A lógica de controle, de preferência, inicia o estabelecimento da conexão segura com o servidor em resposta à conexão do dispositivo de autorização ao computador de usuário local. Este processo pode ou não requerer de alguma entrada do usuário, onde a interface de usuário inclui um mecanismo de entrada, por exemplo, para digitar um número de identificação pessoal (*Personal Identification Number* - PIN) de usuário. Em qualquer caso,

o estabelecimento da conexão segura é dependente da lógica de controle ter acesso a alguma forma de dados de segurança que possam ser usados para o processo de autenticação mútua. Os dados de segurança compreendem, tipicamente, uma chave secreta fornecida pelo provedor de serviços que executa o servidor, porém, em geral, poderia compreender quaisquer dados, tais como senhas de uso único ou outros dados sigilosos mutuamente conhecidos para protocolos de resposta de desafio que permitem autenticação mútua do dispositivo de autorização e do servidor para estabelecimento da conexão segura. Os dados de segurança poderiam ser armazenados na memória do dispositivo de autorização, por exemplo, em um chip inviolável incorporado no dispositivo. Alternativamente, os dados de segurança poderiam ser armazenados em um dispositivo de segurança separado com o qual o dispositivo de autorização possa interagir para permitir acesso da lógica de controle aos dados de segurança. Um fator de forma preferido para o dispositivo de segurança aqui é um *smart card*.

[0009] O dispositivo de autorização em si pode assumir uma variedade de formas. Por exemplo, onde o dispositivo está adaptado para interagir com um dispositivo de segurança, tal como um *smart card*, transportado pelos usuários de autorização, então, o dispositivo é, convenientemente, um dispositivo desktop portátil pequeno que incorpora o leitor de cartões ou outra interface de dispositivo de segurança. Tal dispositivo poderia ser dedicado exclusivamente à finalidade de autorização ou pode ser integrado com algum outro dispositivo que forneça

funcionalidade adicional, por exemplo, um *mouse*. Onde os dados de segurança são armazenados no dispositivo de autorização em si, o dispositivo é, de forma ideal, um dispositivo portátil pequeno o qual possa ser facilmente transportado por um usuário, novamente dedicado exclusivamente à finalidade ou tendo uma funcionalidade combinada. Como exemplos aqui, o dispositivo pode ser incorporado em um cartão de memória ou *music player* pessoal, tal como um MP3 *player*. Em qualquer caso, para evitar a necessidade de incorporar mecanismos de proteção para evitar interferência por um software malicioso, de preferência, o dispositivo não incorpora a funcionalidade de computação para uso geral. Isto é, o dispositivo é, de preferência, configurado de modo que um código arbitrário não possa ser carregado no processador do dispositivo.

[0010] A interface de usuário compreende, de forma ideal, um monitor para exibir a informação de solicitação de operação, com ou sem processamento interveniente no dispositivo de autorização, ao usuário. No entanto, podem ser consideradas alternativas, conforme discutido abaixo. Em concretizações preferidas, a interface de usuário também inclui um mecanismo de entrada para introdução de autorização de usuário no dispositivo, a lógica de controle sendo adaptada para transmitir a autorização de usuário para o servidor através da conexão mutuamente autenticada. Mais uma vez, no entanto, podem ser consideradas alternativas, conforme descrito abaixo. Sempre que a interface de usuário inclui um mecanismo de entrada, este permite, de forma ideal, a introdução de alguma informação

de segurança do usuário, por exemplo, um PIN de usuário, para permitir que um usuário autorizado "desbloqueie" o dispositivo para o procedimento de autorização.

[0011] Um segundo aspecto da invenção fornece um dispositivo para controlar as operações de um servidor solicitadas a partir de computadores de usuário através de uma rede de comunicações de dados. O dispositivo compreende uma memória para armazenamento de dados da regra que definem operações que requerem autorização por um ou mais usuários de autorização e uma lógica de controle adaptada para:

em resposta a uma solicitação de um computador de usuário, executar a dita operação, determinar, a partir dos dados de regra, se a autorização por pelo menos um usuário de autorização é necessária para esta operação e, em caso afirmativo, postergar esta operação;

se comunicar com um dispositivo de autorização de acordo com o primeiro aspecto da invenção para estabelecer a dita conexão mutuamente autenticada;

fornecer, ao dispositivo de autorização através da dita conexão, informação indicativa de quaisquer operações postergadas solicitadas a partir de computadores de usuários e que requerem autorização por um usuário do dispositivo de autorização e receber a autorização a partir do usuário; e

iniciar a execução de uma operação postergada em resposta ao recebimento de autorização a partir de cada usuário de autorização dos quais é requerida autorização para esta operação.

[0012] Em concretizações deste aspecto da invenção, a lógica de controle pode enviar a informação de solicitação de autorização em resposta a uma solicitação do dispositivo de autorização através da dita conexão autenticada mutuamente. Tal solicitação poderia ser explícita ou implícita, conforme discutido anteriormente, e poderia ser tratada pelo dispositivo como uma solicitação autônoma pela qual quaisquer novas solicitações de operação recebidas durante um intervalo de tempo predeterminado, e que requerem autorização pelo usuário do dispositivo, serão enviadas ao dispositivo de autorização através da conexão segura.

[0013] Um terceiro aspecto da invenção fornece um servidor para execução de operações solicitadas a partir de computadores de usuários através de uma rede de comunicações de dados. O servidor compreende:

um circuito de comunicações para comunicação com computadores de usuários através da rede de comunicações de dados;

uma lógica de servidor para execução de tais operações em resposta à solicitação a partir de computadores de usuários; e

um dispositivo de acordo com o segundo aspecto da invenção para controlar a execução das ditas operações pela lógica de servidor.

[0014] Um quarto aspecto da invenção fornece um sistema de comunicações de dados que compreende:

um servidor de acordo com o terceiro aspecto da invenção;

pelo menos um computador de usuário para se comunicar com o servidor através de uma rede de comunicação de dados; e

pelo menos um dispositivo de autorização de acordo com o primeiro aspecto da invenção para conexão ao computador de usuário através da dita interface de computador do dispositivo;

em que o computador de usuário está adaptado para retransmitir comunicações entre o dispositivo de autorização e o servidor por meio da dita conexão mutuamente autenticada.

