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

(21) PI 0715284-1 A2

* B R P I 0 7 1 5 2 8 4 A 2 *

(22) Data de Depósito: 14/09/2007
(43) Data da Publicação: 16/07/2013
(RPI 2219)

(51) Int.Cl.:
G06Q 20/00

(54) Título: SISTEMA E MÉTODO PARA VERIFICAR A IDENTIDADE DE USUÁRIO EM TRANSAÇÕES ELETRÔNICAS

(30) Prioridade Unionista: 29/09/2006 US 11/537,461

(73) Titular(es): DAN SCAMMELL

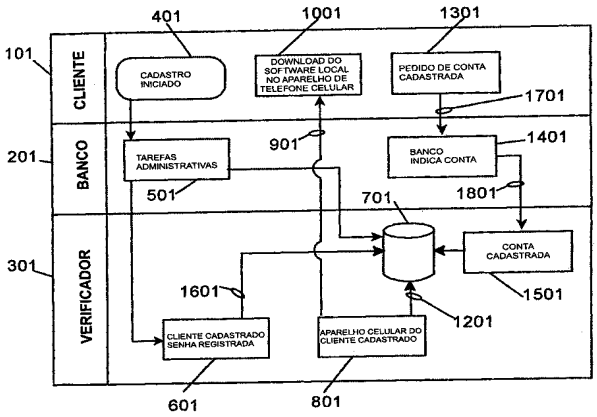
(72) Inventor(es): STEWART GOODIN

(74) Procurador(es): Miranda Lynch Kneblewki S/C Ltda

(86) Pedido Internacional: PCT CA2007001639 de 14/09/2007

(87) Publicação Internacional: WO 2008/037062de 03/04/2008

(57) Resumo: SISTEMA E MÉTODO PARA VERIFICAR A IDENTIDADE DE USUÁRIO EM TRANSAÇÕES ELETRÔNICAS. A invenção diz respeito a um método e sistema para verificar a identidade de usuário no curso de transação eletrônica. A invenção provê um processo e sistema para bloquear uma conta até que um verificador conclua o processo de verificação de identidade para verificar a identidade da pessoa que inicia a transação. O processo compreende o pré-cadastro da pessoa e do dispositivo de comunicação pessoal. Opcionalmente, uma ou mais contas são cadastradas pela indicação de contas de modo que as trasações sejam sujeitas à verificação da identidade de usuário. No momento que a transação é iniciada, o verificador envia um pedido de verificação de identificação (PVI) ao dispositivo de comunicação portátil da pessoa que inicia a transação eletrônica. A seguir, a pessoa verifica sua identidade fornecendo um identificador seguro em resposta ao PVI. Opcionalmente, é solicitada à pessoa a autorização da transação antes da transação ser aceita.



SISTEMA E MÉTODO PARA VERIFICAR A IDENTIDADE DE USUÁRIO EM TRANSAÇÕES ELETRÔNICAS

HISTÓRICO DA INVENÇÃO

CAMPO DA INVENÇÃO

A invenção diz respeito a sistemas e métodos para verificar a identidade de usuários que iniciam transações eletrônicas.

DEFINIÇÕES

As seguintes definições são fornecidas para estabelecer o escopo e significado de determinados termos usados na revelação e nas reivindicações. Os exemplos usados nas definições ilustram e esclarecem as definições e não limitam a definição ou o escopo do termo. Os termos definidos nesta invenção incluem o plural e singular, bem como congêneres gramaticais e alternativas.

"Transação eletrônica" significa o pedido de bens ou serviços que inclui, quando aplicável, uma oferta de pagamento pelos bens ou serviços e uma resposta ao pedido, em que alguma etapa do pedido e/ou resposta envolve a comunicação eletrônica de informações. O termo "Serviços" inclui amplamente qualquer ação solicitada. "Transação eletrônica", conforme a aplicação do termo nesta invenção aplica-se a transações envolvendo bens, serviços/ações de qualquer espécie virtual. Embora transações de cartão de crédito sejam transações eletrônicas de exemplo comum usado aqui para descrever as configurações preferidas da invenção, outros exemplos de transações eletrônicas que se enquadram no escopo da invenção incluem, a título de exemplo, o fornecimento de acesso a um espaço seguro, como uma sala, veículo, prédio, caixa de depósito ou outra unidade de armazenamento; a provisão de crédito seguro e não seguro; a prestação de serviços

bancários ou outros serviços financeiros; o fornecimento de permissão para cruzar fronteiras.

"Pessoa" significa pessoa física ou jurídica e suas combinações.

"Usuário", "cliente" e "fonte pagadora" referem-se alternadamente a pessoas que procuram obter bens ou serviços por transação eletrônica. "Cliente" e "fonte pagadora" referem-se preferencialmente a transações de varejo; "usuário" refere-se preferencialmente a transações de não varejo. "Computador de acesso" refere-se a computador de acesso por usuário para executar várias etapas do método da invenção.

"Fornecedor", conforme amplamente definido na revelação e nas reivindicações, inclui sistemas e subsistemas de pessoa física e jurídica que fornecem bens e serviços a um usuário por transação eletrônica, que inclui serviços derivativos ou implícitos prestados por terceiros. Em uma transação eletrônica por cartão de crédito, por exemplo, o termo "fornecedor" inclui vendedor de varejo, comerciante ou outro recebedor que fornece e recebe por bens ou serviços "vendidos", e também o subsistema de várias entidades bancárias terceiras que fornecem os serviços derivativos de adiantar o crédito solicitado pelo cliente quando este oferecer seu cartão de crédito.

"Banco" refere-se funcionalmente a uma entidade ou grupo de entidades que interagem na prestação de serviços financeiros relacionados a uma transação eletrônica, que inclui a concessão de crédito, transferência de recursos e a gestão de contas financeiras. O termo também inclui sistemas e subsistemas das entidades que interagem na prestação de serviços financeiros como, por exemplo, associações de transferência de pagamento ou administradoras de cartão de crédito tais como VISA® e MasterCard®. Portanto, o termo refere-se a um conjunto de funções executadas por instituições financeiras no processamento de transações eletrônicas.

"Verificador" refere-se funcionalmente a uma entidade que presta serviços de verificação de identidade como parte de uma transação eletrônica. O verificador pressupõe a existência independente de partes que conduzem a transação, como em uma empresa comissionada que presta serviços de verificação de identidade. Alternativamente, a função de verificador pode consistir em um fornecedor de bens e serviços, um banco, administradora de cartão de crédito ou outra parte integrante da transação. Nas figuras e revelações feitas a seguir, a representação do verificador separadamente do fornecedor não implica que as entidades são necessariamente distintas, e sim ilustra que as funções do verificador são distintas das funções do banco e do fornecedor. Da mesma forma, o termo "computador verificador" refere-se funcionalmente a um computador, servidor ou rede que oferece a funcionalidade de verificação da presente invenção, independentemente da sua localização física ou de seu operador ou controlador. Um passo a ser tomado por um "computador verificador" deve ser considerado equivalente a um passo a ser tomado pelo "verificador" e vice-versa.

"Banco de dados verificador" refere-se a uma compilação de registros de usuário que são acessíveis por um computador verificador.

"Dispositivo de comunicação" inclui amplamente dispositivos de comunicação de qualquer natureza conectados a um sistema de comunicação, por meio do qual o sistema de comunicação de uma primeira pessoa ou aplicativo de software se comunica com uma segunda pessoa ou aplicativo de software. O termo inclui computadores conectados à Internet, telefones conectados a sistemas de telefonia fixa e telefones celulares e outras conexões em sistemas *wireless* (sem fio). "Dispositivo de comunicação pessoal" refere-se a um dispositivo de comunicação suficientemente pequeno e móvel a ser realizada por usuário, incluindo telefones celulares, PDA's, computadores *wireless*, aparelhos

Blackberry®, Bluetooth®, *pagers*, *beepers* e demais aparelhos de uso pessoal com dispositivo de transmissão sem fio.

"Software local" refere-se a um software com acesso por computador de usuário na realização da invenção. Software local "executando" uma etapa refere-se ao computador de usuário que executa a função especificada, segundo as instruções do software local.

"Número de acesso de usuário" - representação de dados alfanuméricos ou outros dados usados para acessar um dispositivo de comunicação de usuário.

"Pedido de Verificação de Identidade (PVI)" - pedido eletrônico iniciado por um verificador e enviado a um usuário que solicita a verificação da identidade de usuário.

"Identificador seguro" - um termo genérico para representação de dados segura usada na identificação de uma pessoa. O termo inclui, a título de exemplo, representações alfanuméricas seguras, senhas, códigos, números protegidos, PINs, códigos de acesso ou representações digitais de recursos biométricos que podem ser utilizados na identificação de pessoa ou entidade. Nos exemplos fornecidos, o uso de "senha" não exclui outros tipos de identificadores seguros, sendo, de fato, representativo do gênero. O termo "suposto identificador seguro" refere-se a um identificador seguro que é oferecido em resposta a um PVI. "Identificador seguro" refere-se a um identificador seguro válido conhecido com o qual se compara um suposto identificador seguro.

ESTADO DA TÉCNICA

A presente invenção soluciona o complexo problema da forma de verificação da identidade de uma pessoa que inicia uma transação eletrônica.

A transação eletrônica comum é do tipo iniciado por um cliente que insere um cartão de crédito em uma leitora de cartão de ponto de venda, fazendo um pedido primário para a compra de bens ou serviços. Esse pedido inclui um pedido implícito ou derivativo

para concessão de crédito ao cliente ou pedido de transferência de recursos da conta do consumidor para a conta de um comerciante ou prestador de serviço. Outros exemplos de solicitações eletrônicas incluem o uso de um cartão codificado ou recursos biométricos para obter acesso a uma sala ou prédio; o uso de um cartão codificado em caixas eletrônicos (ATMs); e transações comerciais on-line nas quais o número de uma conta é fornecido através da Internet a um comerciante on-line.

Embora essas solicitações eletrônicas sejam extremamente convenientes para todas as partes envolvidas, são ignoradas ou desconsideradas muitas fraudes e problemas de segurança apresentados pelas transações eletrônicas. Consequentemente, tem se tornado um grande problema a identificação de furto, que ocorre quando as informações pessoais e financeiras de uma pessoa são obtidas e utilizadas por pessoas não autorizadas. Em 2004, segundo estimativas da Comissão Federal de Comércio dos EUA, os prejuízos anuais para empresas decorrentes de furto de Identidade foram em torno de $50 bilhões. O custo para pessoas físicas foi em torno de $5 bilhões. Em 2000, as administradoras de cartão de crédito VISA® e MasterCard® divulgaram prejuízos relacionados a fraudes de $114 milhões, com um aumento anual de aproximadamente 10% em relação aos últimos quatro anos. Os prejuízos relacionados a furto de identidade no Canadá subiram 2,6 vezes em apenas 1 ano – de $8,5 milhões para $21,5 milhões em 2002 até 2003.

Durante aproximadamente o mesmo período em que houve o aumento no uso e uso indevido de tecnologia de transação eletrônica, houve ainda uma taxa maior de aumento no uso de dispositivos de comunicação portáteis, mais especificamente aparelhos de telefone celular. Nos 33 anos após a primeira ligação *wireless* de Martin Cooper de um aparelho de telefone celular portátil em 1973, o número de aparelhos de telefone celular em uso aumentou para mais de 2,5 bilhões no mundo inteiro – um número que atinge atualmente

50% de toda a população humana. Em muitos países, o número de contratação de serviços de telefonia celular atinge de maneira significativa 100% da população. Nenhuma outra tecnologia eletrônica é tão ubíqua ou universal como as comunicações portáteis; consequentemente, nenhuma outra tecnologia eletrônica está melhor posicionada para ser explorada na melhoria da segurança.

