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

(21) **PI0802251-8 A2**

BRPI0802251A2

(22) Data de Depósito: 07/07/2008
(43) Data da Publicação: 23/08/2011
(RPI 2120)

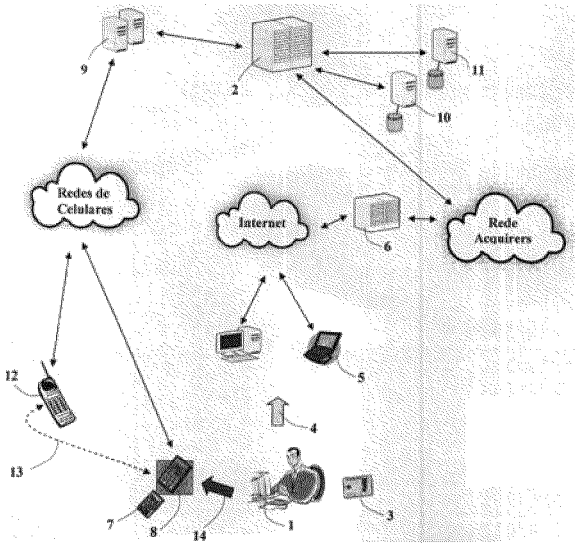
(51) Int.Cl.:
H04L 9/32 2006.01
G07F 7/08 2006.01

(54) Título: **SISTEMA, MÉTODO E DISPOSITIVO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**

(73) Titular(es): TÁCITO PEREIRA NOBRE

(72) Inventor(es): TÁCITO PEREIRA NOBRE

(57) Resumo: SISTEMA, METODO E DISPOSITIVO PARA AUTENTICAÇAO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS A presente invenção situa-se no campo da Tecnologia da Informação, especificamente no campo da autenticação de usuários de sistemas mediante o uso de tecnologias de comunicação à distância, sem fio e refere-se a um sistema, um método e a dispositivo capaz de autenticar usuários e provedores de serviços centralizados, com segurança e de forma recíproca. Mais especificamente, o campo de aplicação da invenção é o dos métodos de gerenciamento de autenticação de pessoas, em seus relacionamentos através de meios eletrônicos digitais.



SISTEMA, MÉTODO E DISPOSITIVO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS

Campo da Invenção

A presente invenção situa-se no campo da Tecnologia da Informação, especificamente no campo da autenticação de usuários de sistemas mediante o uso de tecnologias de comunicação à distância, sem fio e refere-se a um sistema, um método e a dispositivos capazes de autenticar usuários e provedores de serviços centralizados, com segurança, e de forma recíproca.

Mais especificamente, o campo de aplicação da invenção é o dos métodos de gerenciamento de autenticação de pessoas, em seus relacionamentos através de meios eletrônicos digitais como a Internet, por exemplo na realização de transações com cartões de crédito e bancárias, ou ainda na realização de quaisquer outras atividades que envolvam a necessidade de conexão a um servidor central para solicitar serviços, autorização de transações de qualquer natureza ou ainda a assinatura digital de documentos existentes na forma de arquivos digitais, ou ainda através de terminais bancários e de POS (*Point-of-sale*), ou ainda de microcomputadores, ou de simples terminais, com acesso a sistemas centralizados em servidores, ou em rede, como por exemplo os sistemas internos de trabalho de empresas ou organizações de qualquer natureza, ou ainda na efetivação de transações de qualquer natureza através de telefones celulares ou fixos.

Descrição do Estado da Técnica

Os métodos de gerenciamento de autenticação de pessoas buscam assegurar que se tenha a garantia de que uma pessoa que deseja estabelecer um relacionamento, ou efetivar determinada transação digital eletrônica, seja realmente quem afirma ser, para que, desse modo, lhe seja permitido acessar os recursos ou realizar as transações que lhe tenham sido previamente autorizadas.

Desse modo, os citados métodos objetivam reduzir fraudes com falsidade no uso de informações de identidade pessoal, senhas pessoais, números de contas bancárias e de cartões de crédito. Tais fraudes resultam de roubo das informações, através da Internet, mediante o uso de técnicas como *keylogging, spyware, phishing, man-in-the-middle, ou skimming* no caso de acesso a máquinas ATM (*Automatic Teller Machine*) ou terminais de auto-atendimento, bem como do roubo físico de cartões bancários, de crédito, ou de identificação pessoal.

Tais métodos normalmente exigem que os usuários se autentiquem perante os sistemas com os quais se relacionem eletronicamente, fornecendo elementos que sejam dos seguintes tipos:

1) Uma informação pessoal do usuário mas também de conhecimento público, embora de forma tipicamente restrita, como um número de conta corrente, um número de cartão de crédito, um número de apólice de seguro, um número de usuário ou conta de *e-mail*.

2) Uma informação de conhecimento exclusivo do usuário, como uma senha, ou determinada frase secreta.

3) Um elemento físico de propriedade exclusiva do usuário, tal como um cartão com banda magnética, um *Smart card* que se comunique mediante contatos físicos ou sem fio, um *SIM card* usado em celulares, um *token* que gere senhas de validade para uma única vez (*one-time passwords*), um *Smart card* mais um equipamento de leitura deste que, funcionando de forma *off-line*, forneça senhas de validade para uma única vez (*one-time password*) ou ainda um cartão com senhas associadas a posições numericamente identificadas.

4) Uma informação fisicamente contida num cartão, legível por quem o tenha, como um código em alto relevo, sua data de validade, ou código impresso numa banda em seu verso.

5) Uma informação escolhida randomicamente, e assinada digitalmente, por meio de um procedimento de cálculo de um HASH da mesma, e subseqüente encriptação do mesmo com uma chave secreta, chave esta de propriedade comum e exclusiva entre o usuário e o servidor central da organização. A chave secreta e o procedimento aqui descrito são mantidos dentro de um *Smart card* de uso exclusivo do usuário.

6) Uma informação de propriedade e acesso exclusivos do usuário, tal como uma chave privada armazenada em um *Smart card* ou *token*, que tenha sua chave pública correspondente disponível em um certificado digital publicamente disponível e possível de ser reconhecido como válido pelo servidor central. O *Smart card* ou *token* será ativado somente mediante o fornecimento, ao mesmo, de um PIN (*Personal Identification Number*), um número de conhecimento e

uso exclusivo do usuário, de tal forma que o fornecimento consecutivo de um número PIN diferente daquele originalmente cadastrado pelo usuário (usualmente após três vezes) levará o *Smart card* a travar e tornar-se inoperante. Adicionalmente, a chave privada contida ao *Smart card* é de tal forma que nunca poderá deixar seu interior. O recebimento por parte do servidor central de uma mensagem assinada digitalmente com o uso da chave privada contida no *Smart card*, e feita por este a verificação de que a mesma é autêntica, com o uso da chave pública contida no certificado digital do usuário, aceito este como válido pela confiança depositada na Autoridade Certificadora que o assinou, permitirá que a organização reconheça que a pessoa com a posse do *Smart card*, e com a qual está se relacionando pelo meio eletrônico, é efetivamente a pessoa cujos dados de identificação estão contidos no certificado digital correspondente.

7) Uma informação de natureza biométrica obtida de elementos da constituição orgânica do usuário como, por exemplo, suas impressões digitais, formato de suas mãos, formato de seu rosto, desenho de sua íris ou seu DNA.

Atualmente a autenticação é feita tipicamente, das seguintes maneiras, dependendo da situação:

a) NOS RELACIONAMENTOS PRESENCIAIS COM CARTÕES BANCÁRIOS OU COM CARTÕES DE CRÉDITO

A autenticação é feita mediante a apresentação de um cartão de propriedade do usuário contendo apenas banda magnética ou do tipo *Smart card* contendo também uma banda magnética. Tal cartão contém um número de conta bancária ou de cartão de crédito, ou de apólice ou um número de usuário (informação de natureza pública).

O cartão é inserido na leitora de um POS ou de uma ATM que faz parte do sistema, ou da rede da organização com a qual a pessoa deseja relacionar-se e, em seguida, conforme o caso, a pessoa também digita uma senha que seja de seu conhecimento exclusivo.

Os riscos de fraude nestes casos ocorrem quando há roubo ou clonagem de um cartão bancário ou de crédito que faça uso apenas de banda magnética, em que o fraudador não precisa conhecer uma senha, como no caso dos cartões de crédito; ou então a obtém por meio de um dispositivo que, anexado a uma ATM ou um POS, é capaz de recolher a informação do número da conta e da senha, sem o conhecimento do usuário proprietário do cartão ou da instituição a que pertençam estes terminais.

As organizações emissoras de cartões de crédito precisam e mantêm sistemas de monitoração constante das compras realizadas com os cartões que, ao detectarem compras que fujam de um padrão de comportamento reconhecido para a pessoa, ou segundo algum outro critério definido, alerta um grupo de atendentes que, por telefone, buscam entrar em contato com o titular do cartão e, dependendo do caso, chegam mesmo a bloquear o cartão à revelia de seu titular, caso não consigam contatá-lo.

Quando os cartões são do tipo *Smart card* , o risco é substancialmente reduzido, pois a informação da senha fica armazenada no chip do cartão, sendo acessada de forma controlada pelo dispositivo ATM, POS ou leitor de cartão da organização com a qual a pessoa se relaciona, para ser confrontada com a senha digitada pelo usuário que apresenta o cartão para efetuar a transação.

Atualmente muitos bancos já fornecem cartões deste tipo a seus clientes, os cartões com chip, como são os cartões com bandeira *VISA* e *MASTERCARD*, que operam com uma arquitetura interna denominada EMV (*Europay, Mastercard e Visa*), por elas definida, como padrão.

A arquitetura de padrões EMV prevê o uso de cartões *Smart card* com processador simples, o padrão EMV nível 1, ou ainda com dois processadores, o segundo com capacidade de cálculos criptográficos, o padrão EMV nível 2.