[0015] Um quinto aspecto da invenção fornece um programa de computador que compreende um meio de código de programa para fazer com que um processador de um dispositivo de autorização adaptado para conexão a um computador de usuário para comunicação com um servidor remoto através de uma rede de comunicações de dados e que tem uma interface de usuário para apresentar informação a um usuário do dispositivo:

use os dados de segurança associados ao dispositivo de autorização para estabelecer, através do computador de usuário local, uma conexão mutuamente autenticada para comunicações "*end-to-end*" criptografadas com o servidor;

colete, a partir do servidor por meio da dita conexão, informação indicativa de qualquer operação solicitada através de uma conexão diferente para o servidor e que requer autorização por um usuário do dispositivo; e

apresente a dita informação a um usuário através da dita interface de usuário para solicitar autorização para a dita operação.

[0016] Um sexto aspecto da invenção fornece um programa de computador que compreende um meio de código de programa para fazer com que um servidor adaptado para execução de operações solicitadas a partir de computadores de usuários por meio de uma rede de comunicações de dados e que tem uma memória para armazenamento de dados de regras que definem operações que requerem autorização por um ou mais usuários de autorização:

determine, a partir dos dados de regras, em resposta a uma solicitação de um computador de usuário para executar a dita operação, se autorização por pelo menos um usuário de autorização é requerida para esta operação e, em caso afirmativo, postergar esta operação;

se comunique com um dispositivo de autorização de acordo com o primeiro aspecto da invenção para estabelecer a dita conexão mutuamente autenticada;

forneça, ao dispositivo de autorização por meio da dita conexão, informação indicativa de qualquer operação postergada que requer autorização por um usuário do dispositivo de autorização e receba a autorização do usuário; e

execute uma operação postergada em resposta ao recebimento da autorização de cada usuário de autorização do qual é requerida autorização para esta operação.

[0017] Um programa de computador que incorpora a invenção pode constituir um programa independente ou pode

ser um elemento de um programa maior e pode ser fornecido, por exemplo, incorporado em um meio legível em computador, tal como um disco ou um meio de transmissão eletrônica para carregamento em um computador. O meio de código de programa do programa de computador pode compreender qualquer expressão, em qualquer linguagem, código ou notação, de um conjunto de instruções destinadas a fazer com que um computador execute o método em questão, quer diretamente ou após um ou ambos de (a) conversão para outra linguagem, código ou notação e (b) reprodução em uma forma material diferente.

[0018] Em geral, onde são descritas aqui características com referência a uma concretização de um aspecto da invenção, as características correspondentes podem ser fornecidas em concretizações de outro aspecto da invenção.

[0019] As concretizações preferidas da invenção serão agora descritas, a título de exemplo, com referência aos desenhos anexos, nos quais:

[0020] A figura 1 é uma representação esquemática de um sistema de comunicação de dados que incorpora a invenção;

[0021] A figura 2 ilustra em maiores detalhes um dispositivo de autenticação, o PC do usuário e o servidor do sistema da figura 1;

[0022] A figura 3 indica as etapas executadas pelo servidor no momento de recebimento de uma solicitação de operação a partir de um PC do usuário;

[0023] A figura 4 indica as principais etapas na operação do dispositivo de autenticação da figura 2; e

[0024] A figura 5 indica a operação do servidor quando de recebimento de uma solicitação de informação sobre transação proveniente do dispositivo de autenticação da figura 2.

[0025] A figura 1 mostra um sistema de comunicações de dados que incorpora a invenção para implementação de um sistema de autorização de transação com múltiplas partes seguro em um cenário de computação móvel. O sistema 1 inclui um servidor 2, o qual pode se comunicar com vários computadores de usuários 3 através de uma ou mais redes de comunicações de dados representadas na figura geralmente pela rede 4. Assumimos aqui que o servidor 2 é implementado por um computador de uso geral configurado para executar as funções descritas embora, em geral, a funcionalidade do servidor 2 possa ser distribuída através de uma pluralidade de máquinas físicas de um sistema de servidor. Os computadores de usuários 3 poderiam ser implementados por uma variedade de dispositivos de computação, tais como PCs, PDAs (*Personal Digital Assistants*), telefones móveis, etc., os quais são capazes de comunicações de dados com o servidor 2 através da rede 4. Para fins deste exemplo, presume-se que o servidor 2 permite acesso a um serviço bancário on-line ao qual os usuários que operam os computadores 3 podem se conectar periodicamente para realizar transações bancárias. A implementação de transações pelo servidor 2 está sujeita a um processo de autorização de múltiplas partes. Em particular, pelo menos

algumas operações as quais poderiam ser solicitadas a partir dos computadores de usuários 3 devem ser autorizadas por um ou mais usuários de autorização antes que elas sejam implementadas pelo servidor 2. Para autorizar transações, um usuário de autorização usa um dispositivo de autorização transação (*Transaction Authorization Device* - TAD) móvel dedicado o qual pode ser conectado a um computador de usuário 3, três de tais dispositivos sendo indicados na figura 1.

[0026] A figura 2 é diagrama de blocos esquemático de um TAD 5, PC de usuário 3 e servidor 2 que mostra os principais elementos envolvidos no sistema de autorização. O TAD 5 do presente exemplo é um dispositivo desktop pequeno que tem uma interface de computador, aqui uma interface de USB 6, para conectar o dispositivo ao computador do usuário 3 e uma interface de usuário que compreende um monitor 7 e um teclado 8 para entrada do usuário. O TAD 5 também tem uma interface de dispositivo de segurança na forma de leitor de cartão 9 para interagir com um *smart card* 10. A lógica de controle 11 controla a operação do dispositivo em geral e implementa as várias etapas do processo de autorização descrito abaixo. O servidor 2 inclui o circuito de comunicações 13 habitual para interagir com rede(s) de comunicações de dados 4 e a lógica do servidor 14 para executar as várias funções do serviço bancário on-line. Além disso, o servidor 2 inclui um dispositivo de autorização que compreende a logica de controle de autorização 15 e a memória 16 que contém vários dados usados pela lógica de autorização 15 em operação.

