

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

(21) **PI 0621842-3 A2**

(22) Data de Depósito: 11/07/2006
(43) Data da Publicação: 12/06/2012
(RPI 2162)



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

(54) Título: DISPOSITIVO TERMINAL MÓVEL E RESPECTIVOS MÉTODOS DE OPERAÇÃO, LOJA DE REDE DE COMERCIANTE, CENTRO DE AUTORIZAÇÃO E PROCESSAMENTO, SISTEMA E PARCEIROS MÚLTIPLOS, CLIENTES E SERVIDORES EM REDE CLIENTE-SERVIDOR E EM SISTEMA DE PARCEIROS MÚLTIPLOS, PRODUTO DE PROGRAMA DE COMPUTADOR CONTENDO CÓDIGO DE PROGRAMA, MEIO LEGÍVEL EM COMPUTADOR, SINAL DE DADOS MODULADOS OU SINAL DE DADOS DE COMPUTADOR, SISTEMA DE PERMUTA DE DADOS DE TRANSAÇÕES E PARTICIPANTE

(73) Titular(es): Ultra Proizvodnja Elektronskih Naprav D.O.O.

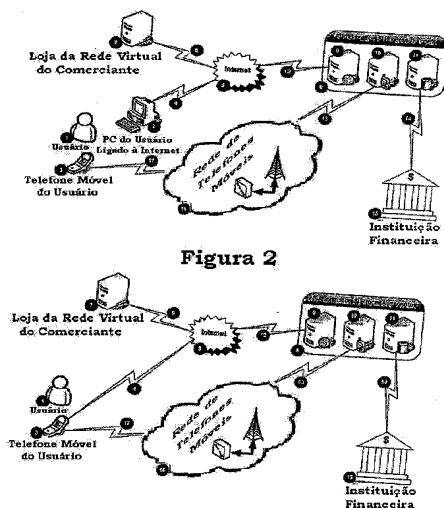
(72) Inventor(es): Amor Chowdhury, Bor Prihavec, Gregor Breznik, Klemen Verdnik

(74) Procurador(es): Hugo Silva, Rosa & Maldonado-Prop. Int

(86) Pedido Internacional: PCT IB2006001904 de 11/07/2006

(87) Publicação Internacional: WO 2008/007162de
17/01/2008

(57) Resumo: Dispositivo Terminal Móvel e Respectivos Métodos de Operação, Loja de Rede de Comerciante, Centro de Autorização e Processamento, Sistema de Parceiros Múltiplos, Clientes e Servidores em Rede Cliente-Servidor e em Sistema de Parceiros Múltiplos, Produto de Programa de Computador Contendo Código de Programa, Meio Legível em computador, Sinal de Dados Modulados ou Sinal de Dados de Computador, Sistema de Permuta de Dados de Transações e Participante" Esta invenção mcistra um dispositivo termina.l móvel (3) que tem uma unidade de memória (3a) e um dispositivo de interface (3b) que é conectável de modo liberável a um sistema de parceiros múltiplos (7,9,15) e capaz de comunicação nele, em que a referida 'comunicação é proporcionada por um terminal frontal formado pelo citado dispositivo terminal móvel (3) em combinação eom um dispositivo de computador pessoal (2) e um terminal posterior formado por um parceiro do citado sistema de parceiros múltiplos via modos de comunicação, sendo dita comunicação adequada para executar transações de dados com requisitos de segurança variantes, de tal modo que as partes complementaresou partes dentro de uma aplicação distribuída, correndo dentro de um sistema de parceiros múltiplos, são executadas dependentes de seus requisitos de segurança atuais, em que a referida comunicação é usada para permutar informações pelo uso dos citados modos de comunicação de características diferentes e variantes (4, 6, 12, 17, 13) usando diferentes canais de comunicação e padrões ou protocolos de interface diferentes.



“Dispositivo Terminal Móvel e Respective Métodos de Operação,

Loja de Rede de Comerciante, Centro de Autorização e

Processamento, Sistema de Parceiros Múltiplos, Clientes e

Servidores em Rede Cliente-Servidor e em Sistema de Parceiros

5 **Múltiplos, Produto de Programa de Computador Contendo Código**

de Programa, Meio Legível em Computador, Sinal de Dados

Modulados ou Sinal de Dados de Computador, Sistema de Permuta

de Dados de Transações e Participante”

Relatório Descritivo

10

Área da Invenção

A presente invenção relaciona-se em geral com um sistema de permuta de dados de transação financeira entre um ponto de venda da Internet, um dispositivo terminal móvel e um centro de autorização e processamento.

15

Antecedentes da Invenção

20 A tecnologia de telecomunicação móvel está experimentando sucesso mundial sem precedentes. Nunca antes na história alcançou uma tecnologia elevada a penetração de mercado em tão pouco tempo. Por outro lado, a popularidade da Internet continua a crescer devido à abundância de informações, serviços, comércio e entretenimento que as pessoas desfrutam a partir de recursos baseados na Internet.

Todavia, a fim de ter acesso a muitas das informações e

serviços mais úteis, ao mesmo tempo em que mantém um nível aceitável de segurança, os usuários devem lembrar-se de um número crescente de nomes dos usuários, contra-senhas, Números de Identificação Pessoal (PINs) etc. Para serviços que exigem segurança incrementada, tais como comércio eletrônico, m-comércio, serviços bancários online etc. o uso de contra-senhas ou PINs como um meio de identificação e autenticação não é suficientemente forte. Exigem-se meios de identificação e autenticação mais poderosos.

Os sistemas de pagamento da Internet de hoje estão usando diferentes tipos de métodos de identificação e autenticação. Como por exemplo:

- nome do usuário e contra-senha
- códigos de segurança pré-gerados
- certificados
- introduzir um código de verificação recebido via Serviços de Mensagens Curtas (*Short Messages Services*) SMS.

Alguns dos sistemas de pagamento estão usando o SMS para identificar um cliente. O serviço de pagamento envia um código de verificação para o telefone móvel do cliente. Ele introduz o código no navegador de rede e o sistema identifica-o. Este tipo de métodos não é conveniente para os clientes, porque os procedimentos são difíceis, levam tempo, não são compreensíveis. Ao lado disto, os clientes poderiam ficar com o sentimento de que seus números de telefone móveis poderiam ser explorados.

A presente invenção propõe uma abordagem que contribui para os serviços relacionados com a segurança de redes de telefones móveis para a Internet. Como já descrito WO-0233669, intitulado

“*System for Payment Data Exchange and Payment Terminal Device Used Therein*”, a presente invenção concentra-se nos serviços relacionados com a segurança a respeito de telefones móveis tais como cartões inteligentes GSM mais precisamente o Módulo de Identidade de Subscritor (SIM).

Em particular, é revelada a descrição de um cenário de pagamento móvel, em que uma transação de pagamento que é realizada na Internet é feita com a combinação de telefone móvel e *links* de comunicações da Internet.

Diferentemente de outros tipos de métodos de identificação e autenticação, é o mais rápido e o caminho mais fácil para identificar um cliente e habilitá-lo na transação de pagamento seguro da Internet.

Sumário da Invenção

Um objetivo da presente invenção consiste na operação de um procedimento de identificação e autenticação de cliente para pagamentos *online* na Internet usando um telefone móvel.

De acordo com a invenção, é proporcionado um sistema e um procedimento de pagamento.

De acordo com a invenção, é proporcionado um sistema de parceiros múltiplos tendo as características da Reivindicação 10, um cliente numa rede cliente-servidor tendo as características da Reivindicação 11, é proporcionado um cliente híbrido num sistema de parceiros múltiplos tendo as características da Reivindicação 13, é proporcionado um servidor numa rede cliente-servidor 1 tendo as características da Reivindicação 15, é proporcionado um método para operar um dispositivo terminal móvel num procedimento de pagamento tendo as características da Reivindicação 16, é proporcionado um método para operar

R/

um dispositivo terminal móvel numa identificação e autenticação de usuário do citado procedimento de pagamento de acordo com as características da Reivindicação 17, um produto de programa de computador contendo o código de programa, um meio legível em computador, um
5 sinal modulado de dados ou sinal de dados de computador, cada um disposto de forma a executar um de dito método é proporcionado nas Reivindicações 22, 23, 24, respectivamente, é proporcionado um sistema de permuta de dados de transações com as características da Reivindicação 25 e é proporcionado um participante de sistema de
10 permuta de dados de transações com as características da Reivindicação 26.