Houve uma série de tentativas de abordagens para solucionar problemas de segurança relacionados a transações eletrônicas pela combinação de tecnologia de comunicações eletrônicas e identificadores de segurança. Por exemplo, a Patente dos EUA 6.954.740 de Talker revela um sistema no qual as assinaturas de cartão de crédito e as transações em cheque são verificadas pela transmissão do PIN com o pedido de transação. A Patente dos EUA 6.868.391 de Hultgren revela um sistema no qual um cliente que inicia uma transação eletrônica liga para uma entidade de verificação de um ponto de venda (POS) e informa o número PIN, o qual é comparado pela entidade com um número PIN validamente conhecido. Enquanto esses sistemas oferecem melhorias valiosas de segurança em transações eletrônicas, em geral eles não oferecem facilidade na sua implementação, em especial do ponto de vista do cliente. Por exemplo, Hultgren pede ao cliente que entre em contato com a entidade de verificação, a qual necessita saber e inserir o número do telefone do verificador e a seguir aguardar a resposta da ligação e o processamento.

São necessários um método e sistema para verificar a identidade de um usuário durante uma transação eletrônica, em que o método ofereça facilidade na implementação, uso e seja substancialmente transparente ao usuário, e ainda flexível o suficiente para ser utilizado em qualquer lugar do mundo sem que o usuário tenha a necessidade de realizar ou iniciar ligações para uma entidade de verificação.

BREVE RESUMO DA INVENÇÃO

A presente invenção refere-se a um método e sistema de aplicação de tecnologia de comunicações portáteis na solução de problemas de fornecimento da verificação da identidade exata de usuário em transações eletrônicas. Enquanto o método ofereça muitas aplicações, configurações e adornos, algumas das quais são reveladas a seguir, o método básico compreende um prestador que oferece bens ou serviços, um usuário ou cliente que procura adquirir bens ou serviços por meio de transação eletrônica, e um verificador que atua no bloqueio de operação, a menos que a identidade do solicitante seja adequadamente verificada.

Com relação ao método da invenção, um usuário e o dispositivo de comunicações do usuário são pré-cadastrados em um programa de verificação administrado pelo banco, verificador ou outra entidade. Uma ou mais das contas do usuário também são pré-cadastradas no programa de verificação. Estes pré-cadastros compreendem a inserção de informações em banco de dados verificador e o *download* do software local para um computador de usuário integrado ou de outra forma conectado ao dispositivo de comunicação de usuário. O pré-cadastro da conta pode ser simplesmente o ajuste de um indicador em um registro de banco de dados, de tal modo que indique se as tentativas de acesso àquela conta devem ser submetidas às etapas de verificação de usuário reveladas aqui, ou podem incluir a inserção do número da conta e dados de autorização de acesso no banco de dados verificador para que o verificador possa atuar como *proxy* para o usuário no acesso da conta. Opcionalmente, o pré-cadastro da conta implica de forma adicional ou alternativamente o ajuste de um indicador em registro de banco de dados, que indica se as tentativas de acesso da conta devem ou não ser submetidas às etapas de autorização da transação reveladas aqui.

Como resultado do processo de pré-cadastro, as informações armazenadas em banco de dados verificador são acessíveis por computador verificador, que é adaptado para redigir e recuperar informações do banco de dados. O registro do usuário no banco de dados verificador inclui um identificador seguro para o usuário e o número de acesso de usuário do dispositivo de comunicação do usuário. Nas aplicações da invenção relacionadas a transações financeiras, o banco de dados também contém os vários indicadores que determinam que contas devem ser submetidas à verificação de identidade e autorização da transação.

Quando o usuário (ou qualquer pessoa) efetua uma tentativa de acesso a uma conta protegida por indicação, é enviado um sinal do comerciante para o computador verificador, que tenta abrir um *link* de comunicação com o dispositivo de comunicação do usuário utilizando o número de acesso de usuário armazenado no banco de dados verificador. Uma vez aberto o *link* de comunicação ao dispositivo de comunicação do usuário, o computador verificador envia um pedido de verificação de identificação codificado ("PVI") ao dispositivo de comunicação do usuário. O computador do usuário, que é conectado ao dispositivo de comunicação e a um dispositivo input/output ("I/O"), é adaptado para a intercepção do PVI e seu processamento, incluindo a descodificação do PVI e sua exibição no dispositivo I/O, que aceita o *input* (entrada de dados) do usuário e exibe o *output* (saída de dados) ao usuário. O computador do usuário também é adaptado para adquirir o *input* do usuário e enviar uma resposta ao PVI com base no *input* do usuário. O verdadeiro usuário em poder do dispositivo de comunicação de usuário responderá ao PVI pela introdução de um suposto identificador seguro (correto) ao dispositivo I/O. Em uma configuração, o suposto identificador seguro é codificado pelo software local no dispositivo de comunicação do usuário e enviado ao computador verificador sobre a linha

de comunicação aberta. O computador verificador recebe o suposto identificador seguro, descodifica-o e realiza a comparação do identificador seguro recuperado a partir do banco de dados. Se o suposto identificador seguro e o verdadeiro identificador equivalerem após a comparação, o computador verificador removerá o bloqueio da transação para que a transação seja processada até ser concluída.

Opcionalmente, o método da invenção inclui as etapas adicionais do usuário que autoriza a transação eletrônica específica imediatamente, cuja etapa é referida aqui como "autorização de transação" para distingui-la da etapa de verificação da identidade do usuário. Dependendo da aplicação específica da invenção, esta etapa de autorização pode ser concluída simultaneamente à etapa de verificação da identidade, ou separadamente como, por exemplo, quando o computador verificador enviar um segundo pedido codificado – chamado pedido de autorização de transação – ao dispositivo de comunicação pessoal do usuário. O pedido de autorização de transação é exibido no dispositivo I/O do dispositivo de comunicação, de modo que o usuário possa verificar o valor da transação, o comerciante e outros detalhes. Para autorizar ou negar a transação, o usuário deve enviar uma resposta ao pedido de autorização de transação apenas pressionando a tecla "return". Se a resposta for -autorizar transação-, a seguir o bloqueio é removido e a transação se processa. Em algumas aplicações, a identidade do usuário é verificada antes do usuário autorizar a transação. Em outras aplicações, é mais eficaz realizar a etapa de autorização da transação antes da verificação da identidade.

O efeito do método é explorar a combinação ou o número do telefone celular do usuário e o identificador seguro para montar barreiras de segurança adicionais em transações eletrônicas. Em caso de roubo ou apropriação indevida de cartão de crédito de usuário, qualquer tentativa pelo ladrão de iniciar uma transação com esse cartão resultará

em uma notificação imediata do usuário enviada do computador verificador do PVI ao número de telefone celular do usuário. O ladrão que tentar utilizar o cartão não sabe ainda que fez com o telefone celular da vítima tocasse, desse modo informando ao usuário que alguém está tentando iniciar uma transação com o seu cartão. Mesmo em caso de roubo ou apropriação indevida do telefone celular e cartão de crédito do usuário, quaisquer transações eletrônicas iniciadas pelo ladrão com esse cartão de crédito falharão, a menos que o ladrão saiba o identificador seguro do usuário. Além disso, embora a função de localização por GPS agora seja universal em aparelhos de telefone celular, qualquer tentativa de pedido de verificação falso aciona automaticamente um sistema de rastreamento para localizar imediatamente o aparelho de telefone celular roubado.

Várias configurações do método aumentam sua utilidade de maneira significativa. Por exemplo, o método pode ser adaptado de modo a permitir ao verificador o controle de transações eletrônicas iniciadas por uma parte em nome de uma segunda parte. Por exemplo, se um funcionário carregar um cartão de crédito da empresa, o computador verificador enviará o PVI ao número do telefone celular do funcionário no ponto de venda. Após a verificação da identidade do funcionário, o computador verificador enviará o pedido de autorização de transação à linha fixa ou ao número de telefone celular do empregador, informando que a transação foi solicitada e oferecendo a opção de autorizar ou negar autorização antes da transação ser concluída.

Em outra configuração opcional, o verificador emitirá seu próprio cartão de transação *proxy* ao usuário, que é utilizado para iniciar a verificação de identificação de usuário e a seguir aprovar a transação através da conta de cartão de crédito do usuário, evitando assim a necessidade do usuário em carregar o cartão de crédito e permitindo que informações sejam transmitidas entre o banco comerciante e o verificador diretamente sem

o envolvimento do banco do usuário. Desse modo, o verificador atua como *gateway* para uma ou mais contas do usuário, sendo que o *gate* (acesso) somente pode ser liberado se o usuário digitar um identificador seguro correto ao dispositivo de comunicação do usuário em resposta a um PVI a partir do verificador.

BREVE DESCRIÇÃO DAS FIGURAS

O objeto acima e outros objetos, recursos e vantagens da invenção ficarão mais evidentes a partir da seguinte descrição com relação aos desenhos anexos, nos quais:

A FIGURA 1 se trata de um diagrama que mostra as etapas de pré-cadastro do método da invenção.

A FIGURA 2 se trata de um fluxograma do método da invenção aplicado a uma transação eletrônica por cartão de crédito.

A FIGURA 3 se trata de um diagrama dos vários componentes do sistema e suas interações.

A FIGURA 4 se trata de um fluxograma do método da invenção aplicado a uma transação eletrônica para fornecer acesso a um ambiente.

A FIGURA 5 se trata de um fluxograma do método da invenção com base em um cartão de transação *proxy* emitido pelo verificador.

DESCRIÇÃO DETALHADA DAS CONFIGURAÇÕES PREFERIDAS

O MÉTODO – FASE I: PRÉ-CADASTRO

Uma vez que o método da invenção tem um grande potencial e flexibilidade para ser usado em uma ampla variedade de situações, não é possível divulgar todas as aplicações possíveis. Encontra-se aqui uma configuração relativamente simples do método e sistema da invenção que representa a melhor forma que conheço atualmente para a prática da invenção. Assim, são revelados variações e adornos para ilustrar a flexibilidade

da invenção. A partir dessas revelações, um especialista estará apto para praticar a invenção e aplicá-la para obter muitas finalidades úteis e diversas.

O exemplo ilustrado nas FIGS 1-3 mostra como uma pessoa, aqui referida como "cliente" ou "fonte pagadora", usa a invenção para proteger uma conta de cartão de crédito, por exemplo, uma conta administrada por uma associação de transferência de pagamento como a VISA® e MasterCard®. Conforme mencionado acima, tais entidades financeiras estão aqui referidas genérica e coletivamente como "banco". A apresentação do cliente do cartão de crédito ao vendedor de varejo, comerciante ou outro recebedor constitui ambos e oferece a opção de compra de bens/serviços e um pedido de concessão de crédito da conta do cliente para o pagamento destes. A FIG 1 ilustra o processo de pré-cadastro do usuário, seu dispositivo de comunicação, e suas contas em um programa de verificação. A FIG 2 ilustra o processo do uso da invenção para verificar a identidade do usuário durante a transação eletrônica.