Estes incluem um registro de transação 17 postergado, o efeito dos quais é descrito abaixo, e um banco de dados de regras 18. O banco de dados de regras 18 define as transações as quais requerem autorização por um ou mais usuários de autorização. Em particular, os dados de regras armazenados no banco de dados 18 indicam as transações e, para cada transação, a identidade de cada um dos usuários de autorização cuja autorização é requerida para esta transação. A estrutura de regras no banco de dados 18 pode variar de um simples conjunto de regras a uma complexa estrutura de dados, dependendo da aplicação em particular. Em geral, a lógica de controle 11 no TAD 5 e a lógica 14, 15 no servidor 2 poderiam ser implementadas em hardware, software ou uma combinação dos mesmos, embora seja assumido aqui que esta lógica é implementada por software executado no computador do servidor 2 ou um processador do TAD 5, conforme apropriado. O software adequado será evidente para aqueles versados na técnica a partir da descrição aqui. A lógica de controle que implementa o processador 11 do TAD 5 é concebida de modo que um código arbitrário adicional não pode ser carregado neste processador.

[0027] O servidor 2 é mostrado tendo uma primeira conexão ao PC do usuário 3, indicado pela linha tracejada na figura, através da rede 4. Por exemplo, o PC do usuário tem, tipicamente, uma conexão de internet com o servidor 2 através de um navegador da web executado no PC 3. O PC do usuário 3 também é mostrado como executando um aplicativo de *proxy* 19 o qual serve ao TAD 5, conforme discutido adicionalmente abaixo. Embora, em geral, o *proxy* 19 possa

ser pré-instalado no PC 3, nesta concretização preferida, o *proxy* pode ser carregado a partir do TAD, por exemplo, ao registrar o próprio TAD como um dispositivo de armazenamento em massa USB.

[0028] O *smart card* 10 é emitido para um usuário de autorização fornecido pelo servidor executado pelo banco 2. O cartão 10 contém os dados de segurança para uso no processo de autenticação a ser realizado entre o TAD 5 e o servidor 2. Neste exemplo, os dados de segurança dos dados são uma chave criptográfica secreta, mas o *smart card* também é, convenientemente, personalizado com informações de conta de usuário e certificados, por exemplo, URL do provedor de serviços, certificados TLS/SSL (*Transport Layer Security/Secure Sockets Layer*) confiáveis, nome de usuário, senha, etc., e as chaves criptográficas possivelmente adicionais para uso em comunicações com o servidor 2.

[0029] Em operação do sistema 1, os clientes do banco podem se conectar ao servidor 2 a partir de qualquer computador 3 (não confiável) para entrar no portal banco on-line e solicitar ao servidor para executar operações, tais como transferências de fundos ou outras transações bancárias. A operação do servidor 2 em resposta a tal solicitação de transação é indicada no fluxograma da figura 3. Este processo é desencadeado ao receber a solicitação de transação, conforme indicado na etapa 20. Todas as solicitações de transação recebidas pelo servidor 2 são passadas através da lógica do servidor 14 para a lógica de autorização 15. Na etapa 21, a lógica de autorização acessa o banco de dados de regras 18 para verificar se é

necessária uma autorização para esta transação. Caso negativo, conforme indicado por um "Não" (N) na etapa de decisão 22, a solicitação de transação é retornada para a lógica do servidor 14, a qual simplesmente executa a transação indicada na etapa 23 e o processo é concluído. No entanto, caso autorização seja requerida para a transação, conforme indicado por um "Sim" (Y) na etapa de decisão 22, então, na etapa 24, a lógica de autorização 15 faz uma entrada no log de transações postergadas 17. Esta entrada registra a transação em detalhes, bem como a identidade de cada usuário de autorização cuja autorização é requerida para a transação. A transação é, assim, postergada, pendente de recebimento da(s) autorização(ões) requerida(s) e o processo termina.

[0030] Múltiplos usuários podem instruir transações em vários momentos a partir de diferentes computadores de usuário 3 não confiáveis. Todas as solicitações de transação são tratadas pelo servidor 2 conforme já descrito pelo que, a qualquer momento, o log de transações postergadas poderia conter detalhes de várias transações que aguardam autorização. Cada usuário de autorização identificado no banco de dados de regras 18 porta um *smart card* 10, conforme descrito acima. Usuários de autorização também podem portar um TAD 5 e/ou os TADs 5 podem ser fornecidos para uso com os computadores 3 em algumas localidades. Em qualquer caso, quando um usuário de autorização com um TAD 5 tem acesso a um computador conectado à rede 3, ele pode realizar um procedimento de autorização da seguinte forma. O usuário insere o *smart*

card 10 no TAD 5 e conecta o TAD ao PC do usuário 3 através da interface de USB 6. A operação subsequente do TAD 5 é controlada pela lógica de controle 11 e indicada no fluxograma da figura 4. Em resposta à conexão do TAD 5 ao PC 3, conforme representado pela etapa 30, a lógica de controle 11 inicia o processo de conexão com o servidor 2. Primeiro, na etapa 31, a lógica de controle solicita, através de uma mensagem no monitor 7, que o usuário introduza seu PIN no teclado 8 e o número digitado é verificado em relação àquele armazenado no *smart card* 10. O dispositivo pode permitir ao usuário uma série de oportunidades para introduzir o PIN correto, mas se nenhum PIN válido é inserido (N na decisão 32), o processo será encerrado. Assumindo, contudo, que o PIN é válido (Y na decisão 32), então, na etapa 33, a lógica de controle inicia o aplicativo de *proxy* 19 no PC 3. Em seguida, conforme indicado na etapa 34, a lógica de controle estabelece, com o auxílio do *proxy* 19, uma conexão mutuamente autenticada para comunicações "*end-to-end*" criptografadas entre o TAD 5 e o servidor 2. Esta conexão é indicada pela linha sólida na figura 2. Para estabelecer esta conexão, a lógica de controle se comunica com o *smart card* 10 através do leitor de cartão 9 para acessar os dados de segurança armazenados no cartão 10. A chave secreta pré-acordada é usada para codificação/decodificação de mensagens, permitindo autenticação mútua do TAD e do servidor, e uma conexão SSL/TLS é estabelecida com o servidor 2 ao implementar a configuração de protocolo de uma maneira conhecida. A conexão TLS/SSL é "*end-to-end*"

entre o TAD 5 e o servidor 2 confiável do provedor de serviços do TAD é configurada (através dos dados seguros no *smart card* 10), enquanto que o *proxy* retransmite às cegas os pacotes de rede entre os dois. Consequentemente, o *proxy* 19, bem como o PC 3, podem não ser confiáveis à medida que todos os dados que passam através dos mesmos são criptografados.