Aspectos adicionais da invenção resultam a partir das outras Reivindicações, a partir da seguinte descrição, assim como também a partir dos desenhos.

15 Outras características estão inerentes aos métodos e produtos descritos ou se tornar-se-ão evidentes para aquelas pessoas qualificadas na técnica a partir da descrição detalhada seguinte de modalidades e seus desenhos anexos.

Breve Descrição dos Desenhos

20 As modalidades da invenção serão, agora, descritas, por via de exemplo e com referência aos desenhos anexos, em que:

a **Figura 1** é uma estrutura de sistema com uma interface WEB, de acordo com uma modalidade da invenção;

25 a **Figura 2** é uma estrutura de sistema com uma interface WAP, de acordo com outra modalidade da da invenção;

a **Figura 3** é um diagrama de identificação e autenticação de cliente via a referida interface WEB, de acordo com

uma modalidade da invenção;

a **Figura 4** é um diagrama de identificação e autenticação via a citada interface WAP, de acordo com outra modalidade da invenção;

5 a **Figura 5a a 5c** é um diagrama de fluxograma, em que é introduzido um PIN depois da identificação do cliente, de acordo com uma modalidade da invenção;

a **Figura 6a a 6c** é um diagrama de fluxograma, em que é introduzido um PIN antes da identificação do cliente, de
10 acordo com uma modalidade da invenção.

A Figura 1 ilustra a estrutura inventiva de acordo com uma modalidade da presente invenção.

Um usuário 1, tipicamente um cliente, está posicionado na frente de um Computador Pessoal (PC) 2 que, por exemplo, exibe
15 uma aplicação usando um navegador de rede e tendo um dispositivo terminal móvel 3 à mão, que, por exemplo, tem interface WAP.

O referido PC 2 está conectado via um componente de interface à Internet 5 numa conexão 4, por exemplo, um canal de transmissão. Por outro lado, o dispositivo terminal móvel 3 é conectado
20 de modo liberável por um componente de interface a uma Rede de Telefone Móvel 16 via uma conexão 17.

O PC 2 do usuário 1 e seu dispositivo terminal móvel 3 formam uma unidade de comunicação híbrida 18.

Uma loja de rede virtual 7 de um comerciante está conectada à referida Internet 5 por uma conexão 6. Por outro lado, um APC
25 (centro de autorização e processamento) 8, tendo subsistemas, está também conectado à citada Internet 5 via uma conexão 12.

Os subsistemas da referida APC 8 são um servidor de Rede 9, um portal de rede móvel 10 e um servidor de dados 11.

A referida rede de telefones móveis 16 está conectada ao citado portal de rede móvel 11 de dita APC 8 via uma conexão 13.

5 O referido servidor de dados 11 é conectado a uma instituição financeira 15 via uma conexão separada 14.

O citado usuário 1 é registrado pela APC 8 e tem um instrumento de pagamento móvel válido (Diners, Master, Euro, Amex, Visa Card etc.) emitido a partir da instituição financeira 15.

10 Agora, a função, de acordo com uma modalidade da presente invenção, é, por exemplo, como se segue: um Usuário 1 está surfando em seu PC 2 na aplicação de Internet da loja virtual do Comerciante 7 via a rede de Internet 5.

15 Uma vez que o Usuário 1 tenha concluído as suas compras de bens, serviços ou ambos, o procedimento de pagamento é o seguinte.

A primeira etapa é escolher o método de pagamento na aplicação de Internet da loja virtual do Comerciante 7 que está ativando o pagamento móvel.

20 A seguir, o aplicativo da Internet 7 de compras virtuais de Comerciantes está ativando o aplicativo do servidor da rede do centro de autorização e processamento para o pagamento 9.

25 Além disso, o aplicativo da Internet 7 da loja virtual do Comerciante está passando para o APC 8 todos os dados de transações de pagamento necessários tais como quantia, número de referência da conta etc.

B

A seguir, o navegador de rede que exhibe para o usuário o aplicativo do servidor de Rede APC para pagamento 9 consegue um código de ID de transação que é gerado no APC 8.

Depois de receber um código de ID de transação via navegador de rede em seu PC 2, o Usuário tem de enviar este código de ID de transação via o seu telefone Móvel 3 para o APC 8, mais precisamente para o portal de rede móvel APC 10. A tarefa do portal de rede móvel APC 10 é conseguir o MSISDN (Número de ISDN dosubscritor móvel), um identificador de equipamento do telefone móvel individual 9, que é também enviado como característica de identificação, enquanto o telefone móvel 3 e o código de ID de transação estão sendo usados.

Na próxima etapa, o APC 8 está informando o Usuário 1 sobre o recebimento bem sucedido do código de ID de transação via o seu telefone Móvel 3 ou via o navegador de rede no PC 2 do Usuário ou via ambos.

Além disso, as conexões de Internet 4, 12 são estabelecidas como conexões seguras entre o PC 2 do Usuário e o servidor de rede APC 9. A comunicação encriptada segura está ativando para o Usuário 1 uma seleção segura do instrumento de pagamento no aplicativo 9 do servidor de rede APC e a transmissão de PIN seguro que está ligado ao instrumento de pagamento para o APC 8.

Num lado do APC 8, a conexão de dados para a instituição financeira 14 é ativada para a autorização do instrumento de pagamento.

Se a autorização a partir de um lado da instituição financeira (expedidora) 9 for aprovada, então, a etapa final é uma confirmação da transação de pagamento para o Usuário 1 via o seu navegador de rede. Com isto, a transação de pagamento da Internet está concluída para o Usuário 1.

Depois, todos os dados necessários sobre a transação são registrados no servidor de dados APC 11 e, além deste, todos os dados necessários são enviados para loja da rede do Comerciante 7 e para a plataforma de dados da instituição financeira 15.

5 A vantagem de usar esta configuração de comunicação híbrida usando um dispositivo terminal móvel 3, um PC 2 situa-se em várias possibilidades de variação, por exemplo, usar dois modos de comunicação diferentes, isto é, uma comunicação de modo duplo ou
10 ou WAP para executar um aplicativo.

O referido aplicativo, o pagamento eletrônico, considerados como um todo, é distribuído através de vários participantes de, por exemplo, um sistema de quatro parceiros, em que cada um dos parceiros, os participantes, aqui, por exemplo, o citado usuário, o meio de
15 comunicação híbrida formado pelo dispositivo terminal móvel e o computador pessoal, a dita loja virtual, o referido APC e a citada instituição financeira, podem receber e processar informações de entrada, enviar e remeter informações de saída, adequadas para o respectivo padrão de interface usado no respectivo modo de comunicação, por exemplo,
20 largura de banda ou canal otimizado.

A cada participante do referido sistema de parceiros é proporcionado meio, por exemplo, para receber, remeter, transmitir, processar e filtrar mensagens, incluindo a memória intermediária, estratégias de armazenamento ou agendamento com prioridade conforme proporcionado por um aplicativo de software típico.
25

Por um lado, num dispositivo terminal móvel, existe um ambiente com recursos limitados ou diferentes devido, por exemplo, às capacidades de rede, tela, memória, processador, energia disponível armazenável com relação a tempo operacional realizável e terminais de

entrada/saída em comparação com um PC.

Também os usuários móveis têm tipicamente capacidades limitadas de entrada/saída, por exemplo, um pequeno bloco de entrada alfanumérico ou um pequeno dispositivo de tela, o que resulta
5 das dimensões exteriores dos dispositivos.