Referindo-se primeiro à FIG 1, que estabelece a configuração preferida da forma como o cliente 101, banco 201 e verificador 301 interagem para realizar o processo de pré-cadastro. Na configuração preferida, o verificador 301 fornece software e um servidor ao banco 201. O banco tem então o controle físico do computador verificador no sentido de que o software de verificação e hardware relacionado estão fisicamente nas instalações do banco e são operados pelo mesmo. O processo é iniciado 401 pelo cliente que entra em contato com o banco em busca dos serviços de verificação de identidade. O banco conclui tarefas administrativas necessárias 501, tais como o registro do pedido, verificando a identidade do cliente, e similares. Os dados resultantes são atualizados em um banco de dados 701.

O cliente é pré-cadastrado no programa de verificação fornecendo 601 os dados solicitados ao verificador, incluindo informações de identidade e informações que podem ser usadas para recuperar eletronicamente uma senha perdida. Uma senha é fornecida ao cliente. Todas essas informações estão escritas 1601 em um registro para o cliente no banco de dados verificador 701. Apesar de o banco de dados verificador e o banco de dados do banco estarem representados como uma única entidade na figura, entende-se que a configuração física dos bancos de dados pode ser implementada como banco de dados distintos operando em servidores distintos, conforme discutido em detalhes a seguir.

A próxima etapa consiste em pré-cadastrar um celular ou telefone móvel 801, a qual o cliente tem acesso. Primeiro, o usuário fornece ao verificador um número de acesso de usuário que pode ser usado para abrir o link de comunicação com o telefone móvel do cliente, e o verificador armazena 1201 o número de acesso de usuário no banco de dados 701. O verificador então faz uma ligação 901 para o telefone móvel usando o número de acesso de usuário fornecido. O verificador então faz o *download* 1001 do software local através deste link de comunicação aberto para o computador de usuário integrado no telefone do usuário. Este software local é solicitado durante o processo de verificação,conforme descrito a seguir. Nota-se que o computador de usuário pode ser um computador separado, ou um computador integrado em qualquer dos tipos de dispositivos de comunicação, dependendo da implementação específica da invenção. Neste momento, o verificador pode opcionalmente adquirir do telefone móvel uma informação de identificação de dispositivo que pode ser utilizada para identificar um telefone específico. Em configurações em que o computador de usuário for um laptop, PDA, ou outro computador que não um dispositivo de comunicação móvel, o número serial do CPU do

computador pode ser adquirido pelo verificador. Estes dados de dispositivo de comunicação são então escritos 1201 no banco de dados 701.

A fase final do pré-cadastro é o pré-cadastro 1301 de contas específicas a serem protegidas pelo serviço. O cliente determina qual conta deseja proteger pelo serviço de verificação de identidade de usuário. As transações com estas contas serão bloqueadas em seguida até que o verificador examine a identidade do cliente durante cada transação individual. O cliente 1701 determina a conta ou contas que deverão ser cadastradas. O banco sinaliza as contas designadas 1401 e notifica 1801 o verificador. Este pré-cadastra as contas 1501 realizando a inscrição adequada no banco de dados 701. De forma alternativa, o banco pode manter a sinalização de verificação em seu banco de dados e então notificar o serviço de verificação a cada tentativa de acesso à conta sinalizada. O modo mais eficiente de sinalizar as contas será determinado pela aplicação específica e pelos recursos das partes. A questão principal refere-se ao fato de que as transações usando as contas designadas são bloqueadas do procedimento até que o verificador verifique a identidade do cliente.

No exemplo apresentado, apenas uma pessoa, o cliente, inicia as transações eletrônicas. No entanto, se houver possíveis usuários múltiplos da conta, seus dados de identidade e números de celular também serão fornecidos ao verificador em 601 e registrados no banco de dados 701.

O processo de pré-cadastro já mencionado pode ser fácil e convenientemente iniciado *online* pelo cliente ou através de telefonia fixa e/ou sistemas de comunicação *wireless*. A etapa de *download* de software 1001 é realizada de forma mais conveniente pelo verificador pela abertura do link de comunicação com o celular do cliente. O processo inteiro de pré-cadastro é concluído em questão de minutos. Mesmo se o verificador for

uma entidade distinta do banco, não é necessário que o processo de pré-cadastro envolva diretamente o verificador. O banco pode realizar o processo de pré-cadastro, caso em que o verificador permanece visível ao cliente. Por exemplo, uma companhia de verificação de identidade pode contratar um banco para fornecê-lo software e servidores necessários para a realização do método da invenção. Se o banco então administra o processo de verificação de identidade, o banco estaria realizando a função do "banco" e do "verificador", conforme os termos são aqui utilizados.

É necessário enfatizar que a seqüência do processo de pré-cadastro não é fixo e é acessível em relação à flexibilidade. Por exemplo, a sinalização da conta 1401 pode ser realizada assim que o cliente solicitar pré-cadastro 401.

O MÉTODO – FASE II: VERIFICAÇÃO DE IDENTIDADE DE CLIENTE

A FIG 2 mostra uma seqüência de etapas, pelas quais o cliente 101 deseja usar a conta pré-cadastrada com o verificador 301 para obter uma concessão do crédito do banco 201 como parte da transação para a compra de bens/serviços do vendedor de varejo 102.

O cliente inicia uma transação eletrônica 202 ao apresentar seu cartão ao vendedor de varejo 102. O cartão é engolido através de um dispositivo de leitura de cartão, enviando então um comunicado eletrônico 302 ao banco 201, por exemplo, através de uma rede de telefone público (PSTN) como é realizada atualmente. O banco consulta 502 informações de conta do cliente em seu banco de dados para ver se há crédito ou fundos suficientes para completar a transação. Se houver um problema, a transação pode ser cancelada e o vendedor de varejo notificado 2902, senão o banco consultará o banco de dados para verificar se a conta do cliente está sinalizada 402.

Se a conta não estiver sinalizada 602, a transação ignora a verificação de identificação de usuário e dá continuidade aos procedimentos normais de autorização 2502.

No presente exemplo, o cliente pré-cadastrou a conta para os serviços de verificação de acordo com a FIG 1, e então a conta foi sinalizada. Consequentemente, a transação é bloqueada 3002 até a verificação da identidade do cliente. Uma mensagem é enviada do banco ao verificador para iniciar o processo de verificação de identidade 702. O verificador recupera do seu banco de dados o número de acesso de usuário para o telefone móvel do cliente e abre um link de comunicação 1002 com o telefone móvel do cliente, usando, por exemplo, um protocolo e rede *wireless*. Um sinal de interrogação é enviado para o telefone móvel do cliente, cujo sinal é recebido pelo seu telefone móvel e alerta o software local 802 que foi baixado no telefone durante o pré-cadastro 1001 (Ver FIG 1). Se o telefone estiver desligado ou não responder, então o processo de verificação falha e a transação é cancelada por omissão, sendo assim bloqueada 3002. De maneira similar, se em algum momento antes da conclusão do processo de verificação de identidade a ligação "cair", ou se o link de comunicação não estiver funcionando, como resultado de um tempo esgotado, por exemplo, a transação não será concluída pelo mesmo motivo.

Se o telefone móvel do cliente for atendido, o computador de usuário automaticamente busca informações de transação do computador verificador 1202, e este responde 1102 enviando 1402 as informações de transação ao computador de usuário, que inclui um Pedido de Verificação de Identidade (PVI). O computador de usuário recebe o PVI e o formata para a exibição no dispositivo de input/output do usuário.

O formato do PVI dependerá das tecnologias disponíveis e preferenciais e do tipo de dispositivo de comunicação portátil, mas atualmente, na maioria das áreas, é preferível uma mensagem de texto. O PVI é, em sua essência, um convite ao cliente para a inserção da senha.

O computador verificador pode opcionalmente adquirir do telefone do usuário um número de identificação de dispositivo e compará-lo ao número de identificação de dispositivo gravado no banco de dados para garantir que o dispositivo de comunicação apropriado tenha sido contatado. Esta etapa pode ser realizada de forma conveniente quando o computador de usuário busca informações de transação 1202.

O cliente digita uma suposta senha 1802 no dispositivo de input/output do telefone móvel, cuja senha é formatada pelo computador de usuário e enviada 1602 ao computador verificador como resposta ao PVI. O suposto identificador seguro é recebido pelo computador verificador e comparado 1502 com a senha que este recupera do banco de dados 701 (Ver a FIG 1).

Se a suposta senha não conferir com a senha correta, uma mensagem de "confirmação impossível" é enviada 1702 ao computador de usuário solicitando uma nova tentativa pelo cliente. Após uma série de tentativas fracassadas, a transação é cancelada e o banco é notificado 1302. Neste momento, o banco, o vendedor de varejo e/ou verificador podem adotar uma série de medidas protetoras ou corretivas, como ligar para a telefonia fixa do cliente para informá-lo a respeito da transação cancelada, entrando em contato com a polícia, bloqueando a conta de outras tentativas de transação, ou confiscando o cartão. Dependendo da aplicação específica, se o link de comunicação falhar antes da verificação da suposta senha, o caso pode ser tratado como uma violação de segurança ou a transação pode ser simplesmente cancelada com um aviso adequado ao banco e/ou vendedor de varejo.

Se a suposta senha não conferir com a senha correta, um sinal 902 de "identidade verificada" é gerado, o bloqueio 3002 da conta é revogado e a transação é autorizada, e

uma notificação ao banco 2402 e ao comerciante 2202 é enviada, bem como uma confirmação ao telefone móvel do cliente 2602.

As transmissões entre o computador de usuário e computador verificador são codificadas. O software local automaticamente descodifica o tráfego de entrada e codifica o tráfego de saída sem qualquer entrada do cliente. O cliente também não precisa saber o número do telefone do verificador ou discar qualquer número, uma vez que a telefonia fixa é aberta pela ligação do verificador ao telefone do cliente, e o software local no telefone do cliente automaticamente identifica a mensagem recebida do verificador, mostra a mensagem no dispositivo de input/output do telefone, formata a informação de saída e a transmite ao verificador.

O MÉTODO – FASE III: AUTORIZAÇÃO DE TRANSAÇÃO E CONCLUSÃO

No ponto 2502 da FIG 2 a identidade do cliente foi verificada, e a transação pode ser completada. Em muitas configurações da invenção, o PVI inclui, implícita ou explicitamente, uma solicitação de autorização da transação, sendo que tal autorização é concedida pelo identificador de segurança do cliente. Em outras configurações, é desejável que o cliente autorize a transação em uma outra etapa. Isso é realizado pelo computador verificador que transmite ao computador de usuário uma solicitação de autorização, esperando a resposta adequada do cliente. Se o cliente indica que não autorizará a transação, ou se a ligação for finalizada, a transação é cancelada.

Nas etapas 2402 e 2302, o banco é notificado do resultado do procedimento de verificação de identidade e de qualquer etapa de autorização de transação opcional. Na etapa 2202, o vendedor de varejo também é notificado da situação de transação, e na etapa 2602 o cliente é notificado, o que pode ocorrer imediatamente através do telefone móvel

do cliente, ou em algum momento no futuro, como por exemplo através do extrato mensal do cliente. Se a transação for aprovada, é então concluída.

O SISTEMA

O sistema da invenção compreende componentes de hardware e software em uma combinação nova e não óbvia que realiza o método resumido no exemplo acima. Devido a enorme flexibilidade e larga aplicabilidade da invenção, não é possível descrever, ou mesmo antecipar, todas as formas ou configurações que a invenção pode assumir. Encontra-se aqui uma configuração um tanto elementar do sistema sobre o qual o especialista na técnica poderá fazer muitas alterações óbvias e aperfeiçoamentos dentro no âmbito da revelação.