[0031] Após estabelecer a conexão segura, na etapa 35 da figura 4, a lógica de controle 11 envia uma solicitação ao servidor 2 para obter informações sobre quaisquer transações as quais tenham sido postergadas pendentes de autorização pelo usuário do TAD. Esta solicitação pode incluir dados de ID de usuário recuperados do cartão 10, se já não fornecidas quando de estabelecimento da conexão segura. Se o servidor responde que não há transações relevantes pendentes (N na etapa de decisão 36), a lógica de controle aguarda um intervalo de tempo predeterminado representado pelo bloco de espera 37. O processo, então, reverte para a etapa 35, pela qual a solicitação de informação sobre transação será repetida periodicamente enquanto a conexão segura persistir. Retornando para a etapa de decisão 36, se os detalhes da transação são retornados pelo servidor 2, então, na etapa 38, a lógica de controle exibe detalhes da primeira transação a ser autorizada no monitor 7. O monitor também solicita ao usuário para aprovar ou recusar a transação através de uma entrada no teclado 8. O resultado é detectado na etapa de decisão 39 e a recusa (etapa 40) ou autorização (etapa 41) da transação pelo usuário é

retransmitida para o servidor 2 por meio da conexão segura. Na etapa de decisão 42, a lógica de controle 11 decide se há outra transação a ser exibida e, caso afirmativo, a operação retorna para a etapa 38 para a próxima transação. Caso negativo, a operação reverte para a etapa de espera 37 aguardando a próxima solicitação de informações sobre transação.

[0032] O processo anterior continua enquanto o TAD permanece conectado através de sua conexão segura com o servidor 2. Desta forma, o TAD 5 coleta, por meio da transação segura, os detalhes sobre transações postergadas que requerem autorização pelo usuário do TAD e solicitadas por qualquer usuário através de qualquer uma das outras conexões entre computadores de usuários 3 e o servidor 2, quer solicitadas antes ou após conexão do TAD 5. As transações postergadas podem incluir transações solicitadas pelo usuário do TAD atual através de uma sessão do navegador com o servidor 2, esta sessão do navegador sendo conduzida inteiramente como normal e permanecendo inalterada na presença do TAD. As transações podem, assim, ser autorizadas pelo usuário quando e sempre que ele se conecta ao servidor, os detalhes da transação sendo transmitidos com segurança e autorizados por intermédio de computadores 3 não confiáveis e da rede 4 não confiável.

[0033] A operação do servidor 2 em resposta a uma solicitação de informações sobre transação postergada a partir de um TAD 5 é indicada na figura 5. Todas estas solicitações são passadas para a lógica de autorização 15 do servidor 2. A etapa 50 representa o recebimento de uma

solicitação pela lógica de autorização 15 a qual, então, verifica o log de transações postergadas na etapa 51 para quaisquer transações que requerem autorização pelo usuário do TAD requerente. Se nenhuma transação relevante é encontrada (N na decisão 52), então, isto é comunicado ao TAD na etapa 53 e o processo termina. Se quaisquer transações relevantes são encontradas no log (Y na decisão 52), então, os detalhes da transação são enviados através da conexão segura com o TAD e a lógica 15, então, aguarda a autorização conforme indicado pela espera 55. Se nenhuma resposta de autorização é recebida (N na decisão 56), a lógica 15 determina, na etapa 57, se um limite "*time-out*" para a resposta foi atingido e, caso afirmativo, o processo termina. Se não, a operação reverte para a espera 55 para aguardar mais um intervalo de tempo. Quando uma resposta de autorização é recebida (Y na decisão 56), a lógica de autorização identifica, na etapa 58, se a transação foi aprovada (Y) ou recusada (N). Se recusada, então, nas etapas 59 e 60, a lógica de autorização exclui a transação do log de transações postergadas 17 e notifica a lógica do servidor 14 sobre a recusa. A lógica do servidor 14 pode, então, tomar as medidas adequadas, tal como notificar o usuário requerente de que a autorização para a transação foi recusada. A operação, então, prossegue para a etapa 61, onde a lógica 15 decide se há novas transações que aguardam autorização. Caso negativo, então, o processo termina, mas, caso positivo, a operação reverte para a etapa 55 para aguardar uma nova autorização. Retornando para a etapa 58, se a transação é autorizada aqui, então, na decisão 63, a

lógica 15 determina, a partir do log de transações, se autorização por outros usuários ainda é requerida para a transação. Caso afirmativo, o log é simplesmente atualizado na etapa 64 para indicar a autorização do usuário atual e a operação prossegue para a etapa 61 conforme antes. Caso negativo, no entanto, a lógica de autorização instruirá a lógica do servidor 14 para executar a transação na etapa 65. A transação é excluída do log de transações postergadas na etapa 64 e a operação prossegue 5 para a etapa 61 para a próxima transação que requer autorização. Uma vez que todas as transações tenham sido autorizadas (ou recusadas) pelo usuário do TAD atual ou o limite "*time-out*" para autorização tenha sido atingido, o processo é considerado concluído.