Segundo, o contexto de uso típico dos assim chamados aplicativos sem fios processando no referido dispositivo terminal móvel é muito diferente em relação ao de aplicativos sólido-rede-Internet que processam num computador pessoal.

10 Terceiro, conexões de rede disponíveis, tipicamente pelo ar, não são só consideravelmente mais lentas, seja em vista das influências atmosféricas sobre os canais de transmissão e fenômenos de propagação até aspectos de carga e sinal do canal para aspectos de ruído, mas são também mais dispendiosos.

15 Mas aqui, no campo do pagamento *online*, a maioria das características de um dispositivo terminal móvel, por exemplo, em vistas do tamanho em comparação com um computador pessoal torna-se imediatamente uma grande vantagem, quando combinadas em conjunto, por exemplo, usando modos de transmissão de uma maneira
20 cooperativa ou complementar em vista dos requisitos do aplicativo.

De acordo com uma modalidade da presente invenção relativa a uma transação de pagamento, por um lado, deve ser transmitida uma pequena quantidade de informações muito importantes com a maior segurança, em que o terminal móvel é preferentemente adequado
25 e, por outro lado, uma grande quantidade de informações de importância comparavelmente mais baixa deve ser transmitida, em que um computador pessoal é vantajoso.

Deste modo, o dispositivo móvel está idealmente adapta-

do para um suplemento de um computador pessoal ou mesmo uma solução *standalone* poderosa com características completas.

Em resumo, combinando uma comunicação híbrida que preenche tarefas complementares que são especificamente exigidas dentro de um aplicativo de pagamento, sendo o referido aplicativo formado processando de modo distribuído num sistema energizado por vários participantes, é proporcionado um método de pagamento *online* aperfeiçoado para identificação do usuário.

Por um lado, o referido método de pagamento é inovador para os parceiros cooperantes no sistema, em razão de baixo sobre custo relativo à preocupação principal e competência de núcleo do parceiro respectivo. O sistema é fácil de manter e proporciona um nível avançado de segurança contra uma despesa de custo comparativamente moderada.

Por outro lado, o referido método é de operação conveniente e simples para o usuário e não sobrecarrega o usuário com partes da transação que não são de nenhum interesse.

A Figura 2 ilustra uma modificação da Figura 1 noutra modalidade em que apenas o referido dispositivo terminal móvel 3 está presente. Tem, porém, a citada conexão 4 para dita Internet 5 e a referida conexão 17 para a citada rede de telefone móvel 16.

Num ponto, a Figura 2 é uma versão concentrada para a Figura 1 na medida em que a comunicação híbrida da Figura 1 é agora realizada somente num dispositivo, por exemplo, por um dispositivo terminal móvel, sozinho, usando padrões de interface diferentes. Numa modalidade adicional, o dispositivo móvel oferece a mesma funcionalidade ou uma funcionalidade comparável a um computador pessoal, de tal forma que, neste caso, o dispositivo móvel e o computador pessoais são ou comportam-se de modo igual.

A Figura 3 ilustra um diagrama de opções possíveis sobre como identificar e autenticar um cliente usando uma interface de rede.

Um bloco de geração de ID de transação 35 é conectado ou acoplado a um bloco de recebimento de rede 40.

5 O referido bloco de recebimento 40 é conectado quer aos blocos de envio de ID 50, 55 quer 60 por uma interface de navegador de rede 45.

Os blocos de envio de ID 50, 55 ou 60 são conectados por uma interface de telefone móvel 65 com um bloco de recebimento de dados de transação APC 70.

O referido bloco de recebimento 70 é conectado aos blocos de recebimento 80, 85 ou 90 por uma interface de telefone móvel 72. Também o bloco 70 é conectado a um bloco de recebimento de rede 95 via uma interface de navegador de rede 74.

15 Numa primeira etapa 35, o APC gera o código de ID de transação.

A seguir, na etapa 40, o cliente recebe o código de ID de transação via navegador da rede.

20 Via uma interface de rede mostrada por 45, ao usuário é proporcionada uma mensagem (não mostrada) para escolher uma opção para enviar um código de ID com o seu dispositivo terminal móvel. A seguir, o Cliente envia, como mostrado por 45, no seu dispositivo terminal móvel, por exemplo, usando a interface do navegador de rede, o código de ID de transação quer

25 - através do serviço de USSD, etapa 50, quer

- o cliente disca o código de ID de transação, etapa

55, ou

- o cliente envia o código de ID de transação por SMS, etapa 60.

5 Este código de ID de transação é enviado a partir do referido dispositivo terminal móvel para o APC via a interface de telefone móvel, como indicado pelo sinal de referência 65.

Na etapa 70, o código de ID de transação é recebido num lado do APC e o cliente é identificado e autenticado começando os procedimentos respectivos.

10 A seguir, o cliente recebe em seu dispositivo terminal móvel uma mensagem por uma das opções seguintes

- através do serviço de USSD, etapa 80 ou (e)

- escuta uma mensagem durante o telefonema via IVR (Resposta de Voz Interativa), etapa 85 ou (e)

15 - recebe uma mensagem de SMS, etapa 90, cada uma usando a interface de telefone móvel 72, quer a identificação e autenticação tenham sido bem sucedidas quer não.

20 Note-se que são possíveis também combinações das etapas supracitadas incluindo confirmações (não mostradas), como indicado por uma notação “ou (e)”.

Também alternativamente ou cumulativamente à mensagem de informação de que a identificação e a autenticação foram bem sucedidas ou não, o usuário obtém informações via o navegador de rede, etapa 95, usando a interface de rede 45.

25 A Figura 4 ilustra um diagrama de opções possíveis sobre

13

como identificar e autenticar um cliente usando uma interface de WAP.

Um bloco de geração de ID de transação 35 é conectado ou acoplado a um bloco de recebimento WAP 42.

O referido bloco de recebimento 42 é conectado quer a
5 blocos de envio de ID 50, 55 quer 60 por uma interface de navegador WAP 48.

Os blocos de envio de ID 50, 55 ou 60 são conectados por uma interface de telefone móvel 64 com um bloco de recebimento de dados de transação de APC 70.

10 O referido bloco de recebimento 70 é conectado a blocos de recebimento 80, 85 ou 90 por uma interface de telefone móvel 76. Também o bloco 70 é conectado a um bloco de recebimento WAP 98 via uma interface de navegador WAP 78.

Como mostrado na Figura 4, a mesma identificação de
15 usuário é apresentada como indicada pelos mesmos sinais de referência em comparação com a Figura 3.

Mas, ao invés um navegador de rede, uma interface de navegador WAP é usada para proporcionar ao usuário o código de ID de transação, conforme representado na etapa 42 usando 48. Até agora,
20 uma interface de navegador WAP é usada para informar o usuário na etapa 98 usando 78.

Na Figura 4, uma informação do usuário pode ser assegurada usando duas interfaces diferentes proporcionando informações para o referido navegador WAP 48 ou 78 e a interface de telefone móvel
25 64 ou 76. Também cada uma das citadas interfaces pode ser provida com a possibilidade de diferentes níveis de segurança ou métodos de transmissão etc.



Portanto, é possível um envio de mensagens usando modos de transmissão diferentes combinados com diferentes características de transmissão combinadas com diferentes interfaces.

5 Note-se também que uma combinação (não mostrada) de interfaces tais como um navegador de rede, um navegador WAP ou uma interface de telefone móvel é também possível. Portanto, é proporcionado usar qualquer mistura de diferentes padrões de interface ou mídia de transmissão de acordo com requisitos de um aplicativo distribuído.

10 Em vista funcional da Figura 3 e da Figura 4, respectivamente, um cliente que está conectado ao servidor de rede APC 9 para fazer um pagamento via Internet receberá um código de ID de transação com tempo limitado de vida.

15 Além disto, o usuário receberá também via seu navegador de rede/WAP instruções sobre como e onde enviar o código de ID de transação via seu dispositivo móvel. Tudo isso será mostrado a um cliente em sua rede ou navegador WAP de acordo com 40 ou 42, respectivamente.