A adoção destes padrões objetivou a redução de fraudes nas transações realizadas através de terminais POS com a inserção física dos cartões, que passaram a ter a necessidade de acolher a leitura dos cartões com chip, além dos já tradicionais com banda magnética.

No Brasil, quase todos os terminais POS, bem como os terminais de leitura de cartões, ligados aos caixas das lojas ou supermercados, bem como as máquinas ATM, já foram convertidos para ter esta capacidade, o mesmo ocorrendo ainda em muitos países da Europa. Nos Estados Unidos, no entanto, praticamente toda a rede de aquisição de transações permanece ainda com a capacidade de ler apenas a banda magnética dos cartões.

O padrão EMV nível 1, que utiliza um sistema de autenticação denominado SDA (*Static Data Authentication*), foi concebido e indicado para as situações em que as transações ocorrem em terminais ligados *on-line* aos servidores centrais e o padrão EMV nível 2, que utiliza um sistema de autenticação denominado DDA (*Dynamic Data*

Authentication) para as transações que ocorrem de forma *off-line*.

A autenticação do tipo DDA requer *Smart cards* com um co-processador capaz de cálculos criptográficos, enquanto que autenticação do tipo SDA requer *Smart cards* mais simples, sem esta característica.

O padrão atualmente mais utilizado em decorrência da expansão da rede de telecomunicações é o EMV nível 1 que, efetivamente, já traz expressivas reduções no nível de fraudes, como constatado no programa CHIP & PIN já implementado na Inglaterra há cerca de três anos.

b) NOS RELACIONAMENTOS NÃO PRESENCIAIS COM BANCOS, ATRAVÉS DA INTERNET

Nos relacionamentos com bancos, a autenticação ocorre através da digitação do número da conta corrente e, em seguida, de uma senha específica, diferente daquela associada ao cartão bancário, utilizando-se de um teclado virtual e, além disso, eventualmente segundo opção do banco, também de uma frase secreta de conhecimento exclusivo do usuário. Em seguida uma informação adicional é solicitada, que poderá ser um código associado a uma determinada posição de um cartão previamente fornecido pelo banco, de uso e conhecimento exclusivo de seu cliente, ou ainda uma senha a ser obtida de um *token*, que se altera a intervalos determinados e curtos de tempo.

Alguns bancos usam ainda sistemas que fornecem um número que deverá ser digitado em um dispositivo que, por sua vez, exibirá um número de resposta em seu visor,

que deverá então ser digitado pelo usuário em seu computador de acesso.

Tais procedimentos de autenticação foram se complicando com o tempo, tanto para as instituições como para seus clientes/usuários, com o objetivo de reduzir os riscos de fraude decorrentes de técnicas em que os fraudadores, por processos dissimulados, procuram capturar os elementos requeridos para a autenticação dos usuários.

A adoção destes procedimentos reduziu muito os riscos de fraude mas, por outro lado, complicou muito a vida para os clientes/usuários e para os bancos, com o simultâneo aumento de seus custos associados. Além disso como a autenticação continua ocorrendo através de informações fornecidas através do PC conectado à Internet e os *hackers* continuam sempre, através de truques persuasivos, tentando levar as pessoas a "clicar" em chamadas atraentes para, desta forma, conseguir introduzir um programa espião em suas máquinas e assim buscar coletar informações que lhes permitam fazerem-se passar por elas e executar fraudes bancárias, algum risco de fraude ainda persiste.

Nestes relacionamentos, tipicamente, o cartão bancário não é utilizado para leitura e obtenção de dados pelo computador utilizado para acesso à Internet, sendo assim indiferente se o mesmo é ou não do tipo *Smart card*. Assim, os benefícios alcançáveis pela adoção da tecnologia de *Smart card* com padrão EMV, muito eficaz na prevenção de fraudes em transações presenciais, não puderam ainda ser estendidos de forma tão prática à Internet.

Alguns bancos desenvolveram aplicações utilizando a tecnologia de certificados digitais, com

armazenamento em *Smart card* dotados de um co-processador criptográfico.

Neste tipo de solução a autenticação do usuário se faz tipicamente por um processo descentralizado de desafio/resposta entre o ambiente ao qual está diretamente conectada a leitora de cartões e o *Smart card* nela inserido, seguindo um procedimento, por exemplo, como o tipicamente estabelecido pela norma FIPS 196. A grande variedade de sistemas operacionais de PCs, tipos e versões de *browsers*, requerendo *softwares* específicos para cada fabricante de *Smart card* e de leitora dos cartões *Smart card* evidenciou, no entanto, que uma necessidade de apoio técnico humano muito grande seria necessária para a adequada operacionalidade destas iniciativas tornando-as de baixa viabilidade prática, embora extremamente seguras.

c) NOS RELACIONAMENTOS NÃO PRESENCIAIS DE COMPRAS COM CARTÕES DE CRÉDITO PELA INTERNET

Nestes casos é fornecido o número do cartão e algumas outras informações que dele constam, tais como a data de validade, o código de segurança inscrito em seu verso, bem como o nome do titular como escrito no cartão, com o objetivo de se assegurar que o cartão esteja em mãos do comprador, supondo que este seja efetivamente o titular do cartão. Este procedimento, no entanto, não consegue cobrir as situações em que o cartão foi fisicamente roubado, ou em que estas informações tenham sido indevidamente capturadas por terceiros quando enviadas pela internet, ou fornecidas por telefone ou fax em processos de transações por estes meios, ou ainda mesmo quando o cartão tenha estado em mãos de terceiros, como um garçom de um restaurante.

Outro procedimento que tem sido utilizado é o de empresas que prestam o serviço de recolher o pagamento através do débito em cartão de crédito e depois repassá-lo à empresa que efetuou a venda através da Internet, como por exemplo a *Paypal* ou a *Moneybrokers*. Neste caso a pessoa precisa abrir uma conta em um destes prestadores de serviço, usando seu *e-mail* como código de usuário e definindo uma senha de seu uso exclusivo e mais algumas informações adicionais de seu exclusivo conhecimento.

Nestes relacionamentos, como no caso das transações bancárias, os cartões não são lidos diretamente pelo PC, sendo apenas usados para que dos mesmos sejam coletadas as informações necessárias à realização das transações pela Internet, também não importando neste caso se o mesmo é do tipo *Smart card* ou não.

Pesquisas atuais indicam que é neste tipo de relacionamento que ocorrem com maior intensidade fraudes e perdas para todo sistema de utilização de cartões de crédito.

Com o objetivo de buscar colher benefícios da utilização de cartões do tipo *Smart card* com o padrão EMV, a Mastercard desenvolveu e disponibilizou um processo tecnológico denominado CAP (*Chip Authentication Program*), que requer o uso de um pequeno dispositivo com um teclado e um visor, no qual é inserido o *Smart card* pelo cliente, e que deve ser ativado e mantido como referência durante a realização de sua transação pela Internet.

Este processo tem por base, de um lado, um servidor central mantido pelo banco emissor do cartão de crédito e, de outro, a necessidade de que o usuário insira seu *Smart card* no dispositivo e o ative mediante a digitação

de seu PIN. A partir daí uma alternativa seria o dispositivo gerar uma senha numérica do tipo OTP (*One Time Password*), que o usuário digita no PC, ou então outra alternativa seria o servidor central no ato da transação gerar um código que é exibido na tela do PC, devendo o cliente copiá-lo para o teclado do dispositivo, e este, por sua vez, com base neste número que lhe é fornecido, calcular um novo número, que exibe em sua pequena tela, e que o cliente/usuário deverá então copiar para o teclado do PC.

Sendo o número digitado igual àquele esperado pelo sistema central a transação será autenticada como válida. Este é um processo que já foi adotado por alguns bancos, em alguns países da Europa, mas que, embora eficaz quanto à prevenção de fraudes, introduz um procedimento que não é simples, e que acaba demandando muito dos clientes/usuários.

d) NOVAS ALTERNATIVAS EM EVOLUÇÃO

As estratégias de autenticação descritas nos itens anteriores buscam sempre utilizar um procedimento de autenticação baseado, no mínimo, em dois fatores (*Two Factor Authentication*), tipicamente uma informação de conhecimento exclusivo da pessoa, como um senha ou um PIN por exemplo, e alguma coisa que seja de posse exclusiva da pessoa, como um cartão ou diapositivo, por exemplo.

Em Outubro de 2005, o *FFIEC - Federal Financial Institutions Examination Council*, órgão que é parte do sistema de regulação do Setor Financeiro dos Estados Unidos, em conjunto com o *Federal Reserve* e a *FDIC - Federal Deposit Insurance Corporation*, publicou um guia que determina o uso de procedimentos de autenticação baseados em dois

fatores, estabelecendo inicialmente o final de 2006 como data limite para adoção dos mesmos pelos bancos americanos em suas operações pela Internet. O FFIEC não fez opção, no entanto, por nenhuma tecnologia específica para a adoção dos procedimentos indicados.

Um trabalho publicado pelo *Forrester Research*, de autoria de *Jonathan Penn*, publicado em Julho de 2006, analisa e sugere diversas alternativas para o atendimento destes requisitos pelos bancos.

Por outro lado, com o desenvolvimento e adoção em larga escala do uso de telefones celulares baseados na tecnologia GSM (*Global System for Mobile Communication*), bem como também em menor escala de tecnologias de comunicação sem fio utilizáveis em pequena distância, como *Bluetooth* por exemplo, surgiram várias iniciativas de experimentos de uso destas tecnologias buscando o estabelecimento de um caminho alternativo, diferente da Internet, para se chegar até o usuário e estabelecer-se um procedimento de autenticação do mesmos.