A FIG 3 apresenta um resumo diagramado dos componentes primários da invenção e como eles podem interagir, usando o exemplo da transação de cartão de crédito.

O cliente 103 possui um dispositivo de comunicação como um celular 2303 ou outro dispositivo de comunicação móvel que compreende um transceptor *wireless* 403, o software local é ativado pelo computador de usuário 603, e um dispositivo de input/output 503 para fazer a interface da comunicação móvel com o cliente. O computador usuário é acoplado ao dispositivo de input/output e ao transceptor e é adaptado em virtude do software local para exibir o PVI no dispositivo de input/output, formatar a resposta do cliente ao PVI como dados de saída e enviá-los através do celular do transceptor ao verificador.

O computador de usuário do dispositivo de comunicação 2303 é adaptado para possibilitar o acesso ao link de comunicação 1503, que é um link *wireless* com o primeiro dispositivo de comunicação 2403 do verificador 203. Este primeiro dispositivo de comunicação do verificador é acoplado ao computador verificador 903. O computador

verificador é adaptado por software para possibilitar o acesso ao banco de dados verificador 703, de forma que o computador verificador possa ler os dados a partir e escrever dados no banco de dados verificador, incluindo dados recebidos e transmitidos pelo primeiro dispositivo de comunicação do verificador 2403 e o segundo dispositivo de comunicação do verificador 803.

O segundo dispositivo de comunicação do verificador 803 é adaptado para comunicar-se com o dispositivo de comunicação do banco/fornecedor 1103 através do link de comunicação 1803. Este link pode ser implementado como um link *wireless* ou uma rede de telefonia fixa como PSTN. Embora seja tecnicamente possível combinar as primeiras e segundas funções de transceptor dos dispositivos de comunicação do verificador, a flexibilidade e a velocidade de comunicação aperfeiçoada da separação dessas funções faz com que essa abordagem seja preferível, quando a tecnologia disponível atualmente é usada.

Dependendo da implementação, tanto o computador de usuário quanto o computador verificador, ou ambos, estão adaptados para receber como primeira entrada um identificador seguro recuperado do banco de dados 703, para receber como segunda entrada uma entrada de um suposto identificador seguro, através do dispositivo de input/output do cliente 503, para comparar a primeira com a segunda entrada, e para produzir uma saída de confirmação que indica se a primeira entrada confere com a segunda. Se não houver uma combinação, a transação é bloqueada, ou assim permanece, do procedimento para a conclusão.

O banco/fornecedor 303 controla o software de acesso às contas operadas pelo computador banco 1203 através do qual o banco de dados da conta 1003 é acessado para dados de conta de leitura e registro. Nota-se que em muitas aplicações da invenção o

banco/fornecedor fornece e administra os serviços de verificação de identidade. Em tais casos, o banco de dados 703 e banco de dados 1003 podem ser fisicamente os mesmo, funcionando em um ou vários servidores. Além disso, nota-se que a entidade 303é designada como "Banco/Fornecedor" na figura para indicar explicitamente que existem aplicações não financeiras da invenção, em que o fornecedor dos bens/serviços é parte da transação com ou sem o envolvimento de entidades de serviços financeiros. Um exemplo de aplicação não financeira da invenção é fornecido a seguir.

De acordo com a configuração preferida, o banco de dados de conta 1003 contém dados específicos de conta, tais como balanços, valores de linha de crédito, atividade e similares. É de particular interesse a sinalização em cada registro de conta que indica se a conta está sujeita a verificação de identidade do cliente ou não. O banco de dados da conta também contém dados específicos de cliente, tais como nomes, números de contato, endereços para cobrança e similares. O banco de dados de conta 1003 é acessível para banco e entidades de varejo com permissão para ativar o software de administração de conta 1203.

Em configurações da invenção em que o verificador é uma entidade distinta do banco, o banco de dados verificador 703 é acessível diretamente apenas pelo verificador 203. No entanto, sob o controle do computador verificador 903, informações circulam a partir e do banco/fornecedor 303 através do link de comunicação 1803. Da mesma forma, informações circulam entre o computador usuário 603 e o banco de dados verificador 703 através do link de comunicação 1503 e computador verificador 903. Finalmente, informações circulam 1703 do cliente 103 para o banco/fornecedor 303 na forma de pedido para iniciar uma transação eletrônica. Esta comunicação pode ser implementada de forma eletrônica ou não eletrônica.

Conforme notado acima, o método da invenção compreende etapas opcionais para a autorização da transação antes que seja concluída. Não são solicitados elementos físicos adicionais para a inclusão de etapas de autorização. Tudo o que é solicitado é que uma parte seja configurada no campo do registro do cliente no banco de dados verificador 703 ou no banco de dados do banco/fornecedor 1003. Alternativa ou adicionalmente, a exigência para a autorização pode ser gerada por um comerciante.

Uma vantagem particularmente útil do sistema revelado aqui é que não exige reprogramação dos computadores POS do comerciante, nem alterações de redes de comunicação existentes. Além disso, o sistema pode ser implementado com adaptações de software restritos ao computador verificador e ao computador usuário.

DETALHES, VARIAÇÕES E ADORNOS

Software local

A sofisticação e a amplitude da utilidade das várias configurações da invenção serão determinadas principalmente pelas funções que podem ser realizadas pelo computador usuário implementando software local que é baixado no dispositivo de comunicação. Dependendo da configuração, o software local inclui funções para: interceptar tráfego de entrada do computador verificador, descodificar/codificar informações circulando para dentro e para fora do dispositivo de comunicação, exibir informações para o dispositivo de input/output do dispositivo de comunicação do usuário, enviar respostas ao computador verificador, comparar identificadores seguros supostos e corretos e manter registros e relatórios da atividade de verificação.

O *download* do software local pode ser convenientemente realizado através de um link de comunicação entre o computador verificador e o computador usuário, mas muitas técnicas alternativas serão óbvias para os especialistas na técnica após compreenderem as

revelações aqui divulgadas. Por exemplo, o software pode ser baixado em um chip que é fornecido pelo verificador. Ou o dispositivo de comunicação pode ser um dispositivo dedicado e o software baixado no momento da fabricação.

Codificação

Muitas aplicações previsíveis da invenção envolvem a transmissão de informações financeiras, seguras e pessoais. Consequentemente, em tais aplicações é essencial que a informação sendo transmitida através de redes *wireless* seja codificada. As várias aplicações de software 603, 1203, 903 da invenção incorporam funcionalidade de codificação e descodificação de informações que circulam através dos respectivos transceptores. Protocolos de codificação e métodos comumente usados na área são aceitáveis para o uso. Após entender a presente revelação, um especialista comum na técnica estará apto para implementar regimes de codificação/descodificação para esta invenção sem experimentos indevidos.

Dispositivos de comunicação de usuário

Embora as configurações reveladas aqui pressupõem que a invenção será implementada em um aparelho de telefone celular ou móvel de um tipo utilizado para fins de comunicação normal, e não para verificar a identidade do cliente, a invenção pode ser facilmente implementada utilizando um dispositivo de comunicação dedicado fornecido pelo verificador ao cliente. Tal dispositivo contém toda a funcionalidade necessária dentro de um pacote de dimensão inferior a um *pager* ou *beeper*. Dependendo da implementação, a interface I/O com o cliente pode ser tanto LED ou *beeper* simples como único, ou tão complexo como o envio de mensagem de texto ou sintetizador de voz.

A invenção não é limitada pelo tipo de transceptor ou *links* de comunicação empregados por qualquer das entidades. Embora seja preferido o uso de comunicações

wireless em muitas aplicações, em especial para comunicações entre o verificador e o cliente, qualquer tecnologia de comunicação então existente ou a ser implementada no futuro que possa ser utilizada na realização das etapas da invenção é considerada no seu âmbito e no âmbito das reivindicações.

Será apreciado a partir desta revelação que, embora a configuração preferida empregue um *link* de comunicação wireless **1503** entre o cliente e o verificador, a invenção é flexível o suficiente a ponto de ser facilmente implementada sem o uso de dispositivos de comunicação móvel ou *wireless*. Por exemplo, o cliente pode ter uma localização geográfica fixa e função totalmente através de um sistema de comunicação de telefonia fixa. Nesses casos, a comunicação entre o verificador e o cliente pode ser efetuada por telefonia fixa ou através de conexão com a Internet utilizando, por exemplo, um protocolo do tipo mensagem instantânea, em que o computador do cliente atua como receptor/transmissor dos vários pedidos e informações requeridos para a execução da invenção.

Processamento de identificador seguro

Nos exemplos acima, o cliente transmite seu identificador seguro ao verificador em resposta ao PVI (Vide Fig. 1, **1602**). Esta é, obviamente, uma transmissão codificada. Uma técnica equivalente é tal que o computador verificador recupera o verdadeiro identificador seguro do cliente a partir do banco de dados verificador **703** e envia o verdadeiro identificador seguro ao computador do usuário **603** no momento que o PVI é transmitido. Esta também é uma transmissão codificada. O software local do computador do usuário compara o verdadeiro identificador seguro recebido do computador verificador com o suposto identificador seguro que o cliente introduz em resposta ao PVI. Se os dois identificadores se equivalerem, o computador do usuário envia automaticamente um sinal

de verificação ao computador verificador. Se os dois identificadores falharem, é enviado um sinal de falha de verificação. Independentemente se o verificador envia o verdadeiro identificador seguro ao cliente, ou se o cliente envia o suposto identificador seguro ao verificador, em qualquer caso o identificador seguro é codificado, transmitido e descodificado apenas uma vez para cada transação.

Uma terceira abordagem pode provar ser igualmente satisfatória em algumas aplicações da invenção. Nesta abordagem, é feito o *download* do verdadeiro identificador seguro ao número do telefone celular do cliente durante o processo de pré-cadastro. O verdadeiro identificador seguro então permanece inserido no software do aparelho de telefone. Quando o computador verificador enviar um PVI ao computador do usuário, o cliente introduz um suposto identificador seguro. O computador do usuário compara o dado do cliente com o verdadeiro identificador seguro inserido. Se há equivalência, o computador do usuário envia um sinal de verificação ao computador verificador. Em muitos casos, este sinal não necessita ser codificado devido ao fato de ser um único *bit*. Em configurações que não envolvam a transmissão de informações financeiras ou números de conta, é possível, portanto, implementar a invenção sem a necessidade de transmitir dados codificados. Isto pode ser particularmente desejável para implementações que empreguem pequenos dispositivos de comunicação dedicados.

Complexas entidades de cliente

Em uma de várias possíveis variações da invenção, o cliente é uma complexa entidade que compreende, por exemplo, um agente principal e um ou mais agentes. Exemplos desses complexos clientes são empregador/empregado, pais/filhos e cônjuges. A questão é que uma entidade, o agente inicia uma transação eletrônica enquanto uma entidade separada, o agente principal, é responsável pela transação e autoriza a transação.

Nesta configuração da invenção, o PVI é enviado a partir do computador verificador ao número do telefone celular do agente, conforme descrito acima. O PVI é processado pelo computador usuário do agente de acordo com a Figura 1. O agente introduz sua senha, que é enviada ao verificador e processada pelo computador verificador **1502**. A seguir, ocorre a etapa de autorização na qual o computador verificador recupera o número do telefone do agente principal a partir do banco de dados verificador, liga para o agente principal e requer autorização da transação iniciada pelo agente. Se a transação é autorizada, ocorre o processamento até a sua conclusão; se a autorização é negada, o processo é encerrado. Este refinamento permite ao agente principal autorizar transações enquanto elas são conduzidas, ao invés de ter de aguardar até que uma declaração mensal seja recebida e então autorize *post facto*.