20 Com o usuário enviando o procedimento do código de ID de transação de volta para o portal de rede móvel APC 10 via o seu dispositivo móvel 3, o número MSISDN do usuário é capturado num lado do APC de acordo com 70.

25 O número MSISDN é um identificador de equipamento do equipamento de rádio móvel individual, que é também enviado como uma característica de identificação, enquanto o equipamento está sendo usado. Dentro do procedimento inventado existem três opções ou modos possíveis, de acordo com 50, 55 ou 66, sobre como um cliente pode enviar o código de ID de transação para o portal de rede móvel APC 10. Suponhamos que o portal de rede móvel APC 10 tem algum número de dígitos abreviado como, por exemplo, "180", então são



possíveis os seguintes cenários:

- O cliente envia o código de ID de transação através de USSD (*180* transaction_ID_code#);
- O cliente disca o código de ID de transação com
5 prefixo de discagem (180transaction_ID_code);
- O cliente envia o código de ID de transação por SMS (sms “transaction_ID_code” para 180).

As transmissões possíveis de códigos de ID de transação diferem de um para o outro – o primeiro está usando o serviço de USSD
10 do operador móvel. A segunda opção usa um prefixo de discagem simples – isso significa que o cliente apenas disca o número do centro de APC adicionando um número de código de ID de transação de n dígitos.

O APC recebe um telefonema e reconhece o número de
15 prefixo de discagem, que é o número de código de ID de transação. A última opção usa SMS para transferir o número de código de ID de transação para o APC.

Quando o código de ID de transação é transmitido com
20 sucesso para o APC, a próxima fase é a identificação e autenticação do cliente.

Se esta parte do procedimento integral for bem sucedida, então, o cliente receberá instruções adicionais necessárias para finalizar o pagamento através do navegador de rede/WAP ou USSD ou SMS ou IVR ou combinação de todos os meios de comunicação possíveis mos-
25 trados por 80, 85 e 90 usando as interfaces 72, 74, 76 e 78.

Em caso oposto, quando for negada a autenticação do cliente, o cliente receberá as informações sobre isto através de um

dentre canais de comunicação possíveis (navegador de rede, navegador WAP, USSD, SMS ou IVR).

5 Fica entendido que o tipo de modo de saída que informa o usuário sobre o estado de sua identificação e autenticação (por exemplo, por serviço USSD, IVR, SMS, etapas 80, 85 e 90, respectivamente) pode responder ao tipo do modo de entrada selecionado de acordo com as etapas 50, 55 e 60 ou uso de um ajuste de *default* programável.

10 Comparando as informações do usuário em 40 com 70 em consideração ao tipo de interface de navegador usado, 45 ou 74 para um navegador de rede, respectivamente, a possibilidade de diferentes níveis de segurança ou métodos de transmissão etc., pode ser proporcionada dentro do mesmo padrão de interface.

15 Mas também entre diferentes padrões de interface e diferentes níveis de segurança, são possíveis métodos adequado de codificação e transmissão, neste caso, é possível um envio seguro de mensagens usando dois modos de transmissão diferentes combinados com diferentes características de transmissão.

20 Como os instrumentos de pagamento são normalmente protegidos com PIN, o procedimento de pagamento inventado inclui também dois cenários de implementação da transmissão de PIN.

Caso 1 - PIN Introduzido Depois da Identificação

25 Uma vez o cliente tenha terminado de comprar na loja virtual via rede/navegador WAP, a próxima etapa é o pagamento. Suponhamos que o cliente é usuário registrado do instrumento de pagamento móvel protegido por PIN. Este caso mostra (Figura 5a a 5c) um procedimento sobre como um cliente é identificado usando telefone móvel antes do pagamento real. Este diagrama mostra que o PIN é pedido depois de um cliente ser identificado.

Fases explicadas das Figuras 5a a 5c, começando pela Figura 5a:

Fase 1 - o Cliente Selecciona

o Método de Pagamento *Online*

5 O Cliente coleciona os artigos na cesta de compras e procede à saída, etapa 110. A partir daí, deve seleccionar o método de pagamento - o método de Pagamento *Online*.

Na etapa 120, a loja virtual do Comerciante então redireciona o cliente para a página da rede de APC e transfere, na etapa 130,
10 as informações necessárias sobre a ordem (que varejista, qual é o número de conta e o custo etc.)

Fase 2 – o Cliente Escolhe o Operador Móvel

O servidor de rede APC armazena as informações recebidas a partir da loja virtual na etapa 140 e pede ao cliente que selecione
15 o seu operador móvel (os operadores móveis têm prefixos diferentes, então as instruções são baseadas sobre que operador móvel o cliente selecciona). A mensagem é exibida na rede ou navegador WAP do cliente na etapa 150.

As informações sobre qual operador móvel o cliente
20 seleccionou na etapa 160 são, então, transferidas de volta para o servidor de rede APC na etapa 170.

Todas as informações APC que servidor de rede reuniu na etapa 180 são, então, remetidas na etapa 190 para o APC (número 9, 10 e 11; Figura 1 e Figura 2).

25

Fase 3 - Gerando o Código de ID de Transação

O APC gera um código de ID de transação na etapa 200 com tempo limitado de vida, (isto é como fica assegurado que o APC não fica sem códigos de ID)

5 Nesta etapa 200, o APC procura o código e prefixo de discagem (para USSD, discagem e SMS) com base no operador móvel do cliente e gera o código de USSD para o cliente.

Fase 4 – o Cliente Obtém o Código USSD

ou um Número de Discagem

10 O código é transferido a partir do APC para o servidor de rede APC na etapa 210, a partir de onde as instruções foram geradas na etapa 200 e, depois, exibidas para o cliente (via navegador de rede ou WAP) na etapa 220.

15 O Cliente tem uma opção na etapa 230 para não usar os instrumentos de pagamento de *default* e seleciona um diferente (via prefixo de discagem ou código adicional).

Fase 5 – o Cliente Envia o Código USSD ou Envia o SMS

(Contendo o Código de ID) ou Disca o Número

20 O cliente segue, então, as instruções e envia na etapa 240 o código de ID de transação exibido no seu navegador de rede ou WAP.

O código de ID de transação é transferido a partir do telefone móvel do cliente para o portal móvel do APC na etapa 250 enviando uma mensagem que é recebida no APC na etapa 260.

Fase 6 – o Cliente Obtém uma Resposta

O APC verifica na etapa 270 se o código de ID de transação (mostrado para o cliente) foi submetido ao APC.

Não: a Identificação falhou

Se o código de ID de transação não foi submetido a tempo
5 (antes que o código de ID de transação expire), o APC informa o subscritor do operador móvel na etapa 300 que o número de ID não foi corretamente enviado. O cliente recebe uma mensagem, em sua rede ou navegador WAP, etapa 310, de que o número não foi corretamente enviado. O cliente deve repetir o procedimento, etapas de 320 a 390,
10 entrando na fase 7 e, depois disso, retornando à etapa 190 na fase 3.

Fase 7 – a Identificação do Cliente Falhou

Na etapa 320, é esperado que o usuário clique a seguir. Na etapa 330, é pedido um estado a partir do referido APC pelo citado servidor de rede de dito APC. A seguir, a etapa 340 está enviando uma
15 mensagem a partir do referido servidor de rede do citado APC para dito APC para perguntar se o ID está certo. Na etapa 350, o servidor de rede do referido APC é informado pelo citado APC de que o número não foi enviado corretamente. A seguir, é feito o envio de uma mensagem a partir de dito APC para o referido servidor de rede do citado APC na
20 etapa 360 indicando que o ID não foi recebido. O usuário é informado na etapa 370 de que o número não foi corretamente enviado e ao usuário é pedido pelo citado servidor de rede de dito APC que repita o procedimento. Na etapa 380, é proporcionada uma mensagem ao referido usuário a ser recebida no seu navegador de rede ou WAP de que o
25 número não foi enviado corretamente, se o código de ID de transação não foi submetido a tempo antes que o citado código de ID de transação expirasse. É, então, esperado até que o usuário esteja clicando a seguir na etapa 390. O procedimento é repetido pelo usuário indo para a fase 3, etapa 190 (Figura 5a).