Iniciativas com o uso de celulares ocorreram em formatos simples, com o envio de mensagens SMS para o celular do usuário no momento de realização de sua transação com o banco, e o aguardo de que ele responda com outra mensagem SMS, confirmando-a, bem como em formatos mais elaborados em que o *SIM card* (*Subscriber Information Module*) pequeno *Smart card* presente no celular, foi utilizado para armazenar uma chave privada e um correspondente certificado digital do usuário, criando assim a possibilidade de sua autenticação com base nesta tecnologia com o uso do *SIM card*. Adicionalmente, foram também disponibilizadas soluções de softwares que, instalados nos celulares, permitem que os

mesmos possam ser utilizados também como um token gerador de OTP (One Time Passwords), dispensando assim a necessidade dos tokens físicos.

Alguns exemplos destas iniciativas são:

1) O projeto CASTING (*Smart Card* Applications and Mobility in a World of Short Distance Communication), desenvolvido em conjunto pela ETH Zurich e a Swisscom AG Bern que, segundo publicação de janeiro de 2001, criou e implementou uma solução de autenticação com base no uso do SIM card de um celular, mas usando apenas a capacidade deste de comunicar-se via Bluetooth com um PC, que centralizava todas as comunicações com o servidor central.

2) Um Experimento de Mobile PKI (Public Key Infraestructure), conduzido na Inglaterra por uma iniciativa conjunta da Vodafone, operadora de serviços de celulares com a G&D, fabricante de *Smart cards* alemã.

3) A formação de um consórcio em 1999, formado por companhias tais como Deutsche Bank, Ericsson, Matena, Microsoft, Sema Group, Siemens e TC Trust Center, com o objetivo de viabilizar a adoção de mobile signatures (assinaturas em equipamentos móveis) com base nos SIM cards dos celulares.

4) A publicação WO2005/041608 - do pedido de patente "METHOD OF USER AUTHENTICATION" reivindicando método para autenticação de usuários baseado no uso de SIM cards, com chave privada e certificado digital, pedido este cujo relatório de buscas relaciona-se com dois outros anteriores de números WO02/19593 - "SERVICE PROVIDER INDEPENDENT SAT-

BASED END-USER AUTHENTICATION" e WO2003/0101345 - "SUBSCRIBER AUTHENTICATION".

5) Iniciativa desenvolvida pelo NIST (National Institute of Standards and Technology) reportada em sua publicação NISTIR 7206, e denominada "*Smart Cards* and Mobile Device Authentication: An Overview and Implementation", em que é descrita implementação de uma solução protótipo que utiliza um *Smart card* montado num formato de cartão multimídia, denominado SMC (Smart Multimedia Card), encaixado na leitora para este tipo de cartão existente num dispositivo móvel PDA (Personal Digital Assistant). Adicionalmente implementou também protótipo de um dispositivo independente do PDA, e que com este comunicava-se via Bluetooth, capaz também de receber em conexão o SMC e proceder à autenticação. Os SMC são *Smart cards* diferentes daqueles de uso comum, na forma de cartões plásticos como os dos bancos ou SIM cards dos celulares, sendo montados na forma de multimedia cards, estes segundo os pequenos cartões de memória usados em celulares, PDAs e máquinas fotográficas.

6) Iniciativa da operadora de celulares da Turkcell, que lançou em março de 2008 um programa de oferta a seus usuários para que optando por registrarem-se junto a E-Guven, Certificadora Oficial da Turquia, possam ter seu SIM card substituído por outro com capacidades criptográficas, e assim poderem ter seu certificado digital gerado em seu próprio celular, com apoio da Turkcell. Sua intenção é que assim aplicações possam ser disponibilizadas pelos bancos e outras entidades para autenticação segura dos usuários, bem como de geração de assinaturas digitais pelos mesmos.

Deficiências que ainda persistem nas soluções atuais

Embora o emprego do padrão EMV já tenha sido um grande avanço na prevenção de fraudes nas operações com o uso físico de cartões *Smart card* em dispositivos POS ou ATM, persistem ainda diversas situações que demandam por uma solução que seja ao mesmo tempo segura, prática e economicamente viável.

As situações são as seguintes:

1) Nas transações com cartões de crédito pela Internet, em que o cartão não está presente ao vendedor, ou nas operações com cartões de crédito que disponham de apenas uma banda magnética, permanece o alto risco de ocorrência de fraudes.

A solução CAP sugerida pela Mastercard, utilizando o padrão EMV, embora seja eficaz, representa um processo bastante complicado de ser seguido pelo cliente do banco ou cartão de crédito e tem levado os bancos a relutarem muito em sua adoção.

Por outro lado as soluções de OTP (One Time Password), disponíveis através de tokens específicos, ou através de softwares rodando em celulares tem eficácia apenas nas transações de Internet banking, e nenhuma eficácia nas transações com cartões de crédito pela Internet.

2) As soluções que buscam a autenticação do usuário através do caminho secundário à Internet, representado pelo acesso até ele através da rede GSM de celulares, com a utilização do SIM card como plataforma para

autenticação do usuário, apresenta ainda duas dificuldades básicas consideradas pela ótica do banco ou instituição financeira emissora do cartão, a saber:

a) Como obter, de forma prática e viável, a garantia de que o par de chaves foi emitido de forma segura e de forma correta para seu cliente, e de que o certificado digital foi assinado de forma apropriada por uma autoridade certificadora de sua confiança.

b) Não ter o controle fundamental de propriedade sobre o SIM card, que serviria de apoio vital para seu relacionamento com seus clientes, na medida em que este continuaria a ser de propriedade da Operadora da rede de celulares. Haveria assim uma perda de autonomia para eles quanto, a este possível canal de relacionamento com os clientes.

3) Nas soluções experimentais em que num dispositivo móvel com conexão via celular, em que foi utilizado um *Smart card* diferente do SIM card, este foi de natureza especial, diferente da atualmente usada em larga escala, no formato de um cartão multimídia, e assim embora podendo ser de propriedade do banco emissor, tem características que tornam a solução de baixa efetividade prática.

4) Na soluções em que foi considerada a tecnologia de certificação digital, o processo de autenticação do usuário tem seguido sempre o padrão definido pela FIPS 196, em que a autenticação se dá junto do terminal com o qual se conecta o *Smart card*, de tal forma que após o cartão provar ao terminal que ele tem dentro de si a chave privada que é par do certificado apresentado, as credenciais do usuário contidas no certificado são então consideradas

válidas e utilizadas para identificá-lo perante o servidor com o qual este deseja conectar-se.

Em nenhuma solução encontrada houve o aproveitamento do fato de que o usuário já mantém um relacionamento com a organização, e que, em função disto, poderia ter seu certificado digital armazenado em seus servidores centrais, o que facilitaria em muito o processo inverso em que o servidor central tenha necessidade ou desejo de encontrá-lo e comunicar-se com ele de forma autêntica e segura.

5) Em nenhuma solução encontrada foi considerada a possibilidade de uso da tecnologia WI-FI como canal para que os servidores centrais da organização encontrassem e se comunicassem de forma autentica e segura com os usuários.

Em resumo, com o crescente aumento de sistemas que permitem às pessoas o acesso remoto para a realização das mais diversas transações, notadamente via internet, e com maior destaque as aplicações financeiras bancárias ou com cartões de crédito, e tendo em vista as deficiências acima apontadas nas soluções atualmente reconhecidas, identificou-se a oportunidade e necessidade de um sistema, um método e um dispositivo que permitam a autenticação segura das mesmas perante as organizações com as quais desejem se relacionar, buscando ao mesmo tempo reduzir ao mínimo possível o risco de um hacker vir a apoderar-se de suas informações pessoais e, assim, realizar fraudes utilizando-se das mesmas.

A adoção de um sistema com estas características deverá aumentar significativamente a

confiança das pessoas no uso da Internet, possibilitando assim uma base concreta e firme para uma ampliação substancial do comércio eletrônico com inúmeros benefícios para a economia do país.

Objetivos da Invenção

Constitui o escopo principal da presente invenção prover um sistema de autenticação de pessoas em seus contatos por meios eletrônicos, com organizações com as quais mantenham relacionamento, de forma a atender as necessidades que resolvam as deficiências acima indicadas, isto é, de forma segura, prática e abrangente, incluindo todas as possíveis formas de relacionamento eletrônico à distância.

O escopo acima é atingido por meio dos seguintes objetivos.

Prover uma forma de autenticação segura dos usuários que seja eficaz, prática e economicamente exeqüível, nas operações de compra com cartão de crédito pela Internet, ou nas operações de compra com a utilização física do cartão em POSs ou ATMs, quando este disponha apenas de banda magnética.

Prover uma forma de autenticação que se baseie no uso de um *Smart card* cujo conteúdo esteja sob controle pleno do banco ou instituição que o emita em favor do usuário, e que faça uso das facilidades e segurança das redes de comunicação via tecnologia *GSM* ou *3G*, ou mesmo ainda CDMA ou TDMA, apenas como meio de suporte do relacionamento entre o banco ou instituição e seu usuário ou cliente.

Prover uma solução que seja apoiada no uso de *Smart cards* de formato padrão de mercado, considerando sua escala de disponibilidade, viabilidade quanto aos sistemas de emissão em escala de grande volume com a geração segura de chaves criptográficas, bem como sua praticidade de guarda e manuseio seguro por parte dos usuários.

Prover uma solução em que haja o mais eficaz e eficiente aproveitamento dos certificados digitais dos usuários, utilizando-se de uma arquitetura em que sua guarda e utilização ocorra de modo a tornar o processo de identificação dos usuários a mais rápida e prática possível.

Prover uma solução que utilize todas as tecnologias de comunicação sem fio disponíveis no momento, além das baseadas em *GSM* ou *3G, ou mesmo ainda CDMA ou TDMA*, tais como *WI-FI*, *WIMAX*, *Bluetooth*, *NFC* (*Near Field Communication*) e *MYFARE*.