Alternativamente, o sistema pode ser facilmente configurado de modo que tanto a verificação da identidade como as etapas de autorização sejam realizadas pelo agente principal. Nessas configurações, o computador verificador se comunica com o agente principal e verifica a sua identidade, ainda que seja o agente que tenha iniciado a transação.

Se o agente principal estiver em uma localização fixa, não é necessário que o aparelho de comunicação do agente principal seja móvel ou *wireless*. Por exemplo, o departamento de contabilidade de uma empresa pode ser responsável pelo processamento de pedidos de autorização a partir do computador verificador, no qual a telefonia fixa do departamento poderia ser mais conveniente para a comunicação com o computador verificador. Entretanto, tanto o agente como o agente principal que opere através de comunicação *wireless* estão no âmbito da invenção e possuem muitas vantagens.

Aplicações não comerciais da invenção

Após compreender as revelações acima, a diversidade de possíveis aplicações úteis da invenção ficará evidente aos especialistas da técnica. Por exemplo, a invenção pode ser utilizada para verificar a identidade de uma pessoa que utilize um cartão para ter acesso ao quarto de hotel controlado por cartão eletrônico ou outro espaço seguro, em que a transação eletrônica solicitada é a abertura da porta.

Tal aplicação de transação não financeira da invenção é ilustrada na Figura 4. O hóspede **104** procura a entrada **404** em seu quarto inserindo seu cartão-chave. Como é normalmente executado no estado da técnica, é feita a leitura do código do cartão e verificada por um computador de segurança **504**. Se o código não for válido ou se houver alguma outra irregularidade, é soado um alerta **1404**, o acesso é negado e a situação é investigada pela segurança.

Se o código for válido, o computador do hotel determina **1504** se o quarto é indicado como tendo exigido a verificação da identidade do hóspede. Por exemplo, esta pode ser uma opção do hóspede no *check-in*. Não havendo exigência de verificação da identidade, o hotel registra a entrada **1604**, e o quarto é liberado **604**. Se o quarto for indicado para verificação de identidade do hóspede, então uma mensagem é enviada ao verificador **304**, que inicia a verificação da identidade do hóspede **1304**. Ao utilizar um número de acesso de usuário para o telefone celular do hóspede, que foi previamente armazenado no banco de dados verificador no momento do *check-in* do hóspede, o verificador realiza a discagem do número do telefone celular do hóspede e envia **1804** um PVI ao hóspede. O aparelho de telefone celular do hóspede toca **704**, e o computador de usuário responde, recebe e processa o pedido, e o exibe no dispositivo I/O do aparelho de telefone celular. Estas etapas são semelhantes ou idênticas ao exemplo dado acima do cartão de crédito, que inclui a descodificação do PVI.

Se não for o próprio hóspede que estiver tentando entrar no quarto, no entanto, o aparelho de telefone celular do hóspede tocará e ele será alertado que alguém possui seu cartão-chave e está tentando entrar em seu quarto. Ele pode entrar em contato com o hotel ou com a polícia.

Pressupondo que a pessoa que está tentando entrar no quarto seja o hóspede, o hóspede insere uma suposta senha no teclado deste aparelho de telefone celular **804**, cujos dados são processados, codificados e enviados ao computador verificador. O computador verificador recebe a suposta senha, descodifica e avalia **1704** se essa senha é igual à verdadeira senha armazenada no banco de dados verificador. Se a senha não for válida, o hóspede é informado e tenta novamente **904**. Após um número predeterminado de tentativas sem sucesso, é soado um alerta **1904** e a segurança realiza a investigação **1404**.

Se a suposta senha for confirmada **1704**, a entrada é aprovada **1204**, o hotel registra a entrada **1104** e a porta é destravada **1004**.

O exemplo dado aqui de obter acesso a um quarto de hotel é facilmente adaptado à obtenção de acesso a qualquer espaço, tal como prédio, veículo, depósito ou caixa de segurança.

Será agora apreciado que a invenção pode ser convenientemente aplicada a um amplo leque de transações eletrônicas comerciais e não comerciais na obtenção de serviços e benefícios. Por exemplo, em fronteiras em que imigrantes que solicitam permissão para entrar em um país tendo um visto previamente obtido apresentam o visto ou passaporte que é roubado, inicia-se assim um pedido de verificação da identidade a um verificador, que pode ser uma empresa privada ou órgão do governo. O verificador liga para o número do telefone celular da pessoa e envia um PVI. Quando o aparelho de telefone celular toca e a pessoa insere um identificador seguro em resposta ao PVI, os agentes da fronteira obtêm a

imediata confirmação da identidade da pessoa. Se o aparelho de telefone celular não toca, os agentes suspeitam de fraude de documentação e tomam as medidas adequadas. Se o aparelho de telefone celular toca e a pessoa não pode fornecer o identificador seguro correto, os agentes suspeitam de roubo de aparelho de telefone e documentação e tomam as medidas adequadas.

Cartão de transação *proxy* emitido pelo verificador

A Figura 5 ilustra uma configuração do método da invenção na qual o verificador emite um cartão de transação *proxy* ao usuário, o qual substitui um ou mais cartões de crédito de usuário e é utilizado pelo usuário para autorizar a verificação do acesso a uma ou mais contas do usuário. Nesta configuração, durante a fase de pré-cadastro, o usuário fornece ao verificador as informações de acesso da conta e uma autorização existente para acesso de uma ou mais contas – neste exemplo, uma conta de cartão de crédito VISA®. O cadastro da conta pode ser feito pelo cliente simplesmente pelo fornecimento de seu cartão VISA® ao verificador, que insere o cartão em uma leitora para adquirir as informações de acesso da conta e salvá-las no banco de dados verificador. Estas informações de acesso da conta de cartão de crédito são armazenadas no banco de dados verificador com outros dados fornecidos pelo usuário durante o pré-cadastro, conforme revelado acima. Nesta configuração, o pré-cadastro, o armazenamento e recuperação de dados e comunicações com a administradora de cartão de crédito são feitas pela empresa verificadora sem necessariamente envolver o banco do usuário.

Após os dados da conta do cartão de crédito terem sido registrados no banco de dados verificador, o verificador emite ao usuário um cartão de transação *proxy*. Este cartão é semelhante em tamanho e formato a um cartão de crédito, tendo uma tarja magnética. A

tarja magnética no cartão de transação *proxy* necessita apenas conter informações mínimas requeridas para abrir um *link* de comunicação entre o vendedor de varejo e o verificador.

Para auxiliar nesta descrição, o termo "vendedor de varejo" inclui nesta configuração tanto o comerciante como o banco do comerciante ou outra instituição financeira na qual os recursos serão depositados, conforme indicado pelo "Banco do Vendedor de Varejo/Comerciante" na Figura 5. Portanto, os dados cuja leitura é feita do cartão de transação *proxy* são enviados do ponto de venda ao banco do comerciante, que abre o *link* de comunicação com o verificador em **305**. Estes detalhes variam de acordo com as necessidades específicas das instituições que empregam o sistema, mas em qualquer caso o fluxo de informações é invisível ao usuário.

No ponto de venda, o usuário **101** inicia uma transação **202** com o vendedor de varejo/banco do comerciante **102** apresentando o cartão de transação *proxy*. O varejista insere o cartão de transação *proxy* na leitora magnética, que realiza a leitura das informações na tarja magnética. O varejista insere os detalhes da transação, tais como item e valor da compra. Abre-se um *link* de comunicação entre o varejista/banco do comerciante e o computador verificador utilizando as informações de comunicação obtidas do cartão de transação *proxy*, e as informações da transação são enviadas **305** ao verificador.

Opcionalmente, o cliente pode ter mais de uma conta acessada pelo verificador através do cartão de transação *proxy*. Nessas configurações, a tarja magnética do cartão de transação *proxy* contém uma "lista" das contas disponíveis e um simples identificador associado a cada conta, cujo identificador não necessita ser seguro. Quando o cartão de transação *proxy* é inserido pelo varejista, aparece na tela uma lista de contas disponíveis. O consumidor indica que conta deve ser utilizada e o identificador para aquela conta é enviado ao verificador, isto é, neste exemplo: VISA®, conta número 1.

No recebimento da comunicação do varejista, o verificador procura os dados do usuário da conta número 1 VISA® no banco de dados verificador **505** e inicia a verificação da identidade de usuário **605** utilizando um método similar àquele ilustrado na Figura 2 e revelado acima. Em resumo, o verificador envia **705** um PVI ao aparelho de telefone celular do usuário, que ativa o software local objeto de *download* no aparelho de telefone durante o pré-cadastro. O computador do usuário então responde **805** ao computador verificador indicando que o *link* de comunicação está operando devidamente. O computador verificador envia um PVI codificado ao aparelho de telefone celular através do *link* aberto. O usuário insere o seu PIN ou senha ou outro suposto identificador seguro **1005** no telefone celular. O suposto identificador seguro é codificado, enviado de volta ao verificador e comparado **1105** com o verdadeiro identificador seguro recuperado a partir do banco de dados verificador. Se o identificador não for válido, a transação é rejeitada **1505**, o varejista é informado **1705** e o usuário é informado **1805**. Obviamente, conforme revelado anteriormente, a rotina de rejeição pode incluir a permissão de múltiplas tentativas e a análise de tempo esgotado, e informar a polícia e autoridades de controle ou iniciar outras respostas apropriadas. Estas etapas não são mostradas na Figura 5. As mesmas etapas de verificação e o mesmo identificador seguro são utilizados, independentemente de qual conta o usuário escolheu debitar; consequentemente, o usuário precisa se lembrar apenas de um único PIN ou senha para acessar qualquer uma das muitas contas.

Alternativamente, o sistema pode ser configurado de modo que a "lista" das contas de usuário disponíveis não seja contida no cartão de transação *proxy*, e sim mantida no banco de dados verificador. Uma vez inserido o cartão de transação *proxy* e aberto o *link* de comunicação entre o varejista/banco comerciante e o verificador, o verificador recupera

a lista de contas disponíveis a partir do banco de dados verificador, abre o *link* de comunicação com o usuário e transmite a lista de contas disponíveis ao dispositivo de comunicação de usuário. A seguir, o usuário introduz sua escolha de conta no dispositivo de comunicação de usuário.

Se o suposto identificador seguro for validado com o verdadeiro identificador seguro **1105**, então o verificador, atuando como *proxy* do usuário, abre um *link* de comunicação ao provedor de crédito apropriado **105** (isto é, VISA® conta número 1). Isto é possível porque foram fornecidas ao verificador as informações de acesso desta conta pelo usuário durante o pré-cadastro. O computador verificador aprova a transação através da conta escolhida mediante a transmissão **1905** das informações da conta e detalhes da transação pendente ao provedor de crédito. O provedor de crédito então pede ao seu banco de dados que determine se a conta do usuário tem créditos suficientes disponíveis para atender a transação, e uma decisão é tomada **1205** se aprova **1305** ou rejeita **1405** a transação. Essa decisão é comunicada ao computador verificador **1605**, que faz as anotações apropriadas em seu banco de dados e informa o varejista **1705** e o usuário **1805** para que a transação possa ser concluída ou cancelada, de acordo com as instruções do provedor de crédito. Todas as etapas acima desde o início da transação podem ser realizadas automaticamente.