[0034] O processo anterior permite que o servidor receba autorizações de transação provenientes de usuários móveis sempre que eles se conectam através de qualquer computador do usuário ao sistema de comunicações. Somente quando as autorizações necessárias tenham sido recebidas de todas as partes necessárias, conforme definido no banco de dados de regras 18, uma transação será implementada pelo servidor. As regras no banco de dados 18 podem implementar requisitos de autenticação múltiplas partes complexos arbitrários, por exemplo, para refletir as responsabilidades organizacionais dentro das empresas, o servidor decidindo quais transações devem ser expressamente autorizadas por quais usuários. Por exemplo, assumindo que o Usuário 1 iniciou uma transação no valor de 1000 dólares, o banco de dados poderia conter uma regra que especifica

que autorização para transação segura é requerida pelo Usuário 1 e também o Usuário N se a transação vale mais de 500 dólares. Neste caso, o servidor indicaria uma transação pendente para os TADs de ambos os usuários quando conectados e somente se ambos os usuários autorizam a transação será processada com êxito pelo servidor. Embora MITM ou um software malicioso possa atacar o processo de início de transação por um usuário, o processo de autenticação de transação por múltiplas partes subsequente é protegido contra tais ataques, mesmo embora os TADs sejam operados em computadores não confiáveis. Os usuários podem confiar na informação exibida sobre o TAD e podem comunicar de forma segura suas decisões de autorização de volta para o servidor confiável do provedor de serviços. A autorização de transação através dos TADs, assim, protege transações eletrônicas contra ataques por MITM e softwares maliciosos e suporta regras de autorização de múltiplas partes complexas, ao mesmo tempo em que mantém a mobilidade do usuário. Desta forma, a autorização de transação por múltiplas partes segura pode ser eficazmente aplicada em um ambiente de computação móvel.

[0035] Embora concretizações preferidas tenham sido descritas acima, podem ser consideradas várias adições e alternativas. Por exemplo, o TAD 5 também poderia ser envolvido durante autenticação de usuário quando um usuário de um computador 3 se registra inicialmente no portal do provedor de serviços, por exemplo, através de um navegador da web, para iniciar uma transação. Quando o usuário solicita acesso ao portal, o servidor 2 pode retornar um

código de autenticação, através da conexão segura, o qual pode ser exibido pelo TAD do usuário apenas como uma transação pendente. O usuário pode, então, usar este código para se autenticar junto ao portal ao digitar o código no teclado do computador 3 ou através do teclado do TAD. Em geral, quando de uso de TADs, enquanto uma decisão do usuário é, de preferência, retornada para o servidor através do canal TLS/SSL seguro, o TAD poderia exibir algum código de autorização específico para usuário/transação gerado pelo servidor, juntamente com os detalhes da transação. O usuário poderia, então, copiar o código da tela e enviá-lo para o servidor através de alguma outra conexão possivelmente não confiável, por exemplo, através do navegador da web. Isto permite compatibilidade com portais da web existentes que requerem códigos de uso único, normalmente distribuídos fora de banda através de "raspadinhas" ou texto SMS, a serem inseridos em um formulário da web pelo usuário.

[0036] Embora a operação tenha sido descrita no contexto de um serviço bancário on-line, o sistema pode ser aplicado para autorização de vários tipos de operações de servidor, incluindo concessão de acesso a qualquer tipo de recurso. Por exemplo, os TADs podem ser usados para autorização de controle de acesso por múltiplas partes da mesma maneira conforme a autorização de transação por múltiplas partes. Aqui, se um usuário tenta fazer login no portal do provedor do serviço, o servidor pode solicitar a aprovação de uma ou mais pessoas através de seu TAD, conforme para as operações no exemplo anterior.

[0037] Os TADs podem tomar uma variedade de formas e podem ser dedicados a finalidades exclusivas ou podem ser integrados com algum outro dispositivo que forneça funcionalidade adicional limitada, tal como um leitor de MP3 ou mouse, conforme mencionado anteriormente. A interface de usuário pode ser implementada em uma variedade de maneiras e pode fornecer avisos sonoros para os usuários e/ou exibir informação visual de forma diferente, por exemplo, usando um mecanismo de laser no mouse para produzir uma exibição de projeção sobre um desktop. As interfaces dos computadores TADs e segurança poderiam em geral implementar qualquer forma conveniente de conexão com fio ou sem fio. Na verdade, os dados de segurança para estabelecer a conexão segura podem ser armazenados na memória fisicamente incorporada no TAD, por exemplo, em um chip seguro, o qual é fisicamente protegido contra violação, usando recipientes de dados autodestrutivos ou sensores de detecção de intrusão, por exemplo.

[0038] A funcionalidade do servidor 2 pode ser distribuída por diferentes máquinas de um sistema de servidor e a memória 16 pode ser implementada por um ou mais diferentes componentes de memória distribuídos em mais de uma máquina.

[0039] Será reconhecido que muitas outras alterações e modificações podem ser feitas nas concretizações exemplares descritas sem se afastar do escopo da invenção.

REIVINDICAÇÕES

1. Dispositivo de autorização (5) para autorizar as operações de um servidor remoto (2) solicitadas dos computadores dos usuários (3) através de uma rede de comunicações de dados (4), o dispositivo (5) **caracterizado pelo** fato de que inclui:

uma interface de computador (6) para conectar o dispositivo (5) a um computador do usuário local (3) para comunicação com o servidor remoto (2) através de uma rede de comunicações de dados (4);

uma interface de usuário (7) para apresentar informações para um usuário; e

lógica de controle (11) adaptada para:

usar dados de segurança acessíveis à lógica de controle (11) em uso para estabelecer entre o dispositivo (5) e o servidor (2), através do computador do usuário local (3), uma conexão mutuamente autenticada para comunicações criptografadas extremidade a extremidade entre o dispositivo e o servidor;

coletar, a partir do servidor (2), através de informações de conexão indicativas de qualquer operação solicitada através de uma ligação diferente para o servidor (2) e exigindo autorização por um usuário do dispositivo (5); e

apresentar essas informações ao usuário através da referida interface de usuário (7) para pedir a autorização da referida operação.

2. Dispositivo (5), de acordo com a reivindicação 1, **caracterizado pelo** fato de que a lógica de controle (11) é adaptada para solicitar essas informações a partir do servidor (2) através da referida conexão mutuamente autenticada.

3. Dispositivo (5), de acordo com a reivindicação 1 ou 2, **caracterizado pelo** fato de que a lógica de controle (11) é adaptada para solicitar essas informações a partir do servidor (2) periodicamente, enquanto a conexão mutuamente autenticada persiste.

4. Dispositivo (5), de acordo com qualquer uma das reivindicações 1 a 3, **caracterizado pelo** fato de que a lógica de controle (11) é adaptada para iniciar o estabelecimento da referida conexão mutuamente autenticada em resposta à conexão do dispositivo (5) ao computador do usuário local (3).