Sim: a Identificação teve sucesso - vai para a fase 9

Se o código de ID de transação foi submetido ao APC, o Subscritor Móvel é comparado com o Cliente *online*. Na etapa 280, o APC informa o subscritor do operador móvel de que o número de ID foi
5 corretamente enviado. O cliente recebe uma mensagem de que a identificação foi bem sucedida, etapa 290, procede para a etapa 400 na fase 8 (Figura 5b).

Fase 8 - Estado Pedido

O APC confere o estado do ID nas etapas de 410 a 430.

10 Em detalhe, na etapa 400, é aguardado que o usuário clique a seguir e o usuário é comparado como um subscritor móvel com o usuário *online*. A seguir, um estado a partir do referido APC pelo citado servidor de rede de dito APC é pedido na etapa 410. Uma mensagem é enviada na etapa 420 a partir do referido servidor de rede do
15 citado APC para dito APC para perguntar se o ID está certo. Na etapa 430, o controle é procedido depois que a referida identificação foi bem sucedida pelo citado APC e pedindo ao usuário que entre com o seu PIN para a conta selecionada.

Fase 9 – o PIN é Pedido a Partir do Cliente

20 O APC pede ao cliente que entre com o seu PIN do instrumento de Pagamento escolhido na etapa 435. O cliente entra o PIN em sua rede ou navegador WAP, na etapa 440, que é enviado para o APC na etapa 450.

Em detalhe, é feito o pedido de um Número de Identificação
25 ção Pessoal a partir do usuário na etapa 430. A seguir, é feito o pedido ao usuário de que introduza o Número de Identificação Pessoal de seu instrumento de pagamento escolhido na etapa 435. Na etapa 440, o

PIN é introduzido pelo usuário em seu navegador de rede ou WAP. Na etapa 450, é enviada uma mensagem a partir do dispositivo terminal móvel para o referido Servidor de rede do citado APC para transferir dito Número de Identificação Pessoal. Na etapa 460, o PIN é recebido a
5 partir do referido usuário pelo servidor de rede do APC e é transferido para o citado APC. Na etapa 470, é enviada uma mensagem a partir do Servidor de Rede de dito APC para o referido APC para transferir o citado PIN. O procedimento e a conferência do custeio dos custos necessários do instrumento de pagamento de dito usuário pelo referido
10 centro de autorização e processamento é feito na etapa 475.

Fase 10 – o PIN é Conferido

Se o PIN estiver em boa ordem, vai para a fase 11, etapa 560; se não, vai para a fase 9, etapa 440; o PIN está, então, sendo verificado diretamente no APC ou transferido a partir do APC para a
15 Instituição financeira.

No caso em que o PIN foi enviado para a Instituição Financeira na etapa 480, então, o PIN e outras informações são conferidas na etapa 500 se são válidas.

Se o PIN for inválido, as informações são enviadas para o APC na etapa 510. O APC, na etapa 540, informa o cliente sobre o PIN incorreto e pede que o cliente introduza o seu PIN corretamente, etapa
20 550.

Se o PIN for válido, a Instituição Financeira confere o saldo do cliente na fase 11, etapa 560.

25 Em detalhe (fase 10), é enviada uma mensagem a partir do referido APC para a citada instituição financeira para transferir os dados de transação, incluindo o número da conta, Número de Identificação Pessoal e o custo na etapa 480. O recebimento pela citada

instituição financeira de ditos dados de transação é feito na etapa 490. Na etapa 500, é feita a verificação sobre o número correto da Identificação Pessoal, pela referida instituição financeira.

Se o PIN estiver em boa ordem (sim), o processamento
5 procede para a fase 11, etapa 560. Se não (não), é enviada uma mensagem de erro na etapa 510 a partir da citada instituição financeira para dito APC de que o referido PIN está incorreto. Na etapa 520, a referida mensagem de erro é transferida ou remetida a partir de dito APC para o referido servidor de rede do citado APC.

10 Na etapa 530, é enviada uma mensagem de erro a partir do citado APC para dito servidor de rede do referido APC, informando que o citado Número de Identificação Pessoal é incorreto. Receber dita mensagem de erro e informar o usuário sobre o PIN incorreto pelo referido servidor de rede do citado APC feito na etapa 540. Na etapa
15 550, é emitido um pedido para o usuário para re-introduzir o Número de identificação pessoal. Na etapa 550, é exibida uma mensagem para o usuário de que o PIN que ele introduziu está incorreto. Nesta etapa 550, o usuário é também pedido para que reintroduza o seu PIN. A partir da etapa 550, o processamento retorna para a fase 9, etapa 440
20 (Figura 5a).

Fase 11 – o Saldo de Conta do Cliente

é Conferido na Etapa 560

25 Numa avaliação geral, se o saldo for baixo, o cliente pode repetir o procedimento escolhendo outro tipo de pagamento; vai para a fase 1.

Se o saldo for baixo, é enviada a informação para o APC. O APC informa o cliente sobre o seu estado de saldo de conta e pede-lhe que escolha outro tipo de pagamento.

Se o saldo for válido, é enviada a informação para o APC na etapa 650. Em detalhe, na etapa 560, é conferido se o saldo de conta é suficiente para custeamento pela instituição financeira. No caso de “não” (a conta não é suficiente), é enviada uma mensagem de erro a partir da instituição financeira para o APC para informar e indicar que o saldo de conta é insuficiente para custeamento. Na etapa 580, o APC transfere a referida mensagem de erro a partir do citado APC para dito servidor de rede do referido APC. Na etapa 590, é enviada uma mensagem de erro a partir do referido APC para o citado servidor de rede de dito APC informando que o saldo de conta é insuficiente para custeamento. Na Etapa 600, a referida mensagem de erro é recebida pelo citado servidor de rede do dito centro de autorização e processamento sobre o estado do saldo de conta e o usuário é informado. Na etapa 610, a mensagem de erro é exibida para o usuário. Também na etapa 610, uma opção para escolher outro tipo de pagamento (instrumento de pagamento) é exibida para o usuário. Possivelmente, o cliente pode ter uma conta que tenha um saldo suficiente para a transação. A seguir, na etapa 620, é conferida a escolha do usuário. Se o usuário escolheu cancelar o pagamento, o processo termina na etapa 630. Se o usuário escolher outro tipo de pagamento na etapa 640, o controle retorna para a fase 1 na etapa 100 voltando para o início. No caso de “sim” (conta suficiente), o processamento pula para a fase 12 para continuar com a etapa 650.

Fase 12 - Pagamento Confirmado Pelo Cliente

Em resumo, o APC pede ao cliente que confirme a ordem na etapa 680. O cliente confirma o pagamento, na etapa 700. Primeiro, é enviada uma mensagem na etapa 650 a partir da instituição financeira para o APC para informar que o saldo de conta é suficiente para custeamento. A seguir, a referida mensagem é enviada na etapa 660 a partir do citado APC para dito servidor de rede do referido APC. Na Etapa 670, a mensagem é enviada a partir do citado APC para dito

30

servidor de rede do referido APC para informar que o saldo de conta é suficiente para custeamento. O recebimento da citada mensagem e o pedido a dito usuário que confirme o seu pagamento é feito na etapa 680 pelo referido servidor de rede do citado centro de autorização e processamento. Na etapa 690, é esperada a confirmação do pagamento pelo usuário. Finalmente, o processo de pagamento é saído por confirmação de dito usuário na etapa 700.