Ainda outro objetivo da presente invenção consiste em que o sistema de autenticação de pessoas em relacionamentos por meios eletrônicos com arquitetura, softwares e dispositivos, que seja uma solução prática e simples de ser implementada e utilizada.

Ainda outro objetivo da invenção é proporcionar um sistema que possa ser utilizado pelas organizações no seu relacionamento com seus clientes, usuários e fornecedores, mas também com seus próprios funcionários ou colaboradores diretos.

Ainda outro objetivo da invenção é que esta seja economicamente viável sob o ponto de vista de todas as partes a quem ela será de utilidade.

Os objetivos enunciados, bem como outros, são atingidos pela invenção mediante o provimento de um sistema que possibilite que os usuários pessoas físicas, que estejam em comunicação eletrônica com uma organização com a qual já tenham um relacionamento definido, sejam autenticadas e identificadas com maior segurança possível.

Tais comunicações eletrônicas podem ser, por exemplo, relacionamentos de usuários em operações de *Internet banking*, em operações de compra com cartão de crédito tanto pela Internet como em redes de POS (pontos de venda), operações em ATMs, ou mesmo entre usuários internos de uma organização através de sua rede privada de Intranet.

Outro objetivo ainda da invenção é prover um método que permita também, quando for o caso, a obtenção conjunta e simultânea da autenticação segura do usuário e, um registro seguro e inequívoco de sua manifestação de vontade, por exemplo autorizando uma transação de débito ou assinando digitalmente um documento eletrônico, utilizando para isto processos e dispositivos que fazem uso da tecnologia de certificação digital.

Descrição Geral da Invenção

A invenção preconiza a adoção de um cartão *Smart card* fornecido a cada usuário a ser utilizado como seu cartão de identificação digital perante a organização com a qual se relaciona.

O cartão *Smart card* conterá a chave privada de uso exclusivo do usuário e seu certificado digital, que tenha sido assinado por uma autoridade certificadora que seja

de confiança da organização com a qual o usuário mantenha relacionamento podendo, conforme o caso, este papel ser exercido pela próprio banco ou instituição financeira.

O certificado digital do usuário garantirá assim o vínculo seguro entre a chave pública do usuário e uma ou mais informações que o identifiquem de forma unívoca para organização, tais como seu número de CPF e seu nome, por exemplo.

A tecnologia de organização do conteúdo do cartão *Smart card* deverá, quando for o caso, ser aberta e padronizada, como por exemplo a estabelecida pela organização *Global Platform*, de tal forma a possibilitar, de um lado, a não dependência de um único fornecedor de *Smart cards* e, de outro, a carga de novas aplicações em seu interior após sua emissão original, entendendo-se que esta carga posterior possa ocorrer sob gestão e controle da organização emissora original do cartão.

Assim a invenção permitirá, quando for o caso, que um cartão *Smart card* de identidade digital que já seja de uso e posse do usuário, possa também ser utilizado no sistema que implementa a invenção, desde que a arquitetura do *smart card* aceite a carga posterior das aplicações necessárias para isto.

A invenção é realizada através da adoção de nova forma de autenticação do usuário portador de um *Smart card* contendo um certificado digital que o identifique perante a organização com a qual este já mantenha um relacionamento definido (por exemplo, mediante uma conta bancária ou um cartão de crédito, um número de apólice, um número de identificação como funcionário, e outros meios

possíveis), em que o certificado digital, previamente cadastrado junto ao servidor central da organização permitirá que o processo de autenticação seja efetivado por método de desafio/resposta, iniciado a partir do servidor central ocorrendo diretamente entre este e o cartão *Smart card*, e não mais de forma descentralizada, como a prática correntemente empregada. Essa é uma das características essenciais da invenção.

O servidor central enviará ao *Smart card* do usuário um resumo da transação desejada pelo mesmo, com um HASH da mesma assinado digitalmente com a chave pública do mesmo, contida em seu certificado digital previamente armazenado junto aos servidores da organização, bem como também com sua própria chave privada.

Chegando o resumo e seu HASH com estas assinaturas, ao interior do *Smart card*, este fará sua decriptação e verificação com a chave privada do usuário e com a chave pública do servidor central, e sendo o resultado desta verificação correto, acrescentará ao resumo a resposta de confirmação ou não da mesma, manifestada pelo usuário, calculará um novo HASH e o assinará com a chave privada do usuário, e também com a chave pública do servidor central, enviando este resultado de volta ao servidor central. Este, ao receber esta resposta fará a decriptação e verificação da mensagem recebida, e sendo o resultado desta verificação correto, terá assim obtido a autenticação do usuário e o registro inequívoco de sua manifestação de vontade, confirmando ou não a transação em questão, garantindo assim uma evidência de não repúdio com relação à mesma. O método de dupla assinatura permitirá que ambas as partes, servidor central e usuário, tenham assegurada sua proteção quanto uma eventual tentativa de fraude por parte de terceiros.

Além disso, a invenção adota um novo caminho de relacionamento entre o servidor central da organização e o *Smart card* do usuário, independente do PC, terminal ou POs através dos quais o usuário submete suas transações pelos processos atualmente vigentes. Este caminho é efetivado através de conexões com tecnologias, conforme o caso, do tipo *GPRS, 3G, WI-FI, WIMAX, Bluetooth, NFC ou MYFARE.*

Compõem ainda a invenção um novo dispositivo e *softwares* necessários à sua operacionalização, como interface seguro com o *Smart card* do usuário, mediante tecnologia com contato ou sem contato, dispondo ainda de um teclado para entrada do PIN que libere o *Smart card* para uso, bem como para que o usuário manifeste sua concordância ou não em relação à transação, e de uma pequena tela para exibição de mensagens. O dispositivo terá a capacidade de estabelecer uma comunicação de dados segura com o servidor central da organização, por meio das tecnologias mencionadas no parágrafo anterior, bem como com o uso de processos de encriptação simétrica das mensagens, em que a chave simétrica utilizada para isto será única para cada cliente, e poderá ainda dispor, se for o caso de uma porta *USB*.O dispositivo terá ainda uma forma e tamanho que permitam ao usuário levá-lo consigo de forma prática, segura e simples.

Na medida em que aparelhos celulares sejam disponibilizados no mercado com a capacidade de leitura direta de cartões *Smart card* de tamanho padrão, além dos *SIM cards* de que já normalmente dispõe, a invenção disponibilizará os softwares necessários para que estes aparelhos celulares, *smartphones* ou *palmtops,* dos principais fornecedores do mercado, possam prover a mesma funcionalidade de leitura e comunicação com o *Smart card* de identificação

digital do usuário, oferecida pelo dispositivo mencionado no parágrafo anterior, de forma que se o usuário assim o desejar possa utilizar diretamente estes aparelhos para efetivar sua autenticação e registro de sua confirmação ou não da transação.

Caso o celular do usuário disponha de capacidade para conexões *Bluetooth* ou *NFC*, o dispositivo acima mencionado poderá conectar-se com mesmo com utilização das mesmas, servindo então o próprio aparelho celular para estabelecer a conexão com o servidor central mediante a rede *GSM* ou *3G, ou ainda CDMA ou TDMA*.

Compõe ainda a solução um sistema de servidores auxiliares nos quais se concentrem as funções de criptografia a serem desempenhadas pelo ponto central da organização, e além destas também a função de *gateway* para conexão entre os servidores centrais da organização e o *Smart card* de identificação digital dos usuários, de tal forma que a adoção desta nova solução possa ser realizada com um mínimo de impacto no ambiente dos servidores centrais atuais da organização.

A solução proporciona ainda, se for o caso, servidores e estrutura de bancos de dados para o armazenamento dos certificados digitais dos usuários, seu número de acesso via rede de celular, e seu código de identificação unívoca perante a organização, por exemplo, seu número de CPF.

A solução disponibiliza ainda, se for o caso, servidores e a estrutura de software adequada para o exercício da função de Autoridade Certificadora , a afim de

se obter a assinatura digital dos certificados de seus usuários ou clientes.

A adoção da solução poderá ser feita de forma gradativa e sem nenhuma alteração nos métodos de autenticação atualmente já adotados pelas organizações em seus processos transacionais com os usuários através de seus POs ou ATMs, ou através das telas disponíveis para suas transações pela Internet. Uma alteração seria feita nos processos que são executados nos servidores centrais, de tal forma que no momento em que os mesmos recebam uma transação para ser autorizada, verificariam se o usuário já dispõe de um *Smart card* de identificação digital habilitado, e executariam o procedimento de autenticação estabelecido pela invenção, como uma garantia adicional ao que já fazem atualmente. Esta possibilidade de implantação facilitará muito a adoção gradativa desta nova solução, com um mínimo de interferência nos sistemas atuais.

Descrição das Figuras

Para melhor compreensão da invenção proposta ela é em seguida descrita fazendo-se referências aos desenhos anexos, em que:

A figura 1 exibe um diagrama de blocos ilustrativo de sistema de Autenticação Segura de Compra com Cartão de Crédito pela internet, composta por (1) Cliente/Usuário que realiza transações pela Internet, (2) Servidores Centrais do Banco Emissor do Cartão de Crédito, (3)Cartões de Crédito atuais, (4)Processos atuais de compras pela internet, (5)Computadores de acesso à internet, (6)Site de venda pela internet, (7) *Smart card* com certificado digital que identifica a pessoa para a

organização - cartão do cliente, (8) Novo dispositivo, (9)Servidores de Criptografia e Gateway, (10) Serviços de armazenamento de Certificados Digitais, (11)Serviços de autoridade certificadora, (12) Celular com Bluetooth, (13) Conexão Bluetooth e (14) Novo Processo de Autenticação Segura.