Há uma série de vantagens desta configuração da invenção. Em primeiro lugar, o consumidor não necessita carregar cartões de crédito, ou informações que identifiquem suas contas. Portanto, o cartão de transação *proxy* emitido pelo verificador se torna um cartão de crédito universal porque permite ao consumidor acessar todas as suas contas de cartão de crédito de maneira segura, sem transmitir qualquer informação da conta através de dispositivos de comunicação de comerciante ou cliente. Em segundo lugar, o

consumidor precisa apenas se lembrar de um único PIN de acesso a todas as suas contas de cartão de crédito. Em terceiro lugar, independentemente do lugar em que o usuário apresenta seu cartão de transação *proxy*, nenhum número de conta ou outra informação relacionada é transmitida a partir do ponto de venda. A única transmissão de informações de conta é a partir do verificador central ao provedor de crédito. Consequentemente, a segurança da transmissão de informações de conta pode ser controlada e aumentada em grande medida. Em quarto lugar, o banco do consumidor não necessita estar envolvido na transação eletrônica porque o verificador atua como *gateway* à administradora de cartão de crédito. As informações são transmitidas do varejista, do verificador e do usuário, bem como do verificador e da administradora de cartão de crédito.

SUMÁRIO

Serão facilmente compreendidos a partir da descrição acima a novidade, utilidade e os meios de interpretação e prática da invenção. As revelações das configurações preferidas da invenção representam a melhor forma conhecida por mim até a presente data. Deve ser entendido que a minha invenção não se limita às configurações reveladas acima, mas abrange todas e quaisquer configurações no âmbito das seguintes reivindicações.

REIVINDICAÇÕES ALTERADAS

recebidas pela Comissão Internacional em 7 de março de 2008 (07.03.2008)

1. Método para verificar a identidade de um usuário no curso de uma transação eletrônica por um verificador, caracterizado por compreender:

(a) o pré-cadastro do usuário, que consiste nas seguintes etapas:

(a1) a atribuição de um identificador seguro ao usuário; e

(a2) o armazenamento do identificador seguro em banco de dados;

(b) o pré-cadastro do dispositivo de comunicação de usuário, compreendendo:

(b1) a obtenção de número de acesso de usuário para o dispositivo de comunicação, sendo que esse número pode ser utilizado para abrir *links* de comunicação com o dispositivo de comunicação de usuário; e

(b2) o armazenamento do número de acesso de usuário em banco de dados;

(c) a recuperação do número de acesso de usuário do banco de dados da Etapa (b2);

(d) a abertura do *link* de comunicação entre o verificador e o dispositivo de comunicação de usuário, utilizando o número de acesso de usuário recuperado na Etapa (c);

(e) o envio de um pedido de verificação de identidade (PVI) ao usuário através do *link* de comunicação aberto na Etapa (d);

(f) a entrada pelo usuário em um suposto identificador seguro;

(g) o envio de uma resposta ao PVI da Etapa (e) através do *link* de comunicação aberto na Etapa (d);

(h) a recuperação do identificador seguro armazenado na Etapa (a2);

(i) a comparação da entrada do suposto identificador seguro na Etapa (f) com o identificador seguro recuperado na Etapa (h); e

(j) a permissão para uma transação somente mediante o cruzamento do suposto identificador seguro e do identificador seguro feito pela comparação da Etapa (i).

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de a resposta enviada na Etapa (g) incluir a entrada do suposto identificador seguro na Etapa (f), e pelo fato de a Etapa (i) ser realizada pelo verificador.

3. Método de acordo com a reivindicação 1, caracterizado pelo fato de a Etapa (b) compreender ainda:

(b3) o *download* do software local ao dispositivo de comunicação de usuário.

4. Método de acordo com a reivindicação 3, caracterizado pelo fato de o PVI enviado na Etapa (e) incluir o identificador seguro recuperado na Etapa (h), e pelo fato de a Etapa (i) ser realizada pelo *download* do software local na Etapa (b3), e ainda pelo fato de a resposta envida na Etapa (g) incluir os resultados da comparação realizada na Etapa (i).

5. Método de acordo com a reivindicação 3, caracterizado pelo fato de o software local após o *download* feito na Etapa (b3) realizar pelo menos a operação da Etapa (g) e da Etapa (i).

6. Método de acordo com a reivindicação 3, caracterizado pelo fato de o software local após o *download* feito na Etapa (b3) realizar:

(k) o recebimento do PVI enviado na Etapa (e);

(l) a formatação do PVI para exibição; e

(m) a exibição do PVI de input/output (I/O) do dispositivo de comunicação de usuário.

7. Método de acordo com a reivindicação 3, caracterizado pelo fato de o software local após o *download* feito na Etapa (b3) realizar pelo menos: (i) a decodificação das informações recebidas pelo dispositivo de comunicação de usuário e (ii) a codificação das informações enviadas pelo dispositivo de comunicação de usuário.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de pelo menos o PVI da Etapa (e) ou a resposta da Etapa (g) ser codificado, quando enviado.

9. Método de acordo com a reivindicação 1, caracterizado por compreender ainda:

(n) o envio de pedido de autorização de transação ao dispositivo de comunicação de usuário;

(o) o envio de resposta ao pedido de autorização de transação da Etapa (n); e

(p) a permissão da transação somente se a resposta da Etapa (i) for autorizar a transação.

10. Método de acordo com a reivindicação 9, caracterizado por compreender ainda o pré-cadastro de uma conta do usuário, que consiste no estabelecimento de uma indicação se as Etapas (n) a (p) devem ou não ser realizadas.

11. Método de acordo com a reivindicação 1, caracterizado por compreender ainda o pré-cadastro de uma conta do usuário, que consiste no estabelecimento de uma indicação se as Etapas (c) a (j) devem ou não ser realizadas.

12. Método de acordo com a reivindicação 1, caracterizado por compreender ainda o pré-cadastro de pelo menos uma conta do usuário, que consiste em (i) adquirir informações de acesso para a conta e (ii) armazenar as informações de acesso da conta em banco de dados verificador.

13. Método de acordo com a reivindicação 12, caracterizado por compreender ainda a emissão ao usuário de cartão de transação *proxy*, caracterizado pelo fato de o cartão de transação *proxy* poder ser utilizado pelo usuário para autorizar o verificador a acessar a conta pré-cadastrada, utilizando as informações de acesso armazenadas em banco de dados verificador.

14. Método de acordo com a reivindicação 13, caracterizado por compreender ainda:

(q) o uso das informações contidas no cartão de transação *proxy* para abrir um *link* de comunicação com o verificador;

(r) a exibição ao usuário das contas pré-cadastradas as quais o verificador está autorizado a acessar;

(s) a seleção pelo usuário das contas exibidas na Etapa (r) as quais o verificador está autorizado a acessar;

(t) o acesso pelo verificador da conta selecionada na Etapa (s), utilizando as informações de acesso de conta armazenadas no banco de dados verificador; e

(u) a aprovação da transação através da conta acessada na Etapa (s) se a transação for autorizada na Etapa (j).

15. Método de acordo com a reivindicação 1, caracterizado pelo fato de a Etapa (b) compreender ainda:

(b4) a aquisição de um identificador de dispositivo do dispositivo de comunicação de usuário; e

(b5) o armazenamento do identificador de dispositivo em banco de dados verificador, e pelo fato de o método compreender ainda:

(v) a recuperação do identificador de dispositivo a partir do banco de dados verificador da Etapa (b5);

(w) a obtenção do identificador de dispositivo do dispositivo de comunicação de usuário;

(x) a comparação do identificador de dispositivo recuperado na Etapa (u) com o identificador de dispositivo obtido na Etapa (w); e

(z) a conclusão da transação se não houver o cruzamento dos identificadores de dispositivo comparados na Etapa (x).

16. Sistema para verificar a identidade de usuário durante o curso de uma transação eletrônica, compreendendo:

a. banco de dados verificador;

b. computador verificador que é adaptado para escrever e recuperar dados do referido banco de dados verificador;

c. um primeiro dispositivo de comunicação verificador para receber e transmitir dados ao usuário, caracterizado pelo fato de este primeiro dispositivo de comunicação verificador ser acessível pelo referido computador verificador;

d. dispositivo de comunicação de usuário para receber e transmitir dados ao verificador, caracterizado pelo fato de este dispositivo de comunicação de usuário ser acessível pelo usuário;

e. dispositivo de input/output (I/O) que recebe dados de entrada do usuário e exibe os dados de saída do usuário; e

f. computador de usuário acoplado ao referido dispositivo de comunicação de usuário e ao dispositivo I/O, em que está adaptado para:

i) exibir no dispositivo I/O a entrada de um pedido de verificação de identidade (PVI) enviado pelo computador verificador através do referido dispositivo de comunicação verificador;

ii) adquirir os dados do usuário inseridos no referido dispositivo I/O, que incluem um suposto identificador seguro; e

iii) enviar uma resposta ao PVI a partir do referido dispositivo de comunicação de usuário ao dispositivo de comunicação verificador,

caracterizado pelo fato de que pelo menos o computador de usuário ou o computador verificador esteja adaptado para:

iv) receber como um primeiro dado o identificador seguro recuperado do referido banco de dados verificador;

v) receber como um segundo dado o suposto identificador seguro;

vi) comparar o primeiro dado com o segundo; e

vii) produzir uma confirmação que indique se há o cruzamento do primeiro com o segundo dado, em que a transação eletrônica seja bloqueada, a menos que a confirmação indique o cruzamento do primeiro com o segundo dado.

17. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de o computador de usuário estar adaptado para decodificar um PVI codificado enviado pelo verificador.

18. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de o computador de usuário estar adaptado para codificar a resposta.

19. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de o dispositivo de comunicação de usuário ser um dispositivo de comunicação pessoal.

20. Sistema de acordo com a reivindicação 16, caracterizado pelo fato de que compreende ainda um segundo dispositivo de comunicação verificador para transmitir a confirmação ao banco.