5. Dispositivo (5), de acordo com qualquer uma das reivindicações 1 a 4, **caracterizado pelo** fato de que inclui memória que armazena os dados de segurança.

6. Dispositivo (5), de acordo com qualquer uma das reivindicações 1 a 4, **caracterizado pelo** fato de que inclui uma interface de dispositivo de segurança (9) para conectar o dispositivo de autorização (5) a um dispositivo de segurança

(10) armazenando os referidos dados de segurança, onde a lógica de controle (11) é adaptada para acessar os dados de segurança através da interface de dispositivo de segurança (9) em uso.

7. Dispositivo (5), de acordo com a reivindicação 6, **caracterizado pelo** fato de que a interface de dispositivo de segurança inclui uma leitora de cartões (9) para conectar o dispositivo de autorização (5) a um cartão inteligente (10) armazenando os dados de segurança.

8. Dispositivo (5), de acordo com qualquer uma das reivindicações 1 a 7, **caracterizado pelo** fato de que a interface do usuário inclui um mecanismo de entrada (8) para a entrada de autorização do usuário, e no qual a lógica de controle (11) é adaptada para transmitir a referida autorização do usuário para o servidor (2) através da referida conexão mutuamente autenticada.

9. Aparelho para controle de operações de um servidor (2) solicitado dos computadores dos usuários (3) através de uma rede de comunicações de dados (4), o aparelho **caracterizado pelo** fato de que compreende memória (16) para armazenar os dados de regra (18) que definem as operações que requerem autorização por um ou mais usuários, que autorizam e lógica de controle (15) adaptada para:

em resposta a um pedido de um computador de usuário (3) para executar uma referida operação, determinar, a partir dos dados de regra (18), se a autorização de pelo menos um usuário de autorização é necessária para essa operação e, em caso afirmativo, adiar a operação, para se comunicar com um dispositivo que autoriza (5), definido em qualquer reivindicação anterior para estabelecer a referida conexão mutuamente autenticada;

fornecer ao dispositivo que autoriza (5) através da referida conexão informações indicativas das operações de adiadas solicitadas a partir de computadores do usuário (3) e exigir autorização por um usuário do dispositivo que autoriza (5), e receber a autorização do usuário; e

iniciar o desempenho de uma operação adiada, em resposta ao recebimento da autorização de cada usuário de autorização, de quem autorização é necessária para essa operação.

10. Aparelho, de acordo com a reivindicação 9, **caracterizado pelo** fato de que a lógica de controle (15) é adaptada para fornecer essas informações para o dispositivo que autoriza (5) em resposta a uma solicitação do dispositivo que autoriza (5) através da referida conexão mutuamente autenticada.

11. Aparelho, de acordo com a reivindicação 9 ou 10, **caracterizado pelo** fato de que a lógica de controle (15) é

adaptada para receber essa autorização do usuário do dispositivo que autoriza (5) através da conexão mutuamente autenticada.

12. Servidor (2) para realização de operações solicitadas a partir de computadores do usuário (3) através de uma rede de comunicações de dados (4), o servidor (2) **caracterizado pelo** fato de que compreende:

um circuito de comunicação (13) para comunicar com os computadores dos usuários (3) através da rede de comunicações de dados (4);

lógica do servidor (14) para a realização de tais operações, em resposta às solicitações dos computadores dos usuários (3); e

aparelho como definido em qualquer uma das reivindicações 9 a 11 para controlar o desempenho de tais operações pela lógica de servidor (14).

13. Sistema de comunicações de dados (1) **caracterizado pelo** fato de que compreende:

um servidor (2), como definido na reivindicação 12;

pelo menos um computador de usuário (3) para se comunicar com o servidor (2) através de uma rede de comunicações de dados (4); e

pelo menos um dispositivo de autorização (5) como definido em qualquer uma das reivindicações 1 a 8, para

conexão com o computador do usuário (3) através da referida interface de computador (6) do dispositivo (5); em que o computador do usuário (3) é adaptado para comunicação entre o dispositivo de autorização (5) e o servidor (2) através da referida conexão mutuamente autenticada.