Caso 2 – o PIN Entrou Antes da Identificação

Este caso mostra (da Figura 6a até 6c) um procedimento sobre como um cliente é identificado usando o telefone móvel antes do pagamento real. Este diagrama mostra que o PIN é pedido antes de um cliente ser identificado. Nele, as fases 9 e 10 da Figura 5b e 5c são diferentes em que o procedimento continua a partir da fase 8, última etapa (430) até a fase 10, primeira etapa (480).

Fase 10 – Verificação de PIN

Uma mensagem é enviada na etapa 480 a partir do referido centro de autorização e processamento para a citada instituição financeira para transferir os dados de transação, incluindo o número de conta, o Número de Identificação Pessoal e o custo;

ditos dados de transação são recebidos pela referida instituição financeira na etapa 490 e conferidos na etapa 500, se o Número de Identificação Pessoal estiver correto;

se ele estiver certo (sim), o processamento procede para fase 11, etapa 560, de outra forma, é enviada uma mensagem de erro na etapa 510 a partir da citada instituição financeira para dito APC de que o referido PIN (Número de Identificação Pessoal) está incorreto. A mensagem de erro é remetida na etapa 520 a partir do citado APC para dito servidor de rede APC.

A seguir, na etapa 530, é enviada uma mensagem de erro a partir do referido APC para o citado servidor de rede APC de que dito PIN está incorreto.

5 Na etapa 540, o servidor de rede APC recebe a mensagem de erro e informa o usuário sobre o PIN incorreto.

Um pedido é emitido na etapa 550 para o usuário para reintroduzir o PIN.

10 A seguir, na etapa 550, é exibida uma mensagem para o usuário de que o Número de Identificação Pessoal que ele introduziu estava incorreto e é-lhe pedido que reintroduza o seu PIN.

O processamento retorna à fase 9, etapa 440.

Fase 9 - Pedido de PIN

Na etapa 440, o usuário introduz um PIN no seu navegador de rede ou WAP.

15 A seguir, é enviada uma mensagem na etapa 450 a partir do dispositivo terminal móvel para o referido servidor de rede do citado APC para transferir dito Número de Identificação Pessoal.

O servidor de rede APC recebe, na etapa 460, o PIN do usuário e transfere-o para o APC.

20 Na etapa 470, é enviada uma mensagem a partir do servidor de rede APC para o referido APC para transferir o citado PIN;

o processamento continua na fase 8, última etapa 430.

“Dispositivo Terminal Móvel e Respectivos Métodos de Operação,

Loja de Rede de Comerciante, Centro de Autorização e

Processamento, Sistema de Parceiros Múltiplos, Clientes e

Servidores em Rede Cliente-Servidor e em Sistema de Parceiros

5 **Múltiplos, Produto de Programa de Computador Contendo Código**

de Programa, Meio Legível em Computador, Sinal de Dados

Modulados ou Sinal de Dados de Computador, Sistema de Permuta

de Dados de Transações e Participante”

Reivindicações

10 **1 - Dispositivo Terminal Móvel**, (3), tendo uma unidade de memória (3a) e um dispositivo de interface (3b) que é conectável de modo liberável a um sistema de parceiros múltiplos (7, 9, 15) e capaz de uma comunicação nele, **caracterizado**

15 por que a referida comunicação é proporcionada por um terminal frontal formado pelo referido dispositivo terminal móvel (3) em combinação com um dispositivo de computador pessoal (2) e um terminal posterior formado por um parceiro do citado sistema de parceiros múltiplos via modos de comunicação, sendo dita comunicação adequada para executar transações de dados com requisitos variantes de
20 segurança, de tal modo que as partes complementares ou partes dentro de um aplicativo distribuído, sendo processadas dentro de um sistema de parceiros múltiplos, são executadas dependentes de seus requisitos de segurança atuais,

25 por que a referida comunicação é usada para permutar informações usando os citados modos de comunicação de característi-

33

cas diferentes e variantes (4, 6, 12, 17, 13) usando diferentes canais de comunicação e diferentes padrões ou protocolos de interface.

2 - **Dispositivo Terminal Móvel**, de acordo com a Reivindicação 1, **caracterizado** por que o dispositivo (3) é operado em combinação com um dispositivo de computador pessoal (2), por que o referido primeiro modo de comunicação (4) é proporcionado por uma rede de comunicação de Internet (5) e o citado segundo modo de comunicação é proporcionado por uma rede de telefone móvel (16), formando ditos modos de comunicação em conjunto uma capacidade de comunicação híbrida em feixe (18).

3 - **Dispositivo Terminal Móvel**, de acordo com a Reivindicação 1 ou 2, **caracterizado** por que é proporcionada uma comunicação segura e por que pelo menos um dos referidos modos de comunicação é seguro.

4 - **Dispositivo Terminal Móvel**, de acordo com qualquer uma das Reivindicações precedentes, **caracterizado** por que pelo menos um dos modos de comunicação é ou está em efeito igual para uma comunicação ponto-a-ponto para um receptor seguro que é parte do referido sistema de parceiros múltiplos.

5 - **Dispositivo Terminal Móvel**, de acordo com a qualquer uma das Reivindicações precedentes, **caracterizado** por que o referido dispositivo terminal móvel (3) e o citado dispositivo de computador (2), respectivamente, é provido, cada um, com uma interface de rede ou com uma interface de WAP ou uma combinação genérica de ditas interfaces, formando um padrão de interface de combinação cooperante.

6 - **Dispositivo Terminal Móvel**, de acordo com qualquer uma das Reivindicações precedentes, operado no referido sistema de parceiros múltiplos, que contém

o citado dispositivo terminal móvel,

34

dito dispositivo de computador pessoal,

uma loja de rede virtual de um comerciante,

um centro de autorização e processamento e

uma instituição financeira,

- 5 **caracterizado** por que o referido terminal móvel compreende um meio de interface para acoplar de modo liberável o citado dispositivo terminal móvel para dito sistema de parceiros para permutar informações de transação.

- 10 **7 - Loja de Rede de Comerciante**, no referido sistema de parceiros múltiplos segundo qualquer uma das Reivindicações precedentes, caracterizado por que tem uma interface capaz de comunicação no referido sistema de parceiros, em que a comunicação é realizada pela Internet.

- 15 **8 - Centro de Autorização e Processamento**, no referido sistema de parceiros múltiplos, segundo qualquer das Reivindicações precedentes, tendo uma interface capaz de comunicação no citado sistema de parceiros, caracterizado por que a referida interface é formada pelos subsistemas seguintes:

um servidor de rede para comunicação de Internet,

- 20 um portal de rede móvel para comunicação com uma rede de telefone móvel e

um servidor de dados para comunicação com uma instituição financeira.

- 25 **9 - Instituição Financeira**, num sistema de parceiros múltiplos, segundo qualquer uma das Reivindicações precedentes, **caracterizado**

38

por que tem uma interface capaz de comunicação no referido sistema de parceiros.

5 **10 - Sistema de Parceiros Múltiplos**, para permuta de transações financeiras, **caracterizado** por que cada um dos referidos participantes de acordo com as Reivindicações de 7 a 9, respectivamente, é capaz de operar de acordo com as características correspondentes das Reivindicações de 1 a 6, respectivamente.

11 - Cliente em Rede Cliente-Servidor, caracterizado por que compreende:

10 o referido dispositivo terminal móvel de acordo com as Reivindicações de 1 a 6 tendo uma unidade de memória que é externa a um servidor.

12 - Cliente em Rede Cliente-Servidor, caracterizado por que compreende:

15 o referido dispositivo terminal móvel e o citado computador pessoal de acordo com as Reivindicações de 1 a 6, tendo, cada um, uma unidade de memória que é externa a um servidor que forma uma configuração de cliente híbrido.

20 **13 - Cliente híbrido em Sistema de Parceiros Múltiplos**, de acordo com qualquer das Reivindicações de 1 a 6, **caracterizado** por que o referido cliente híbrido é operado por uma inteligência humana normal na Terra, um usuário.

25 **14 - Servidor em Rede Cliente-Servidor, caracterizado** por que um servidor é um participante de um sistema de parceiros múltiplos de acordo com as Reivindicações de 7 a 9.