A figura 2 exibe um diagrama de blocos ilustrativo do sistema de Autenticação Segura de Internet Banking, com "*two factor authentication*" via canal secundário, composta por (1) Cliente/Usuário que realiza transações pela Internet, (2) Servidores Centrais do Banco Emissor do Cartão de Crédito, (15) Cartões bancários de conta corrente atuais, (16) Processos atuais de Internet Banking,(5)Computadores de acesso à internet,(7) *Smart card* com certificado digital que identifica a pessoa para a organização - cartão do cliente, (8) Novo dispositivo, (9)Servidores de Criptografia e Gateway, (10) Serviços de armazenamento de Certificados Digitais, (11)Serviços de autoridade certificadora, (12) Celular com Bluetooth, (13) Conexão Bluetooth e (14) Novo Processo de Autenticação Segura.

A figura 3 exibe um diagrama de blocos ilustrativo de compras com cartões de crédito em POS que não tenha leitor de *smart card*, ou quando o cartão de crédito não seja do tipo *smart card* composta por (17)Cliente/Usuário que compra através de POS, (2) Servidores Centrais do Banco Emissor do Cartão de Crédito, (3)Cartões de Crédito atuais,(18) Processos atuais de compra com cartões de crédito via POSs, (7) *Smart card* com certificado digital que identifica a pessoa para a organização - cartão do cliente, (8) Novo Dispositivo, (9) Servidores de Criptografia e Gateway, (10) Serviços de

armazenamento de Certificados Digitais, (11)Serviços de autoridade certificadora, (12) Celular com Bluetooth, (13) Conexão Bluetooth e (14) Novo Processo de Autenticação Segura.

A figura 4 exibe um diagrama de blocos ilustrativo de Operações de Bolsa autorizadas por telefone, composta por (23) Cliente/Usuário que da ordens de bolsa por telefone, (22) Servidores Centrais da Corretora de valores, (19) Bolsa de Valores, (20) Operadores de Bolsa, (21) Processos atuais de compra/venda de ações com ordens por telefone, (7) *Smart card* com certificado digital que identifica a pessoa para a organização - cartão do cliente, (8) Novo dispositivo, (9)Servidores de Criptografia e Gateway, (10) Serviços de armazenamento de Certificados Digitais, (11)Serviços de autoridade certificadora, (12) Celular com Bluetooth, (13) Conexão Bluetooth e (14) Novo Processo de Autenticação Segura.

A figura 5 exibe um diagrama de blocos ilustrativo de Acesso à Rede Intranet de uma Organização composta por (27) Usuário da Intranet, (24)Rede Intranet da Organização, (25) Servidor de controle de acesso da Intranet, (26) Processos atuais de Log In na rede Intranet,(7) *Smart card* com certificado digital que identifica a pessoa para a organização - cartão do cliente,(8) Novo dispositivo, (9) Servidores de Criptografia e Gateway, (10) Serviços de armazenamento de Certificados Digitais, (11) Serviços de autoridade certificadora, (12) Celular com Bluetooth, (13) Conexão Bluetooth, (14) Novo Processo de Autenticação Segura, (28) Ponto de Acesso WIFI à Intranet, (29) Conexão WIFI.

A figura 6 exibe uma implementação preferida do dispositivo em que (31) mostra sua parte frontal e (32) mostra sua parate posterior, em que é indicada ranhura por onde é inserido o *smart card* e um orifico na tampa traseira do dispositivo, por intermédio da qual pode-se retirar o *smart card* do dispositivo, fazendo-o escorregar fazendo pressão sobre o mesmo com um dedo.

Descrição Detalhada da Invenção

O usuário recebe um certificado digital que tem sua chave privada correspondente armazenada em um *Smart card* de seu uso exclusivo, que é habilitado para uso somente mediante um número PIN (*Personal Identification Number*) de conhecimento exclusivo do usuário.

O certificado digital vincula sua chave pública a uma informação que identifica o usuário de forma única perante a organização (por exemplo seu CPF) e é assinado por uma certificadora de confiança da organização, eventualmente ela mesma.

Recebe também o dispositivo que vai permitir a conexão direta dos servidores centrais da organização com o *Smart card*, mediante a liberação desta conexão pelo usuário, ou então fará uso de um celular que seja capaz de ler seu *Smart card* com seu certificado digital e sua chave privada.

Os certificados digitais dos usuários são armazenados nos servidores centrais da organização, em associação à informação que identifica o usuário para a organização e mais outras informações que caracterizam seu relacionamento com ela, tais como um número de conta, um

número de cartão de crédito, um número de apólice, por exemplo.

A informação do número de celular que será usado para enviar mensagens e estabelecer a conexão com o *Smart card* do usuário também é armazenado neste conjunto.

Os processos existentes de relacionamento do usuário com a organização via computadores conectados a ela pela internet, ou através de terminais POS, permanecem os mesmos.

Em todos eles, na etapa em que a transação originada pelo usuário através de seu PC conectado à Internet ou através de um POS, é encaminhada aos atuais servidores centrais da organização para aprovação, estes ao perceberem que o usuário já tem seu certificado digital e o *Smart card* para usá-lo neste novo sistema de autenticação, encaminham um resumo da transação e uma cópia do certificado digital do usuário aos novos servidores de criptografia e *gateway* previstos pela invenção.

Estes, por sua vez, gerarão um desafio criptográfico, incluindo neste uma dupla assinatura digital do resumo da transação utilizando sua própria chave privada e o certificado do usuário que recebeu dos servidores centrais, enviando uma mensagem para o dispositivo ou celular do usuário.

O usuário sabendo a priori que a transação em questão vai requerer sua aprovação explícita, mediante o uso de seu certificado em seu *Smart card*, deverá ligar seu dispositivo, e ativá-lo mediante a digitação em seu teclado de seu PIN.

Assim que a mensagem chegar a seu dispositivo ou celular, este lhe será mostrada na tela deste, solicitando que o usuário pressione uma de duas teclas designadas no dispositivo ou celular para que ele manifeste sua concordância ou não com os dados da transação que incluirão basicamente a identificação da organização, data e valor ou natureza da transação.

O usuário terá a opção de pressionar uma tecla SIM ou uma tecla NÃO. Pressionando a tecla SIM o sistema no dispositivo irá submeter o desafio criptográfico ao *Smart card*, acrescido da resposta SIM do usuário, solicitando sua resposta.

O *Smart card* realizará o processo de verificação das assinaturas recebidas e, acrescentando ao resultado obtido desta a informação do SIM decidido pelo usuário, gerará por sua vez uma nova assinatura digital do pacote resultante, retornando-o ao dispositivo ou ao celular nas mãos do usuário, com o qual está conectado.

Este, ao receber esta resposta, avisará ao usuário que recebeu a informação do *Smart card* e que já a encaminhou a sua resposta aos servidores centrais da organização.

Desta forma bastará a escolha do SIM pelo usuário, teclando a tecla correspondente, para que todo este processo se desenvolva de forma transparente e sem nenhum trabalho adicional para ele, caracterizando-se assim um procedimento extremamente simples e prático de se usar.

O procedimento será seguro também, sem o risco de que alguém possa apoderar-se do PIN do usuário, pois

o *Smart card* será lido num dispositivo do usuário, num teclado e em contato direto e exclusivo com o usuário, sem nenhum intermediário adicional possível entre ele e seu *Smart card*.

Os servidores de criptografia centrais, ao receberem a mensagem de resposta do usuário, verificarão a assinatura digital desta gerada pelo *Smart card*, e se a mesma conferir, encaminharão aos servidores centrais a informação de que autenticação foi bem sucedida. Os servidores centrais retornarão então aos pontos remotos a liberação da transação solicitada pelo usuário.

No caso de transações com cartões de crédito, poderá ser incluída no corpo da mensagem de retorno uma cópia da seqüência de caracteres que constituem a assinatura digital gerada pelo *Smart card* do usuário, que constituirá a evidencia de sua concordância com a mesma, ficando assim dispensada sua assinatura gráfica, como hoje requerida.

Caso o usuário opte por não aceitar a transação, acionando a tecla NÃO, o mesmo processo acima descrito será efetivado, porém com a informação da opção do usuário pelo NÃO, sendo desta forma gerada uma reposta para os servidores centrais com a assinatura digital produzida pelo *Smart card*, caracterizando assim uma resposta inequívoca com o NÃO do usuário.

Ao receber esta resposta os servidores centrais notificarão o ponto remoto de origem da transação da resposta negativa do usuário.

Caso o usuário mantenha o dispositivo desligado ou não ative o *Smart card* através do PIN correto,

os servidores centrais , após a espera de um tempo padrão estabelecido pela organização , retornarão uma mensagem ao ponto de origem da transação negando a autorização para que a mesma seja efetivada, indicando um código que indique o porquê da negativa.

Caso a verificação da assinatura da mensagem recebida pelos servidores centrais de criptografia indique que a mesma não confere, a transação será também negada e informada ao ponto remoto o porquê da negativa.

O resultado final obtido é um processo de autenticação dos usuários extremamente simples, seguro e prático, fazendo uso de diversas tecnologias atualmente existentes de uma nova forma, caracterizando novas possibilidades de redução efetiva de fraudes, e em consequência um aumento efetivo de novos negócios através da internet e dispositivos móveis de comunicação sem fios, na medida em que seja possível assim às pessoas adquirir uma nova e crescente confiança para efetuar suas compras e transações pela Internet.

REIVINDICAÇÕES

1. **SISTEMA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários, caracterizado por por sua arquitetura compreender:

- armazenamento de certificado digital (10) do usuário em servidor (2) central da organização

- utilização de tecnologia de encriptação (9) simétrica e assimétrica.

- utilização de *Smart cards* (7) com coprocessador criptográfico, com elementos para identificação do usuário por meio de seu certificado digital (10).

- dispositivo(8) para leitura e operacionalização do *Smart card* (7) para que se comunique com o servidor central (2) por conexão sem fio de longa ou curta distância, por conexão direta do dispositivo (8) com o servidor central (2), ou conexão *Bluetooth* (13) ou *NFC* entre o dispositivo (8) e um celular (12) ou PC (5).