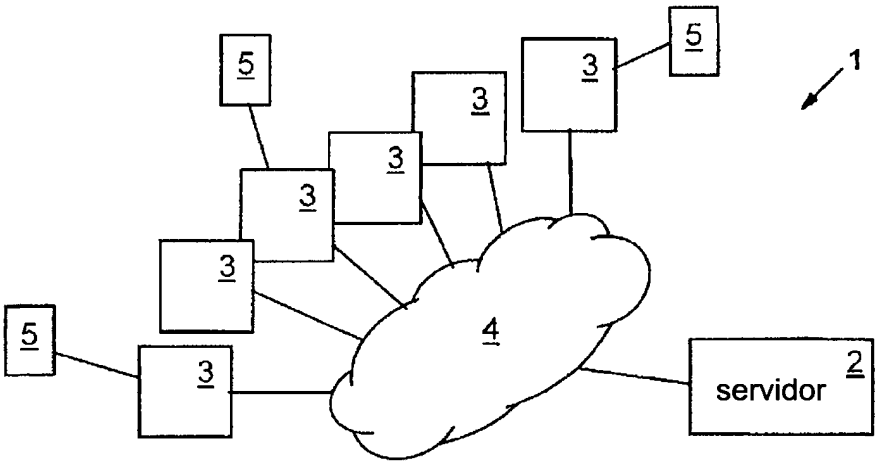

FIGURA 1

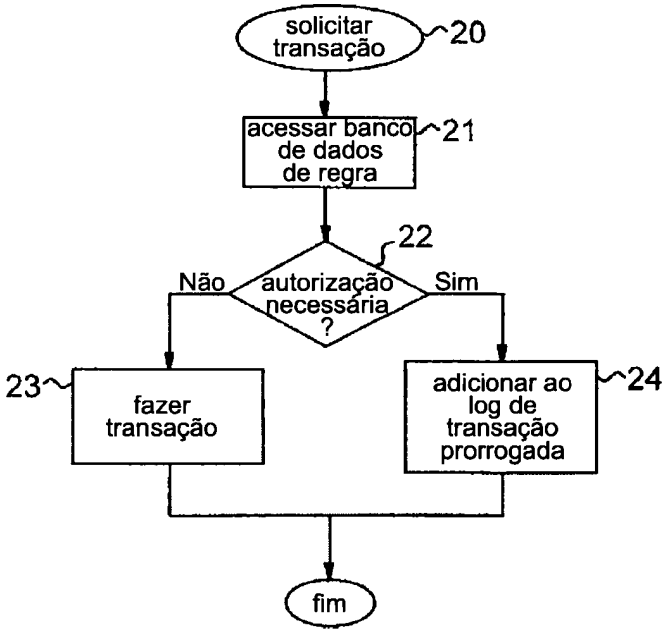

FIGURA 3

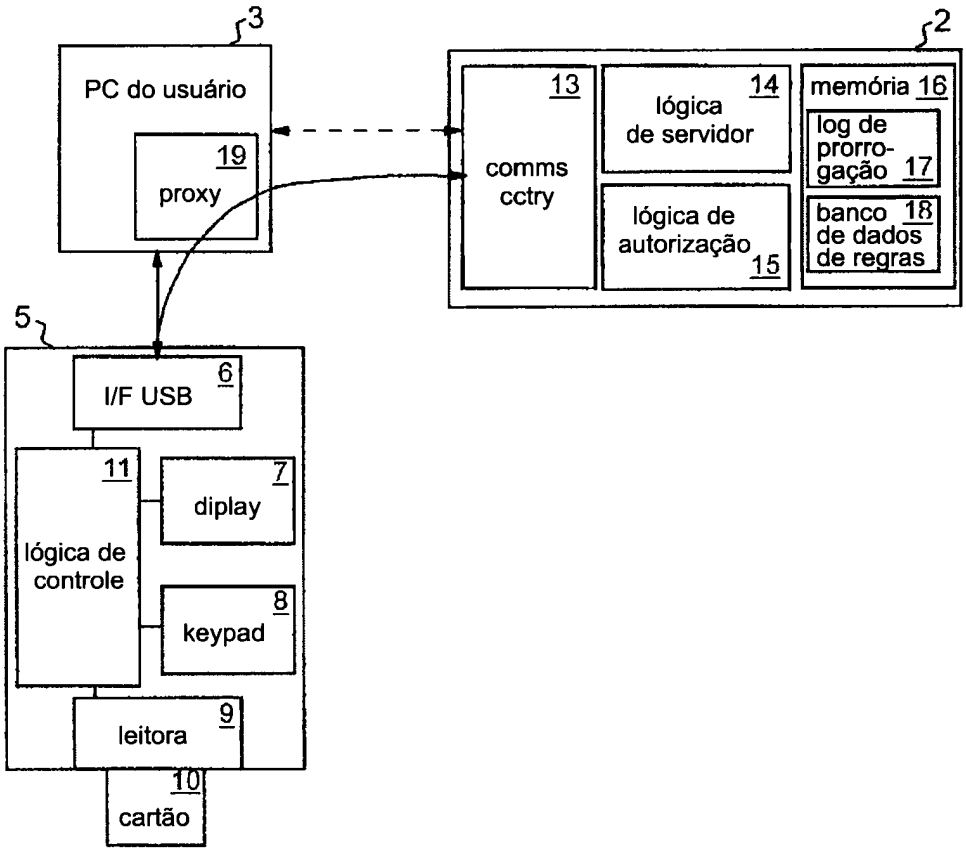
3
PC do usuário
19
proxy
2
13
comms
cctry
14
lógica
de servidor
memória 16
log de
prorro-
gação 17
lógica de
autorização
15
banco 18
de dados
de regras
5
I/F USB
6
11
lógica de
controle
7
diplay
8
keypad
leitora
9
10
cartão

FIGURA 2

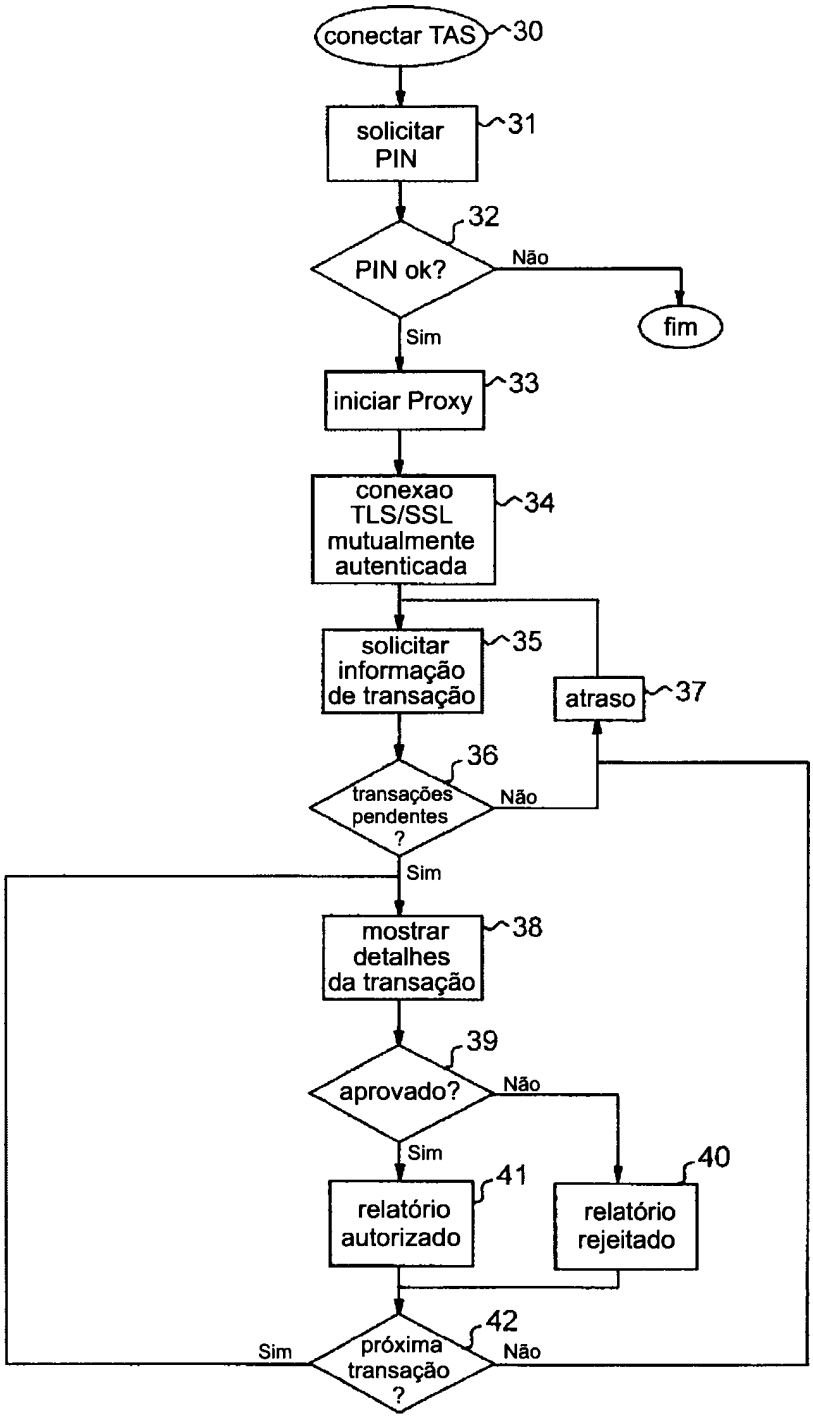
conectar TAS
30
solicitar PIN
31
32
PIN ok?
Não
fim
Sim
iniciar Proxy
33
conexao TLS/SSL mutualmente autenticada
34
solicitar informação de transação
35
atraso
37
36
transações pendentes ?
Não
Sim
mostrar detalhes da transação
38
39
aprovado?
Não
Sim
40
relatório autorizado
41
relatório rejeitado
42
Sim
próxima transação ?
Não