15 - Servidor em Rede Cliente-Servidor, caracterizado por que um servidor é uma entidade não transparente e corresponde a uma plurali-

dade de servidores formados pelo sistema de parceiros múltiplos como um todo, tendo participantes de acordo com a Reivindicação 6, exceto o cliente.

16 - Método de Operação de Dispositivo Terminal Móvel em Procedimento de Pagamento, caracterizado por que compreende as etapas seguintes:

escolher o método de pagamento num aplicativo de Internet de uma loja de rede virtual (7);

10 ativar um aplicativo de um servidor de rede (9) de um centro de autorização e processamento (8) para pagamento;

passar todos os dados de transação de pagamento necessários a partir do referido aplicativo de Internet da dita loja de rede virtual (7) para o referido centro de autorização e processamento (8),

15 em que os citados dados de transação incluem uma quantia, um número de referência de conta;

proporcionar um código de ID de transação para o usuário,

20 em que o navegador de rede exibe para o usuário o aplicativo de servidor do dito centro de autorização e processamento (8) e em que o referido código de ID de transação é gerado no citado centro de autorização e processamento (8);

enviar o citado código de ID de transação pelo usuário via seu telefone móvel 3 para um portal de rede móvel (10) de dito centro de autorização e processamento (8);

25 obter um MSISDN (um número de rede digital de serviços integrados de subscritor móvel), um identificador de equipamento do

388
P

referido telefone móvel individual (3) e o código de ID de transação, em que o citado MSISDN é também enviado como uma característica de identificação, ao mesmo tempo em que dito telefone móvel (3) está sendo usado pelo referido portal de rede móvel (10) do citado centro de
5 autorização e processamento (8);

informar um usuário (1) pelo dito centro de autorização e processamento (8) sobre um recebimento bem sucedido do código de ID de transação via seu telefone móvel (3) ou via um navegador de rede num PC (2) do referido usuário (1) ou via ambos;

10 estabelecer conexões de Internet seguras (4, 12) entre o referido PC (2) do usuário (1) e o citado servidor de rede (9) de dito centro de autorização e processamento (8) para ativar para o referido usuário (1) uma seleção segura de um instrumento de pagamento no aplicativo de servidor da citada rede (9) de dito centro de autorização e
15 processamento (8) e uma transmissão de número de identificação pessoal seguro, que é ligado ao referido instrumento de pagamento para o citado centro de autorização e processamento (8);

ativar dita conexão (14) para uma instituição financeira (15) no lado do referido centro de autorização e processamento (8) para
20 a autorização do citado pagamento;

confirmar a transação de pagamento do usuário (1) via sua navegador de rede, no caso, se for aprovada uma autorização de um lado de dita instituição financeira (15) e/ou a partir do referido servidor de rede (9) do citado centro de autorização e processamento (8);

25 gravar todos os dados necessários sobre a transação em dito servidor de dados (11) do referido centro de autorização e processamento (8) e, além disso, enviar todos os dados necessários para a citada loja de rede (7) do comerciante e para a plataforma de dados de dita instituição financeira (15).

17 - Método de Operação de Dispositivo Terminal Móvel, numa identificação e autenticação de usuário do referido procedimento de pagamento, **caracterizado** por que compreende as seguintes etapas:

5 gerar (35) pelo citado centro de autorização e processamento (8) um código de ID de transação;

 receber dito código de ID de transação via um navegador de rede (40, 45) ou um navegador WAP (42, 48) de um dispositivo terminal móvel;

 enviar o referido código de ID de transação (65; 64);

10 receber o citado ID de transação (70) num lado de dito centro de autorização e processamento e identificar e autenticar o usuário; e

 proporcionar uma mensagem (80) para o usuário, quer a identificação e a autenticação tenham tido sucesso quer não.

15 **18 - Método de Operação de Dispositivo Terminal Móvel**, numa identificação de usuário e autenticação do referido procedimento de pagamento, de acordo com a Reivindicação 15, **caracterizado** por que a etapa de enviar o referido código de ID de transação (45; 48) é executado quer através de um serviço de Dados de Serviço Suplementar Não
20 Estruturado (50) quer digitando o código de ID de transação (55) pelo usuário

 quer enviando o código de ID de transação (60) com SMS.

25 **19 - Método de Operação de Dispositivo Terminal Móvel**, numa identificação e autenticação de usuário do referido procedimento de pagamento de acordo com a Reivindicação 15 e 16, **caracterizado** por que a etapa de proporcionar uma mensagem para o usuário (72; 76) é realizada

quer através de um serviço de Dados de Serviço Suplementar Não Estruturado (80), quer ouvindo uma mensagem durante o telefonema (85) via uma Resposta de Voz Interativa,

quer recebendo uma mensagem de Serviço de Pequenas

5 Mensagens (90)

quer obtendo informações via um navegador de rede (95, 74) ou um navegador WAP (98, 78) ou uma combinação dos precedentes.

20 - Método de Operação de Dispositivo Terminal Móvel, numa
10 identificação de usuário e autenticação do referido procedimento de pagamento, no caso que um Número de Identificação Pessoal é introduzido - depois - de uma identificação, **caracterizado** por que compreende as etapas de:

(fase 1) introduzir no processo de pagamento (100) no
15 deslocamento do citado usuário para a saída com a sua cesta de compras;

selecionar o método de pagamento *online*
(110) pelo usuário; redirecionar o usuário (120) para a página da rede do dito centro de autorização e processamento pelo referido comerciante
20 da loja de rede virtual e enviar uma mensagem (130) a partir da loja de rede virtual para o citado centro de autorização e processamento para transferir as informações necessárias sobre a ordem, em que ditas informações incluem um nome, número de conta e o custo de um varejista;

25 (fase 2) armazenar as informações (140) recebidas a partir da referida loja de rede virtual pelo citado servidor de rede de dito centro de autorização e processamento e pedir ao usuário que selecione o seu operador móvel;

proporcionar uma mensagem (150) que é exibida no navegador de rede ou WAP do usuário;

selecionar um operador móvel pretendido (160) pelo referido usuário e esperar até o próximo clique pelo usuário;

5 enviar uma mensagem (170) a partir do citado dispositivo terminal móvel de volta para dito servidor de rede do referido centro de autorização e processamento para transferir informações sobre qual operador móvel foi selecionado pelo usuário;

10 remeter todas as informações (170) do citado servidor de rede do dito centro de autorização e processamento reunidas para os todos os subsistemas para o referido centro de autorização e processamento;

15 (fase 3) enviar uma mensagem (190) para proporcionar informações prontas para introdução, incluindo o citado operador móvel selecionado, um nome do local da loja de rede, dito número de conta e o referido custo;

gerar um código de ID de transação (200) com tempo limitado de vida pelo citado centro de autorização e processamento usando ditas informações;

20 procurar o código e prefixo de discagem (200) pelo referido centro de autorização e processamento, com base no operador móvel de usuário;

gerar um código de Dados de Serviço Suplementar Não Estruturado (200) para o citado usuário;

25 (fase 4) enviar uma mensagem (210) a partir de dito centro de autorização e processamento para o referido servidor de rede do citado centro de autorização e processamento para proporcionar dito



código de Serviço Suplementar Não Estruturado ou número de discagem para o usuário (220);

exibir (220) o código de Serviço Suplementar Não Estruturado gerado ou número de discagem e uma pluralidade de instrumentos de pagamento para o usuário pelo servidor de rede do referido centro de autorização e processamento;

proporcionar uma opção (230) para o usuário não usar instrumentos de pagamento de *default* e proporcionar uma opção para selecionar um instrumento de pagamento diferente de uma pluralidade de instrumentos de pagamento;