- geração de certificado digital (10) do usuário sob responsabilidade da organização central, vinculando a chave pública do usuário à informação que o identifica, sendo a assinatura do mesmo obtida pela organização (11); e fornecimento do mesmo ao usuário.

2. **SISTEMA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários, de acordo com a reivindicação

1, caracterizado pelo fato de o certificado digital (10) e o par de chaves do cliente/usuário serem gerados pela própria organização, por exemplo o banco, no interior dos *Smart cards*, que são então distribuídos com os certificados e as chaves privadas aos usuários.

3. **SISTEMA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários, de acordo com a reivindicação 2, caracterizado pelo fato de o usuário armazenar junto à organização também um certificado do tipo e-CPF, ou de identificação já existente e aceito como válido pela mesma .

4. **SISTEMA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários, de acordo com a reivindicação 3, caracterizado pelo fato de utilizar um cartão *Smart card (7)* como instrumento de identificação, em aplicação de autenticação segura para compras por cartão de crédito via internet.

5. **SISTEMA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários, de acordo com a reivindicação 4, caracterizado por utilizar aparelho celular (12) para a

conexão e a comunicação entre um servidor central (2) e um *Smart card (7)* distinto do *SIM* cad já existente, junto ao celular.

6. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com oS usuários, caracterizado pelo fato de o certificado digital (10) ser previamente cadastrado junto ao servidor central (2) da organização, de modo que a autenticação seja efetivada por desafio/resposta iniciado a partir do servidor central (2) ocorrendo diretamente entre este e o cartão *smart card* (7).

7. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com oS usuários de acordo com a reivindicação 6, caracterizado por conter um **primeiro passo** em que o servidor central (2) envia ao *Smart card* (7) do usuário um resumo da transação desejada pelo mesmo, com um HASH da mesma assinado digitalmente com a chave pública do mesmo, contida em seu certificado digital (10) previamente armazenado junto aos servidores da organização, bem como também com a própria chave privada do servidor central.

8. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a

qual se relacionem, bem como a autenticação da organização de forma recíproca para com oS usuários de acordo com a reivindicação 7, caracterizado por conter um **segundo passo** em que uma vez chegando o resumo e seu HASH com as assinaturas ao interior do *Smart card* (7), este faz sua decriptação e verificação com a chave privada do usuário e com a chave pública do servidor central.

9. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com oS usuários de acordo com a reivindicação 8, caracterizado por conter um **terceiro passo** em que o resultado de verificação correta, acrescenta ao resumo a resposta de confirmação ou não da mesma, manifestada pelo usuário, calcula um novo HASH e o assina com a chave privada do usuário e também com a chave pública do servidor central, enviando este resultado de volta ao servidor central.

10. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com oS usuários de acordo com a reivindicação 9, caracterizado por conter um **quarto passo** em que ao ser recebida a resposta faz a decriptação e verificação da mensagem recebida.

11. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com oS usuários de acordo com a reivindicação 10, caracterizado por conter um **quinto passo** em que o resultado da verificação sendo correta terá assim obtido a autenticação do usuário e o registro inequívoco de sua manifestação de vontade, confirmando ou não a transação em questão, garantindo uma evidência de não repúdio com relação à mesma.

12. **MÉTODO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários caracterizado pelo fato de, nas situações em que a transação é originada pelo usuário, através de PC conectado à Internet ou através de um POS, quando o mesmo já possui certificado digital e *Smart card*, conter os passos de:

- os atuais servidores centrais da organização, ao receberem a solicitação de aprovação da trasação desejada pelo usuário, encaminharem um resumo da transação e uma cópia do certificado digital do usuário aos novos servidores de criptografia e gateway previstos pela invenção.

- estes novos servidores gerarem um desafio criptográfico, incluindo dupla assinatura digital utilizando sua própria chave privada e o certificado do usuário recebido dos servidores centrais.

- o usuário ligar seu dispositivo e ativá-lo mediante a digitação em seu teclado de seu PIN.

- o usuário manifestar sua concordância, ou não, com os dados da transação informados através da tela existente no novo despositivo, que incluirão basicamente a identificação da organização, data e valor ou natureza da transação.

- o usuário optar por pressionar uma tecla SIM ou uma tecla NÃO, como forma de resgistro desta manifestação, podendo neste momento ser ou não solicitado a novamente digitar seu PIN como forma de ratificar sua escolha.

- o Smart card realizar a verificação das assinaturas recebidas, acrescentando ao resultado obtido a informação do SIM decidido pelo usuário, gerando nova assinatura digital do pacote resultante, retornando-o ao dispositivo ou ao celular nas mãos do usuário com o qual está conectado.

- recebida a resposta, este avisar ao usuário que recebeu a informação do Smart card e que já a encaminhou sua resposta aos servidores centrais da organização.

- os novos servidores de criptografia verificarem a assinatura digital gerada pelo Smart card encaminhando aos servidores centrais a informação de que a autenticação foi bem sucedida.

- os servidores centrais retornarem aos pontos remotos a liberação da transação solicitada pelo usuário.

- os servidores centrais retornarem uma resposta negando a aprovação da transação ao ponto remoto, de onde tenha partido a solicitação de autorização para a transação, podendo este ser por exemplo um site de comércio eletrônico, um PC ou um POS, caso o usuário negue a transação, ou a verificação pelo novo servido central de

criptografia indique um resultado não correto, ou ainda caso o dispositivo do usuário esteja desligado, ou ainda o usário não responder dentro de um intervalo de tempo definido como padrão.

13. **DISPOSITIVO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários, caracterizado por conter tecnologia com contato ou sem contato, em sua comunicação com o *smart card*, dispondo ainda de um teclado para entrada do PIN que libere o *smart card* (7) para uso, bem como para que o usuário manifeste sua concordância ou não em relação a transação, e de uma pequena tela para exibição de mensagens, sendo ainda de dimensão e formato pouco maiores do que o de um smat card de tamanho padrão de mercado, de forma a facilitar seu manuseio e guarda.

14. **DISPOSITIVO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários de acordo com a reivindicação 13, caracterizado por ser específico para conectar-se a longa distância diretamente com um servidor central através de redes de telefonia celular (12), e adicionalmnte a curta distância com algum outro dispositivo que já seja capaz de conectar-se ao servidor central, por exemplo um celular ou um PC, através das tecnologias de *Bluetooth (13), NFc, WI-FI* ou *WIMAX*, de forma a receber mensagem dirigida ao *Smart card* do usuário, se for o caso no

formato SMS, e transmitir de volta aos servidores centrais da organização a resposta nele escolhida pelo usuário, SIM ou NÃO, após seu devido processamento pelo *Smart card* do mesmo.

15. **DISPOSITIVO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS**, para autenticação segura de usuários no estabelecimento de contato e efetivação de transações de qualquer natureza com uma organização com a qual se relacionem, bem como a autenticação da organização de forma recíproca para com os usuários de acordo com a reivindicação 13, caracterizado por dispor da capacidade de armazenar uma certa quantidade das transações que tenham sido assinadas com o uso do mesmo, bem como de transferi-las para algum outro dispositivo, por exemplo um PC, segundo a conveniência do usuário.