FIGURA 4

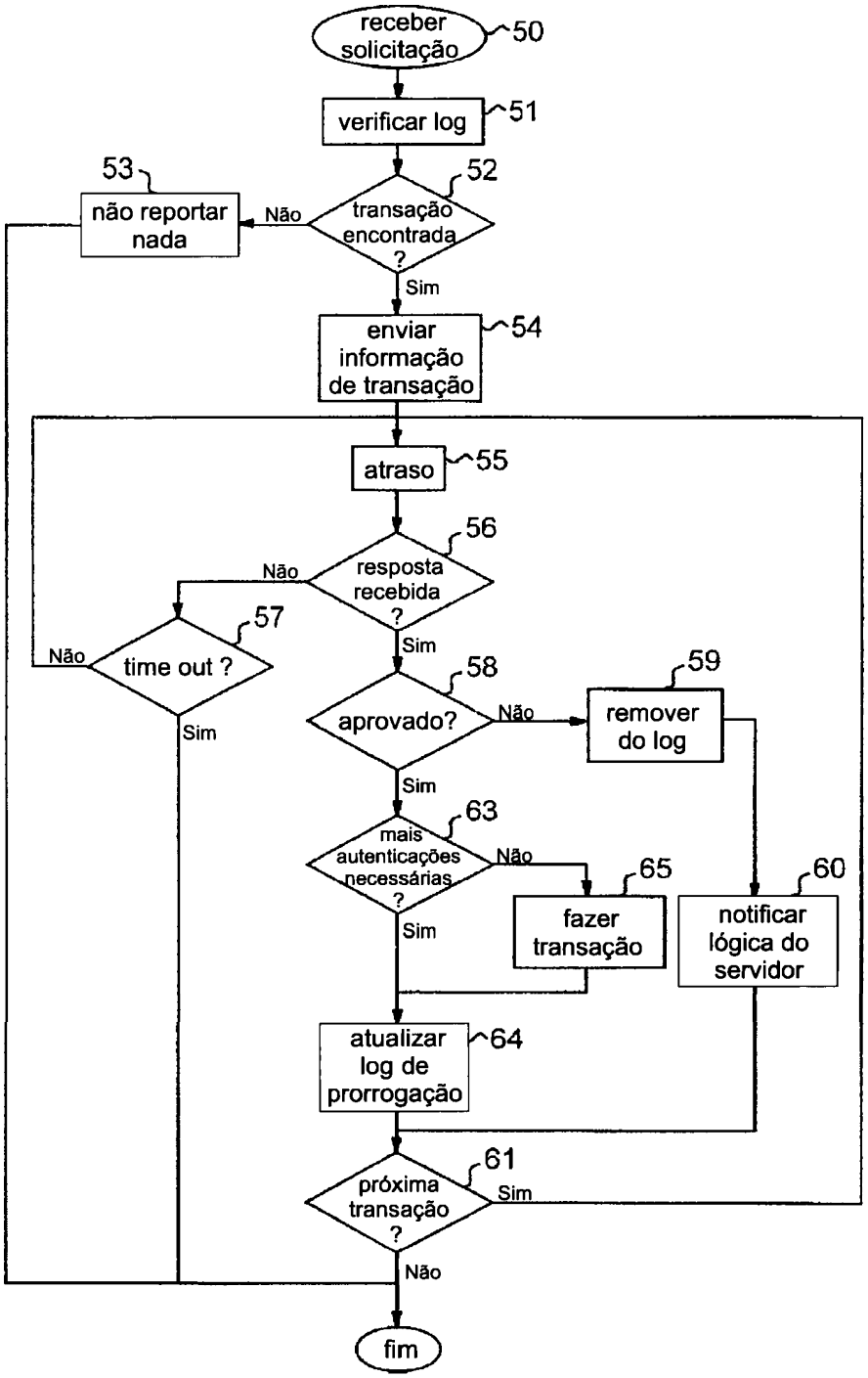
receber solicitação
50
verificar log
51
53
não reportar nada
Não
transação encontrada ?
52
Sim
enviar informação de transação
54
atraso
55
56
Não
resposta recebida ?
Sim
57
Não
time out ?
Sim
58
aprovado?
Não
59
remover do log
Sim
63
mais autenticações necessárias ?
Não
65
fazer transação
Sim
60
notificar lógica do servidor
atualizar log de prorrogação
64
61
próxima transação ?
Sim
Não
fim

FIGURA 5