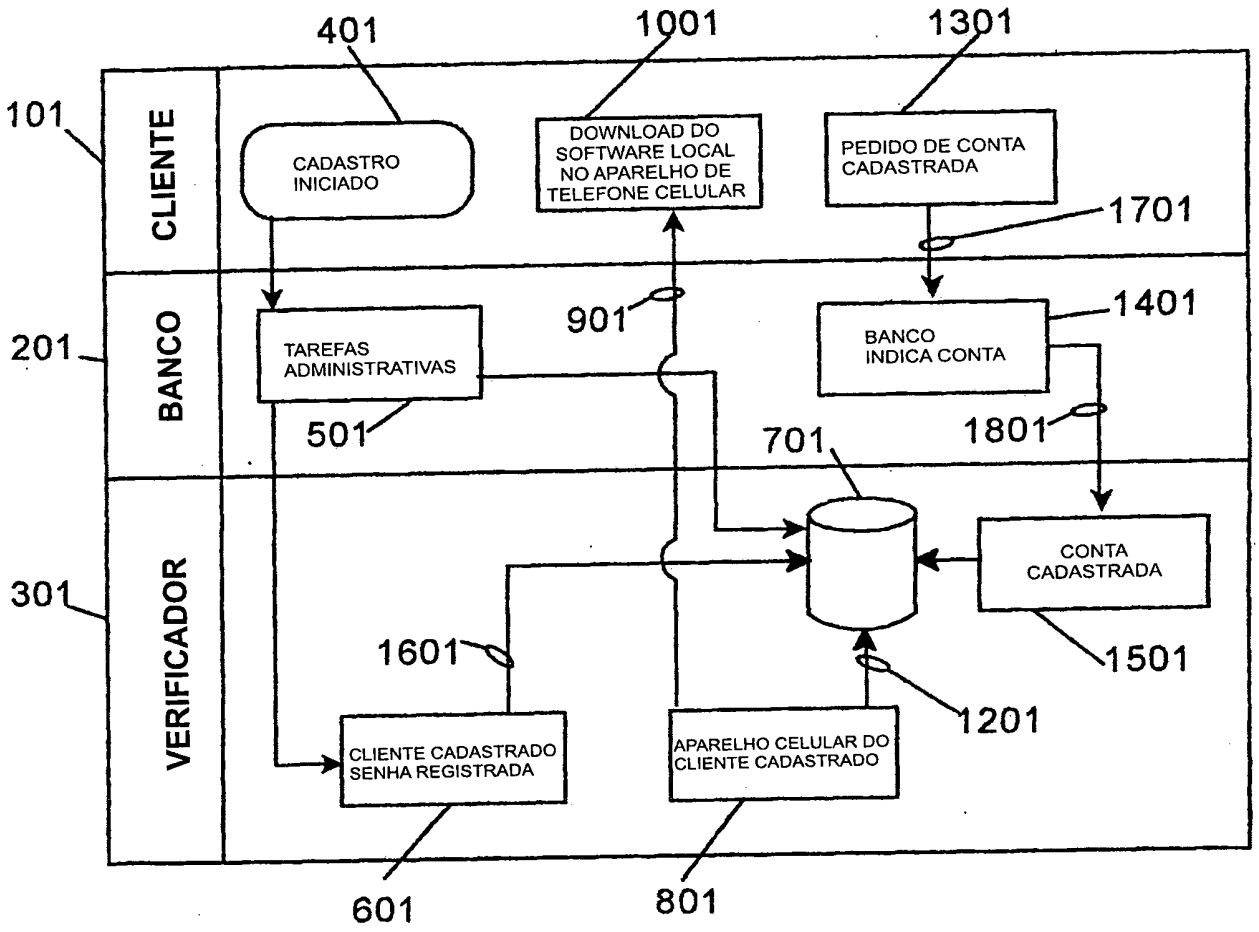

401
1001
1301
101
CLIENTE
CADASTRO INICIADO
DOWNLOAD DO SOFTWARE LOCAL NO APARELHO DE TELEFONE CELULAR
PEDIDO DE CONTA CADASTRADA
1701
BANCO
201
TAREFAS ADMINISTRATIVAS
901
BANCO INDICA CONTA
1401
501
701
1801
VERIFICADOR
301
CONTA CADASTRADA
1601
1501
1201
CLIENTE CADASTRADO SENHA REGISTRADA
APARELHO CELULAR DO CLIENTE CADASTRADO
601
801

Fig. 1

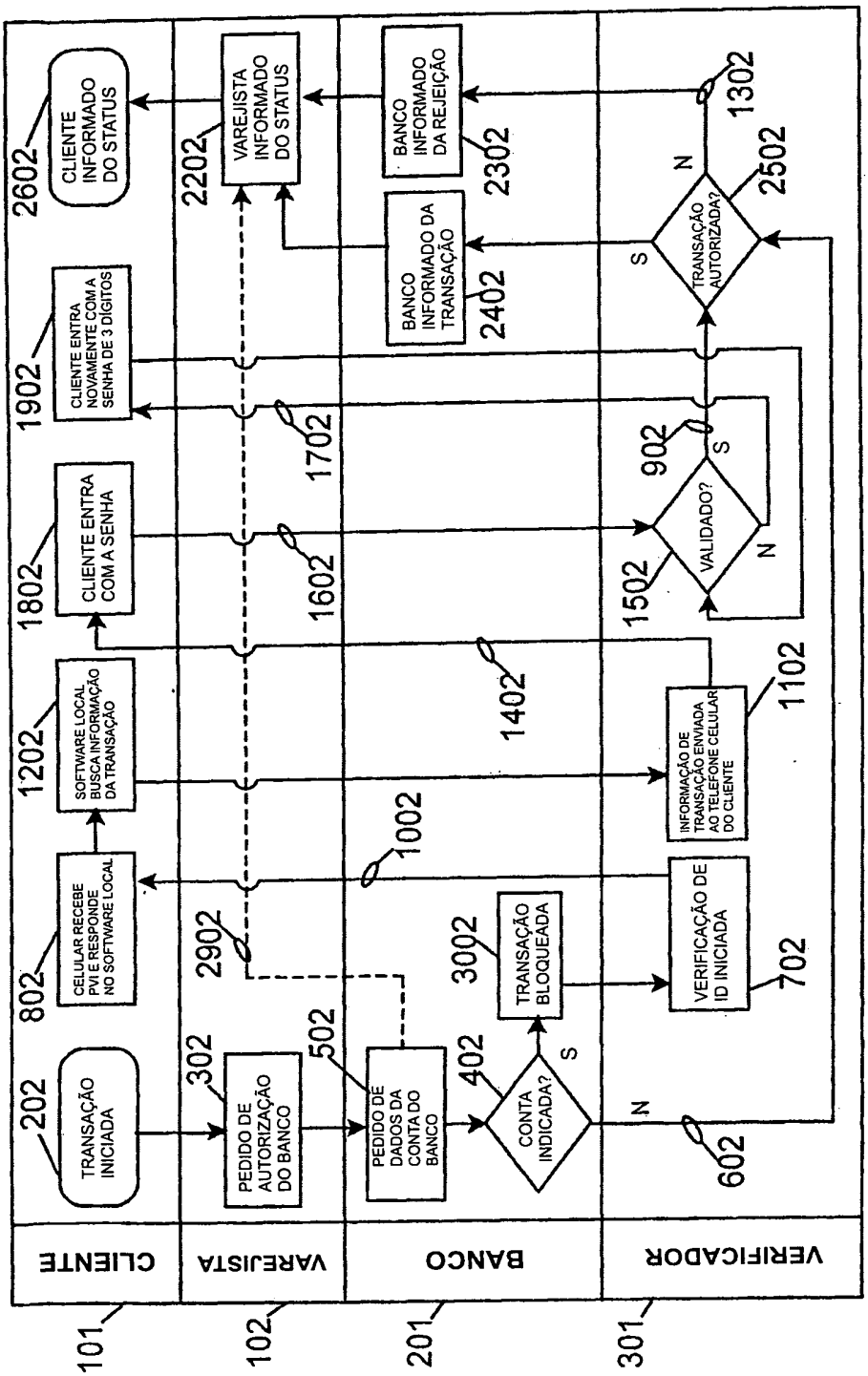

CLIENTE
VAREJISTA
BANCO
VERIFICADOR
101
102
201
301
TRANSAÇÃO INICIADA
202
CELULAR RECEBE PVI E RESPONDE NO SOFTWARE LOCAL
802
SOFTWARE LOCAL BUSCA INFORMAÇÃO DA TRANSAÇÃO
1202
CLIENTE ENTRA COM A SENHA
1802
CLIENTE ENTRA NOVAMENTE COM A SENHA DE 3 DÍGITOS
1902
CLIENTE INFORMADO DO STATUS
2602
PEDIDO DE AUTORIZAÇÃO DO BANCO
302
PEDIDO DE DADOS DA CONTA DO BANCO
502
CONTA INDICADA?
402
S
N
TRANSAÇÃO BLOQUEADA
3002
VERIFICAÇÃO DE ID INICIADA
702
INFORMAÇÃO DE TRANSAÇÃO ENVIADA AO TELEFONE CELULAR DO CLIENTE
1102
VALIDADO?
902
1502
TRANSAÇÃO AUTORIZADA?
1302
2502
VAREJISTA INFORMADO DO STATUS
2202
BANCO INFORMADO DA REJEIÇÃO
2302
BANCO INFORMADO DA TRANSAÇÃO
2402
602
1002
1402
1602
1702
2902

Fig. 2

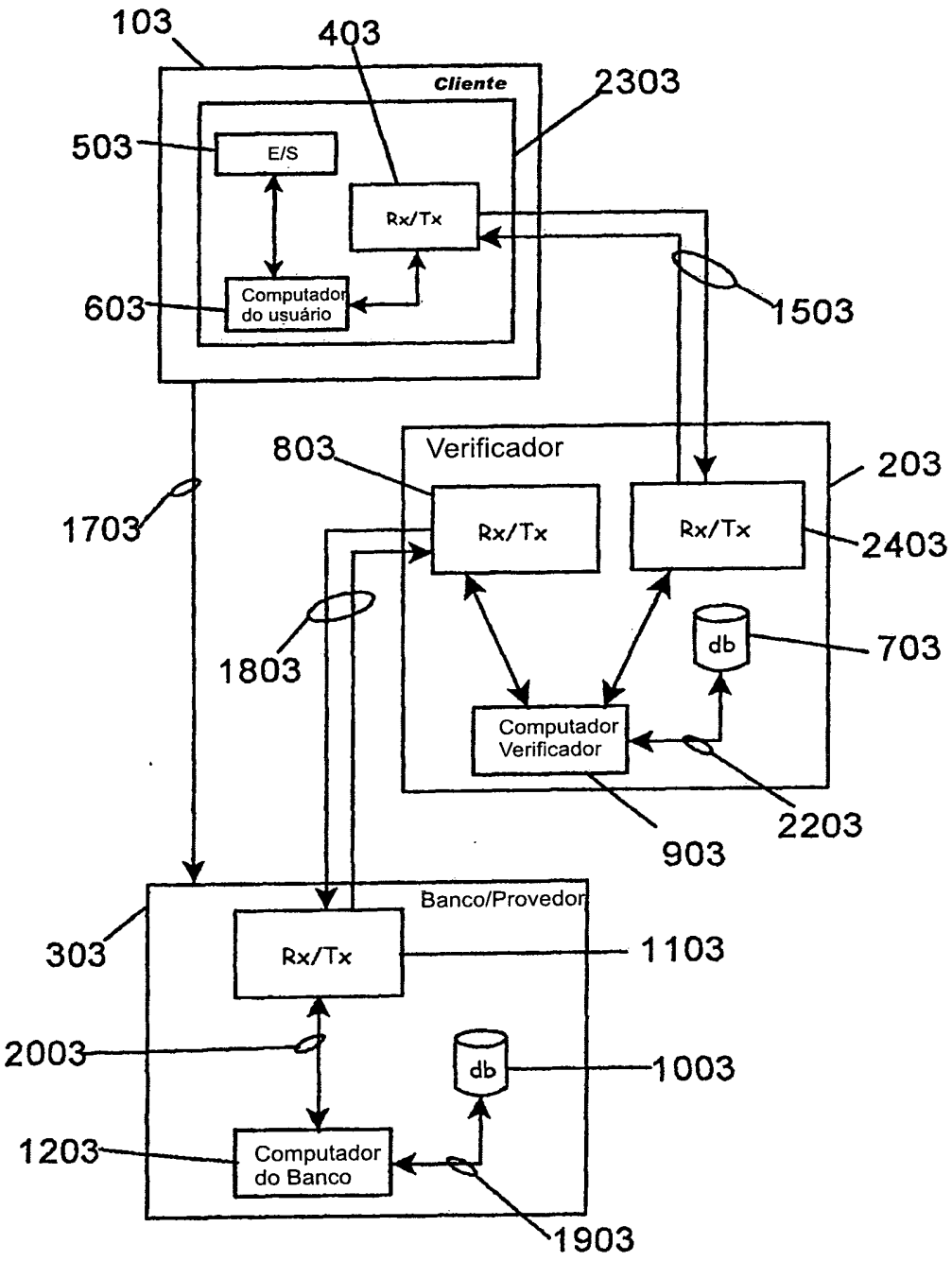

103
403
Cliente
2303
503
E/S
Rx/Tx
603
Computador do usuário
1503
803
Verificador
203
1703
Rx/Tx
Rx/Tx
2403
1803
db
703
Computador Verificador
2203
903
Banco/Provedor
303
Rx/Tx
1103
2003
db
1003
1203
Computador do Banco
1903