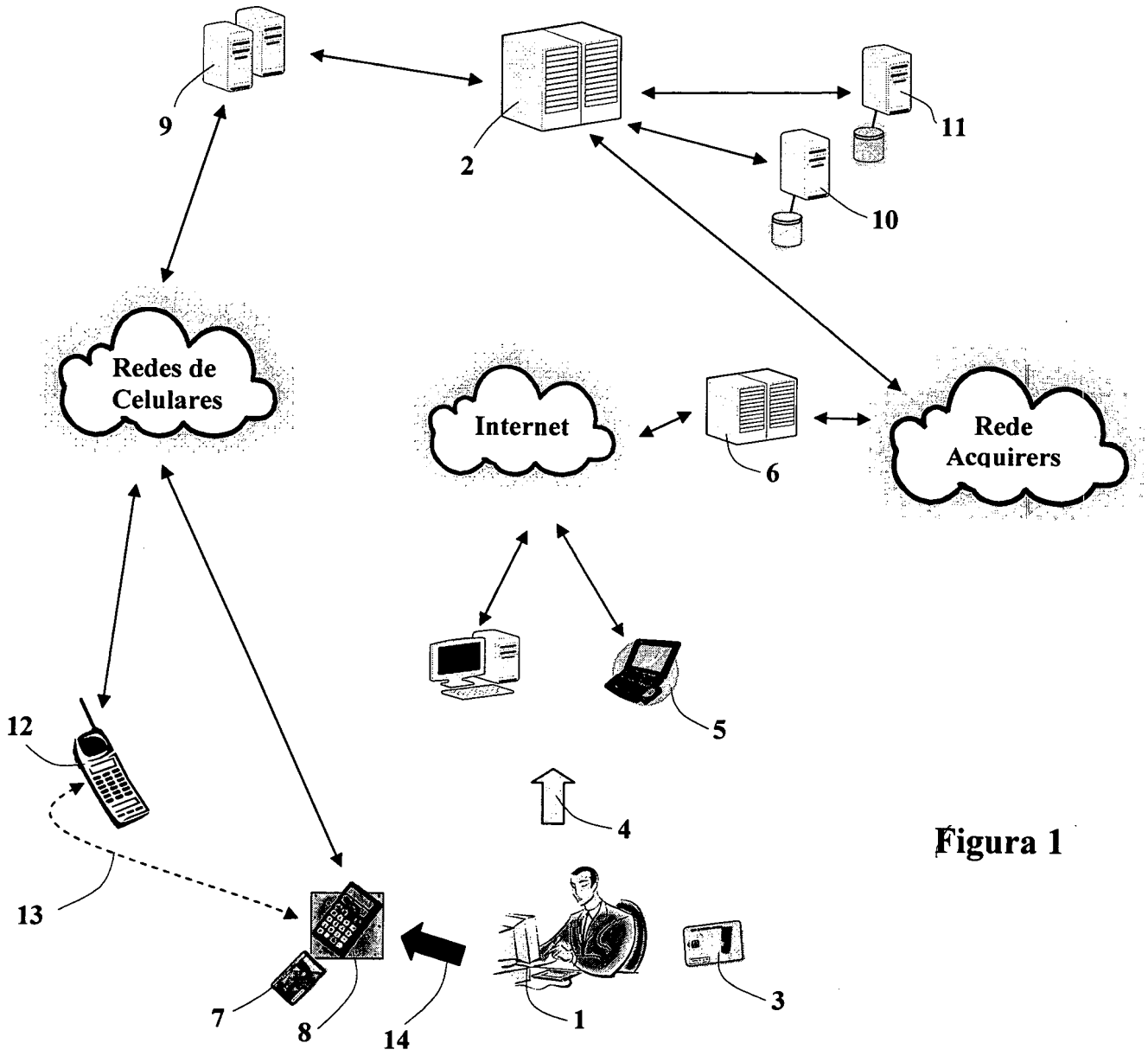

9
2
11
10
Redes de Celulares
Internet
6
Rede Acquirers
5
12
4
13
7
8
14
1
3

Figura 1

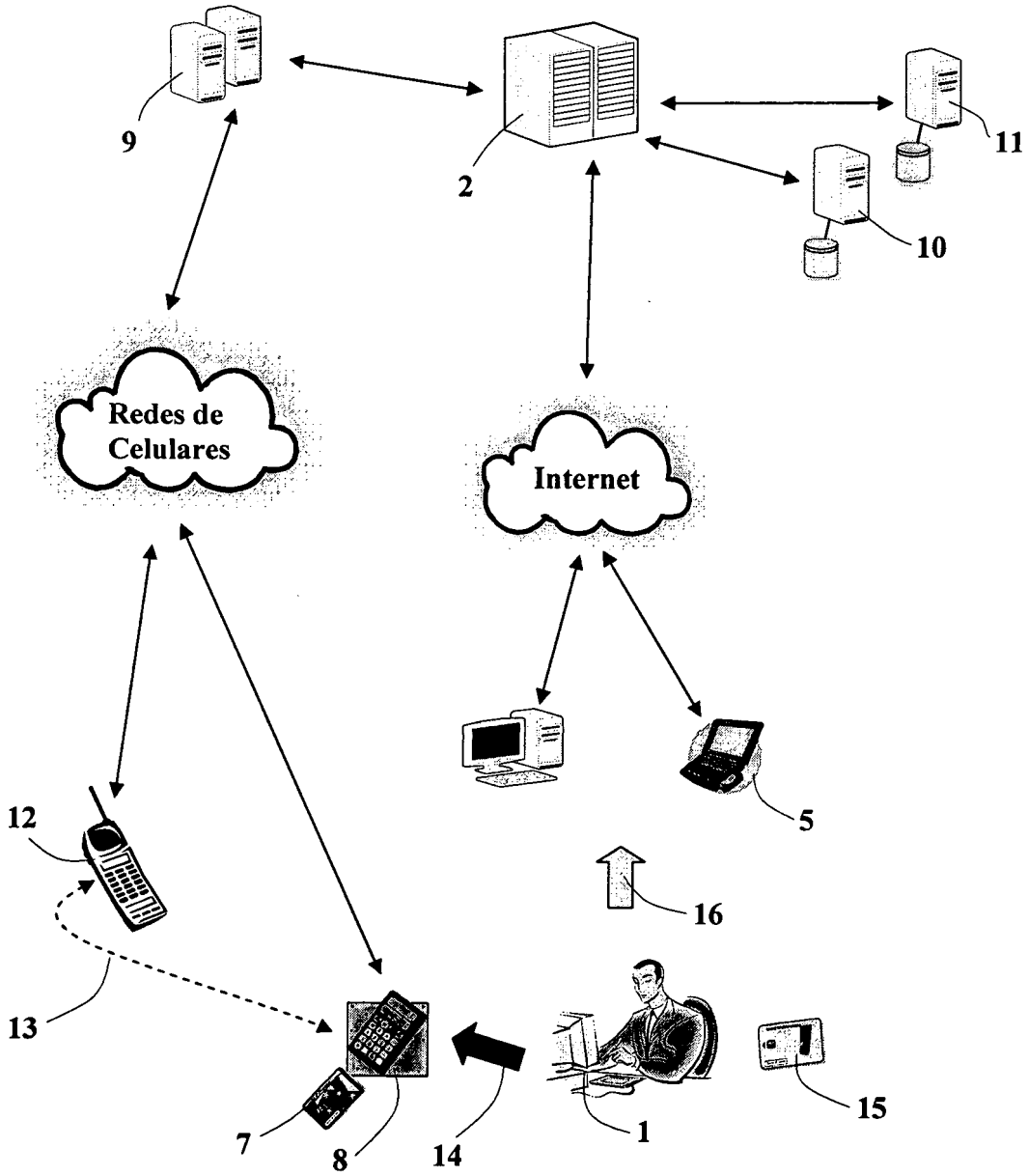


Figura 2

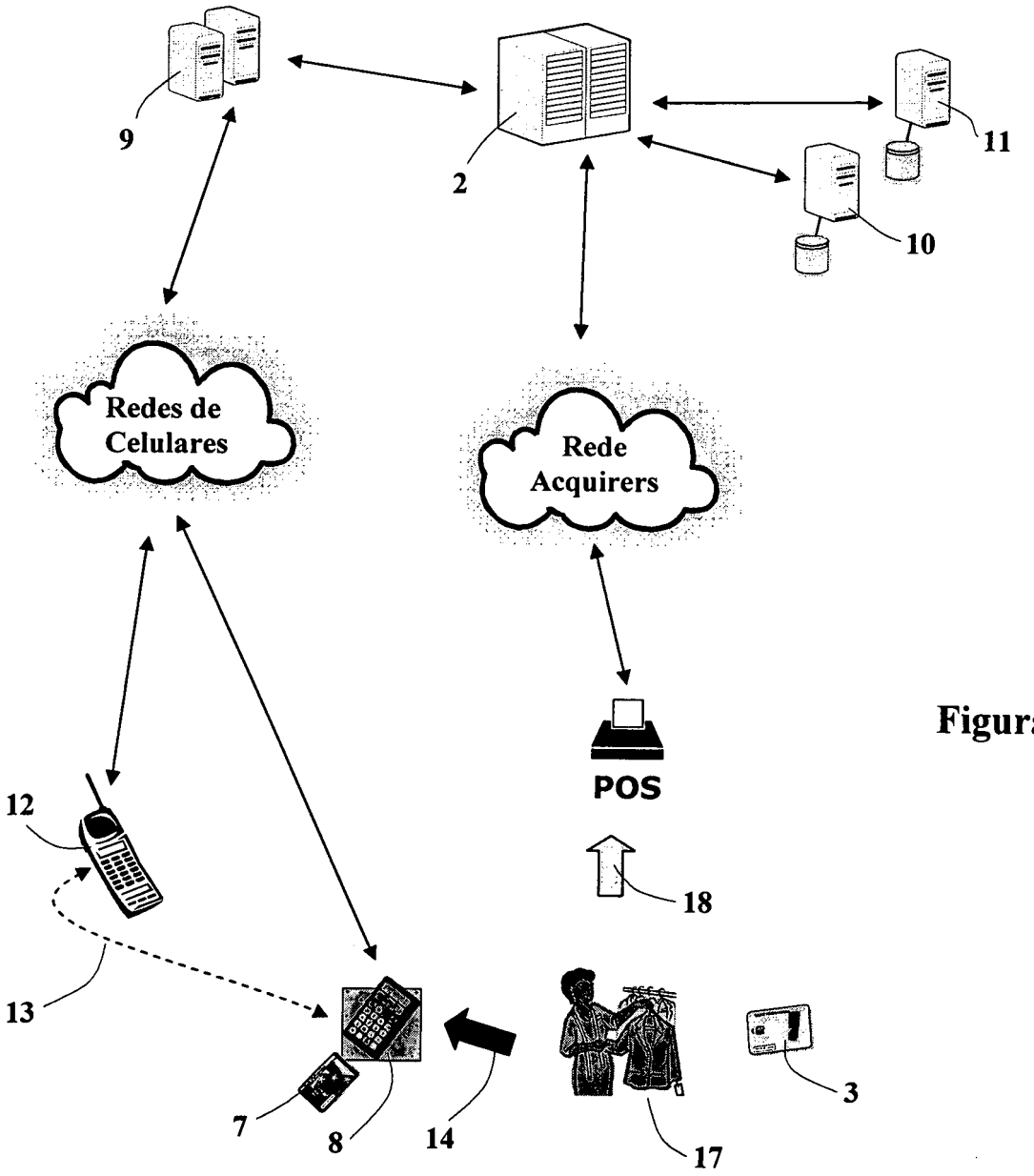

9
2
11
10
Redes de Celulares
Rede Acquirers
POS
18
12
13
7
8
14
17
3

Figura 3

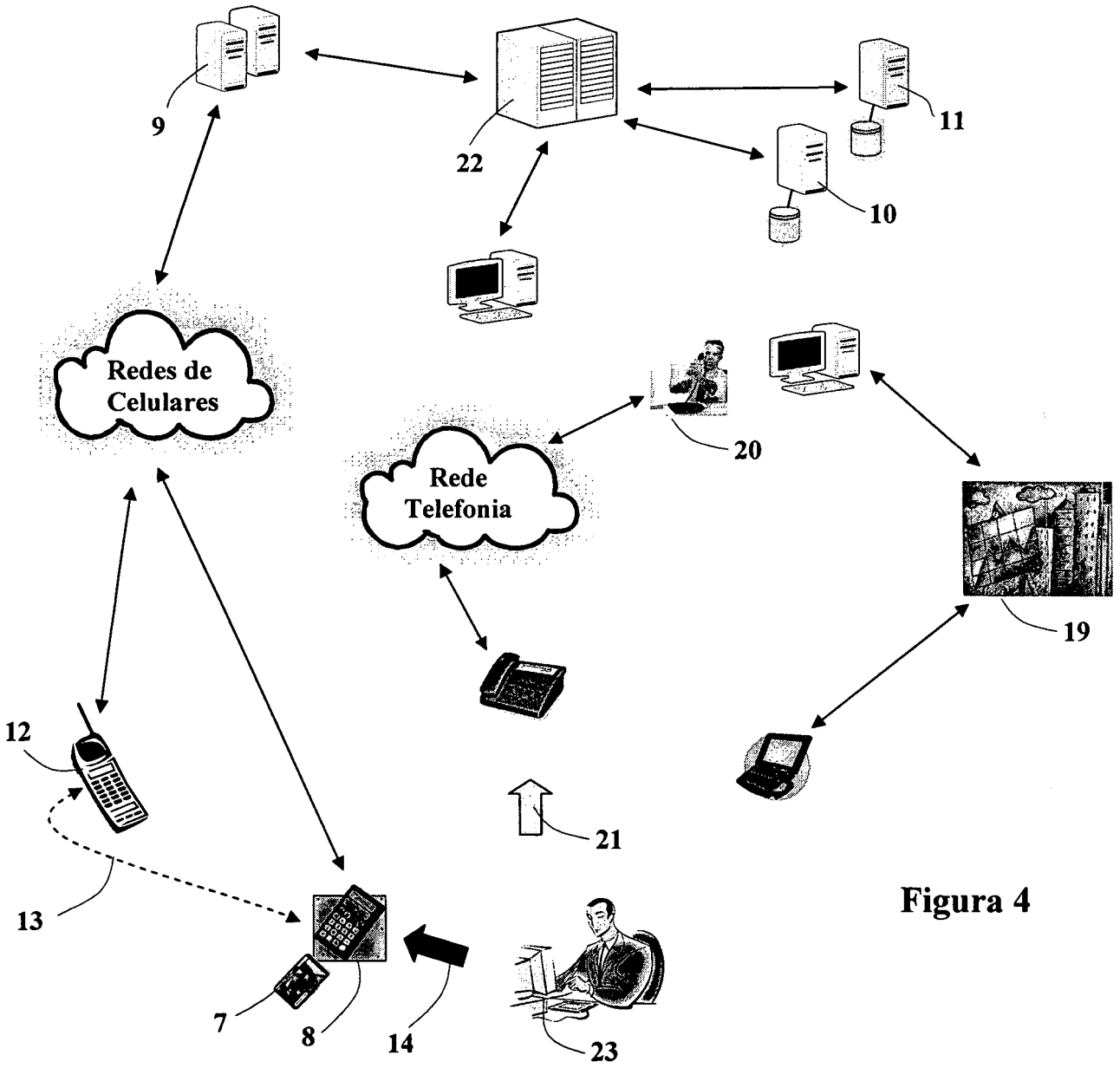

9
22
11
10
Redes de Celulares
Rede Telefonia
20
19
12
13
21
7
8
14
23

Figura 4

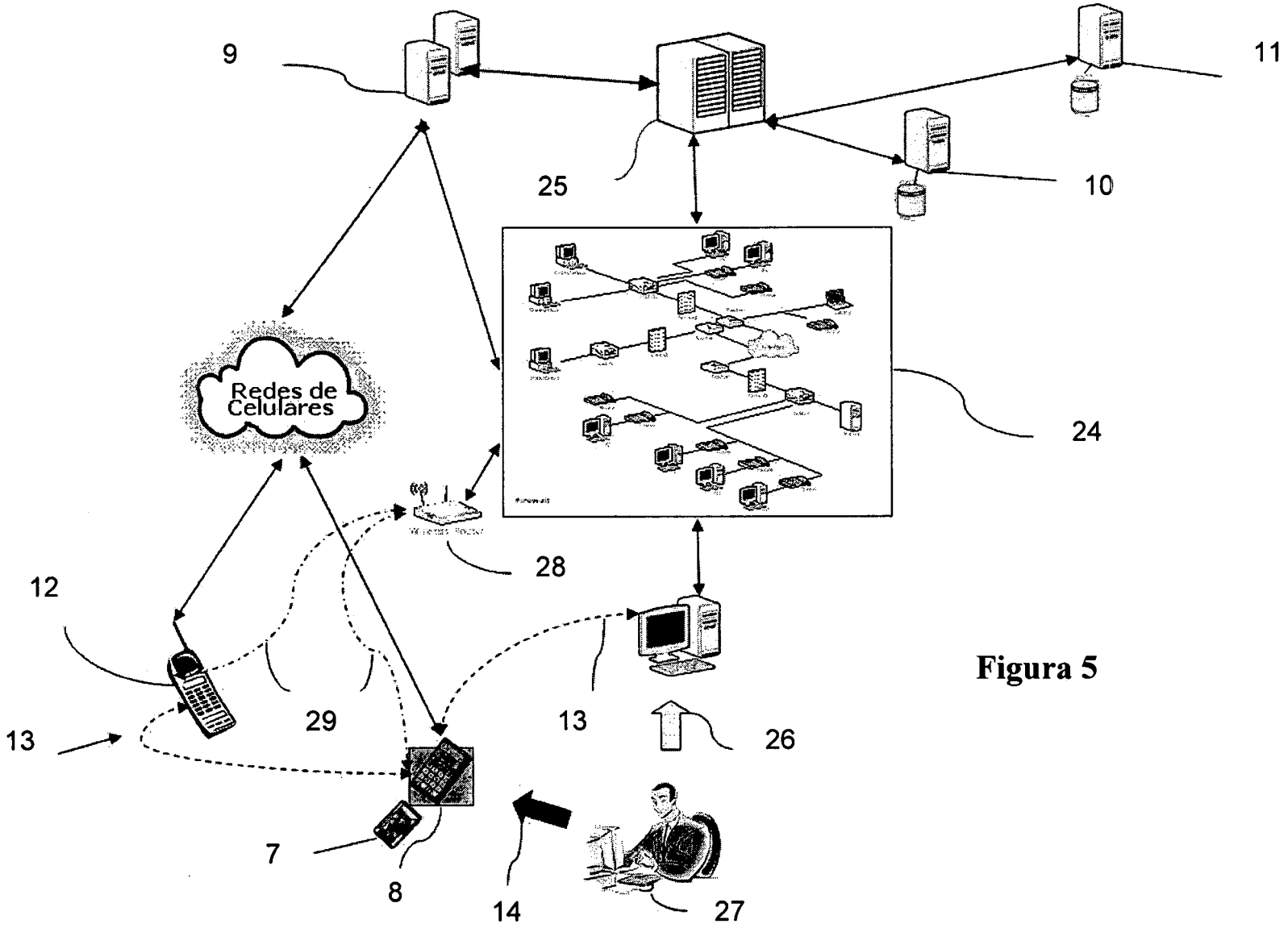


Figura 5

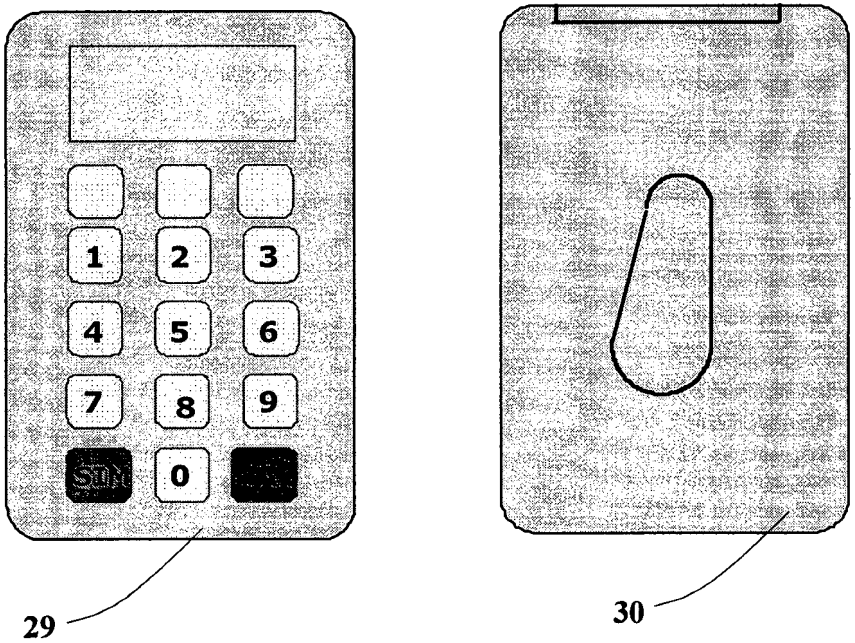


Figura 6

PI0802251-8

RESUMO

SISTEMA, MÉTODO E DISPOSITIVO PARA AUTENTICAÇÃO EM RELACIONAMENTOS POR MEIOS ELETRÔNICOS

A presente invenção situa-se no campo da Tecnologia da Informação, especificamente no campo da autenticação de usuários de sistemas mediante o uso de tecnologias de comunicação à distância, sem fio e refere-se a um sistema, um método e a dispositivo capaz de autenticar usuários e provedores de serviços centralizados, com segurança e de forma recíproca. Mais especificamente, o campo de aplicação da invenção é o dos métodos de gerenciamento de autenticação de pessoas, em seus relacionamentos através de meios eletrônicos digitais.