Fig. 3

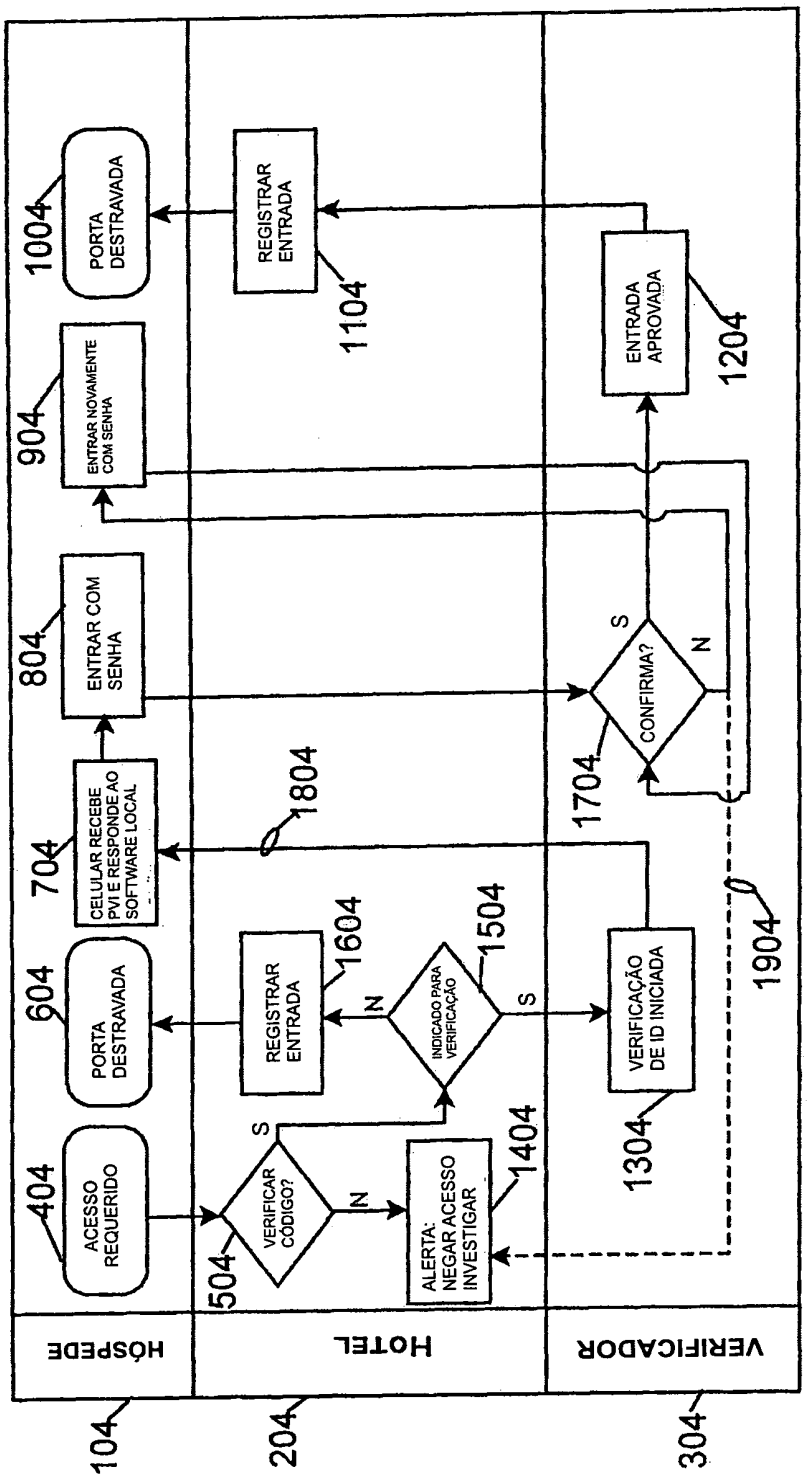

HÓSPEDE
HOTEL
VERIFICADOR
104
204
304
404
ACESSO REQUERIDO
504
VERIFICAR CÓDIGO?
S
N
604
PORTA DESTRAVADA
704
CELULAR RECEBE PVI E RESPONDE AO SOFTWARE LOCAL
804
ENTRAR COM SENHA
904
ENTRAR NOVAMENTE COM SENHA
1004
PORTA DESTRAVADA
1404
ALERTA: NEGAR ACESSO INVESTIGAR
1604
REGISTRAR ENTRADA
1504
INDICADO PARA VERIFICAÇÃO
N
S
1804
1304
VERIFICAÇÃO DE ID INICIADA
1704
CONFIRMA?
S
N
1904
1104
REGISTRAR ENTRADA
1204
ENTRADA APROVADA

Fig. 4

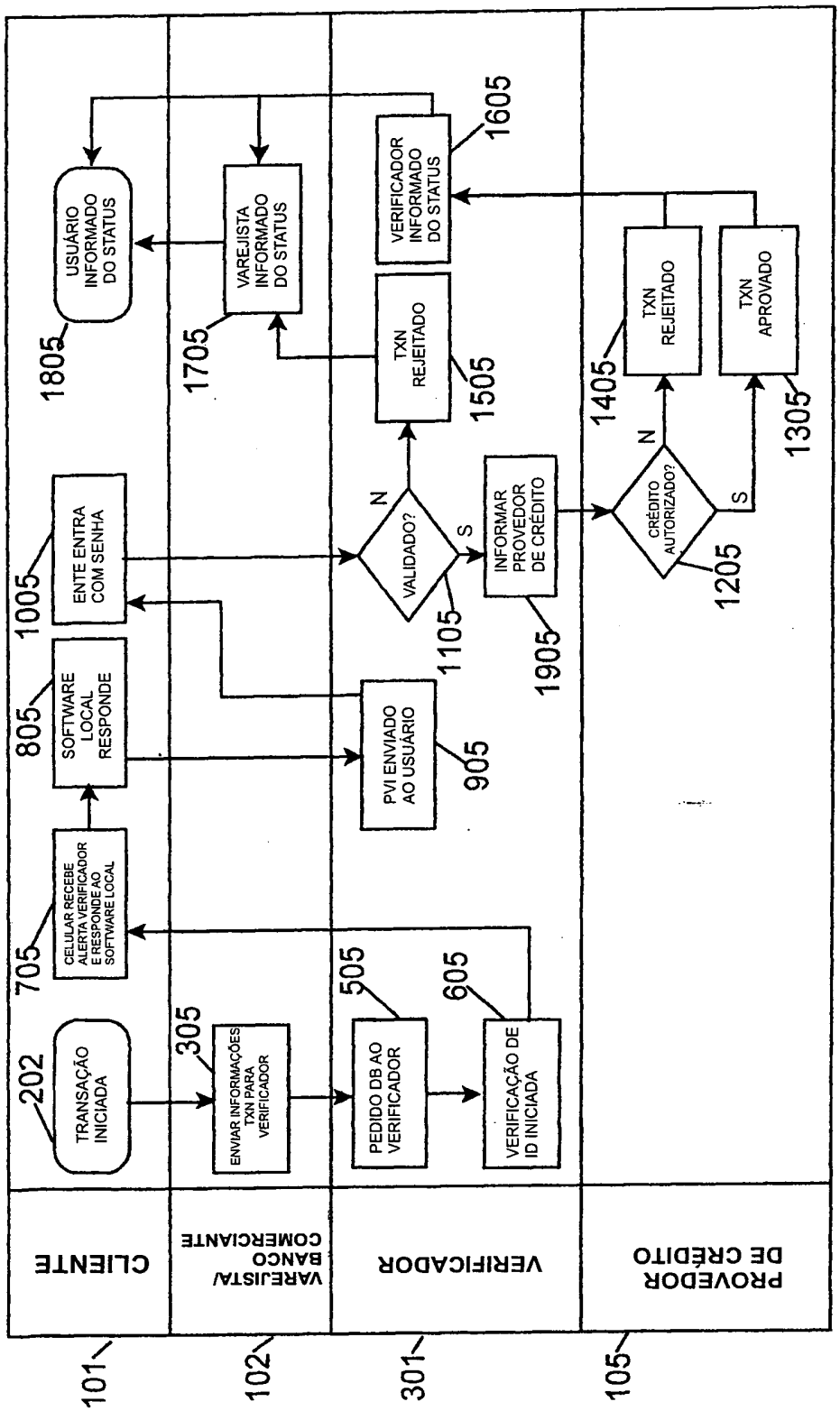

CLIENTE
VAREJISTA/ BANCO COMERCIANTE
VERIFICADOR
PROVEDOR DE CRÉDITO
101
102
301
105
TRANSAÇÃO INICIADA
202
CELULAR RECEBE ALERTA VERIFICADOR E RESPONDE AO SOFTWARE LOCAL
705
SOFTWARE LOCAL RESPONDE
805
ENTE ENTRA COM SENHA
1005
USUÁRIO INFORMADO DO STATUS
1805
ENVIAR INFORMAÇÕES TXN PARA VERIFICADOR
305
VAREJISTA INFORMADO DO STATUS
1705
PEDIDO DB AO VERIFICADOR
505
VERIFICAÇÃO DE ID INICIADA
605
PVI ENVIADO AO USUÁRIO
905
VALIDADO?
1105
N
S
TXN REJEITADO
1505
VERIFICADOR INFORMADO DO STATUS
1605
INFORMAR PROVEDOR DE CRÉDITO
1905
CRÉDITO AUTORIZADO?
1205
N
S
TXN REJEITADO
1405
TXN APROVADO
1305

Fig. 5

RESUMO

SISTEMA E MÉTODO PARA VERIFICAR A IDENTIDADE DE USUÁRIO EM TRANSAÇÕES ELETRÔNICAS

A invenção diz respeito a um método e sistema para verificar a identidade de usuário no curso de transação eletrônica. A invenção provê um processo e sistema para bloquear uma conta até que um verificador conclua o processo de verificação de identidade para verificar a identidade da pessoa que inicia a transação. O processo compreende o pré-cadastro da pessoa e do dispositivo de comunicação pessoal. Opcionalmente, uma ou mais contas são cadastradas pela indicação de contas de modo que as transações sejam sujeitas à verificação da identidade de usuário. No momento que a transação é iniciada, o verificador envia um pedido de verificação de identificação (PVI) ao dispositivo de comunicação portátil da pessoa que inicia a transação eletrônica. A seguir, a pessoa verifica sua identidade fornecendo um identificador seguro em resposta ao PVI. Opcionalmente, é solicitada à pessoa a autorização da transação antes da transação ser aceita.