(fase 5) introduzir as informações pedidas (240) que são exibidas na página de rede ou WAP pelo citado usuário no dispositivo terminal móvel de dito usuário seguindo as instruções seguintes;

enviar uma mensagem para transferir o referido código de ID de transação (250) exibido no navegador de rede ou WAP do citado usuário a partir de dito dispositivo terminal móvel do usuário para o referido portal de rede móvel do citado centro de autorização e processamento;

receber um pedido (260) a partir de dito subscritor de operador móvel incluindo o número de ID e um número de instrumento de pagamento opcional;

(fase 6) verificar (270) se o código de ID de transação (exibido para o referido usuário) pelo citado centro de autorização e processamento foi submetido a dito centro de autorização e processamento;

se (sim), o número foi enviado corretamente e na hora certa:

informar o operador móvel (280) pelo referido centro de autorização e processamento que o número de ID foi enviado corretamente;

5 informar o usuário (290) que a identificação foi bem sucedida e pedir que o usuário proceda a um *input* e siga as instruções;

proceder com o processamento (400) na fase 8;

de outra forma (não)

10 informar o operador móvel (300) pelo citado centro de autorização e processamento que o número de ID não foi enviado corretamente;

15 informar o usuário (310) que o número introduzido era inválido e pedir que o usuário proceda a um *input* e siga as instruções;

(fase 7) a identificação falhou

aguardar até o próximo clique (320) pelo usuário;

20 pedir um estado (330) a partir do citado centro de autorização e processamento pelo dito servidor de rede do referido centro de autorização e processamento;

25 enviar uma mensagem (340) a partir do citado servidor de rede de dito centro de autorização e processamento para o referido centro de autorização e processamento para indagar se o ID está correto;

43

informar o servidor de rede (350) do citado centro de autorização e processamento pelo dito centro de autorização e processamento que o número não foi enviado corretamente;

5 enviar uma mensagem (360) a partir do referido centro de autorização e processamento para o citado servidor de rede de dito centro de autorização e processamento que o ID não foi recebido;

10 informar o usuário (370) que o número não foi enviado corretamente e pedir que o usuário repita o procedimento pelo referido servidor de rede do citado centro de autorização e processamento;

15 prover uma mensagem (380) para dito usuário a ser recebida em seu navegador de rede ou WAP que o número não foi enviado corretamente, se o código de ID de transação não foi submetido a tempo antes que o referido código de ID de transação expirasse;

esperar até o próximo clique (390) pelo usuário;

20 repetir o procedimento pelo usuário indo para fase 3 (190);

(fase 8) esperar até o próximo clique (400) pelo usuário e

comparar o usuário como subscritor móvel com o usuário *online*;

25 pedir um estado (410) a partir do citado centro de autorização e processamento por dito servidor de rede do referido centro de autorização e processamento;

5 proceder (430) depois que a referida identificação foi bem sucedida pelo citado centro de autorização e processamento e pedir que o usuário introduza o seu Número de Identificação Pessoal para a conta selecionada;

pedir que o usuário (435) introduza o Número de Identificação Pessoal de seu instrumento de pagamento escolhido;

enviar uma mensagem (450) a partir do dispositivo terminal móvel para dito Servidor de rede do referido centro de autorização e processamento para transferir o citado Número de Identificação Pessoal;

25 enviar uma mensagem (470) a partir do Servidor de rede do citado centro de autorização e processamento para dito centro de autorização e processamento para transferir o referido Número de Identificação Pessoal; proceder e verificar (475) o custea-

mento dos custos necessários do instrumento de pagamento do citado usuário pelo dito centro de autorização e processamento;

(fase 10) enviar uma mensagem (480) a partir do referido centro de autorização e processamento para a citada instituição financeira para transferir dados de transação, incluindo número de conta, Número de Identificação Pessoal e custo;

receber (490) pela citada instituição financeira ditos dados de transação e verificação (500), se o Número de Identificação Pessoal estiver correto;

se ele estiver correto (sim), proceder para a fase 11 (560),

de outra forma

enviar uma mensagem de erro (510) a partir da referida instituição financeira para dito centro de autorização e processamento de que o referido Número de Identificação Pessoal está incorreto;

transferir a citada mensagem de erro (520) a partir de dito centro de autorização e processamento para o referido servidor de rede do citado centro de autorização e processamento;

enviar uma mensagem de erro (530) a partir de dito centro de autorização e processamento para o referido servidor de rede do citado centro de autorização e processamento que dito Número de Identificação Pessoal está incorreto;

receber a referida mensagem de erro e informar o usuário (540) sobre o Número de Identificação Pessoal incorreto pelo citado servidor de rede de dito centro de autorização e processamento;

emitir um pedido para o usuário (550)
reintroduzir o Número de Identificação Pessoal;

exibir uma mensagem (550) para o usuário
de que o Número de Identificação Pessoal que introduziu é incorreto e
5 pedir-lhe que reintroduza o seu Número de Identificação Pessoal;

retornar para a fase 9, etapa 2 (440);

(fase 11) verificar (560) se o saldo de conta é suficiente
para custeio;

se a conta for suficiente (sim), proceder para a fase 12 (650);

10 de outra forma (não)

enviar uma mensagem de erro (570) a
partir da instituição financeira para o centro de autorização e proces-
samento para informar que o saldo de conta é insuficiente para custeio;

transferir a referida mensagem de erro
15 (580) a partir do citado centro de autorização e processamento para dito
servidor de rede do referido centro de autorização e processamento;

enviar uma mensagem de erro (590) a
partir do citado centro de autorização e processamento para dito servi-
dor de rede do referido centro de autorização e processamento que saldo
20 de conta é insuficiente para custeio;

receber a citada mensagem de erro e
informar dito usuário (600) sobre o estado do saldo de conta pelo
referido servidor de rede do citado centro de autorização e processamen-
to;

25

exibir para dito usuário a referida mensa-

exibir para o citado usuário uma opção para escolher outro tipo de pagamento e uma opção para cancelar o pagamento (610);

se o usuário tiver escolhido cancelar o pagamento, terminar o processamento (630);

10 (fase 12) enviar uma mensagem (650) a partir da instituição financeira para o centro de autorização e processamento para informar que o saldo de conta é suficiente para custeio;

enviar uma mensagem (670) a partir do referido centro de autorização e processamento para o citado servidor de rede de dito centro de autorização e processamento para informar que o saldo de conta é suficiente para custeio;

(690) pelo usuário; e aguardar até confirmação do pagamento

25 sair do processo de pagamento após

confirmação (700) do citado usuário.

21 - Método de Operação de Dispositivo Terminal Móvel, de acordo com a Reivindicação 18, no caso em que um Número de Identificação Pessoal é introduzido - antes - uma identificação, **caracterizado** por

5 que as fases 9 e 10 são permutadas e modificadas enquanto o procedimento continua a partir da fase 8, última etapa (430) para a fase 10, primeira etapa (480):

(fase 10) enviar uma mensagem (480) a partir do referido centro de autorização e processamento para a citada instituição financeira para transferir dados de transação, incluindo o número de conta,

10 o Número de Identificação Pessoal e o custo;

receber por dita instituição financeira (490) os referidos dados de transação e verificação (500), se o Número de Identificação Pessoal estiver correto;

15 se ele estiver correto (sim), proceder para a fase 11 (560), de outra forma

enviar uma mensagem de erro (510) a partir da citada instituição financeira para dito centro de autorização e processamento que o referido Número de Identificação Pessoal está incorreto;

20 transferir a referida mensagem de erro (520) a partir de do citado centro de autorização e processamento para dito servidor de rede do referido centro de autorização e processamento;

enviar uma mensagem de erro (530) a partir do citado centro de autorização e processamento para dito servidor de rede do

25 referido centro de autorização e processamento que o citado Número de Identificação Pessoal está incorreto;

receber dita mensagem de erro e informar o usuário (540)

sobre o Número de Identificação Pessoal incorreto pelo referido servidor de rede do citado centro de autorização e processamento;

emitir um pedido para que o usuário (550) reintroduza o Número de Identificação Pessoal;

5 exibir uma mensagem (550) para o usuário de que o Número de Identificação Pessoal que ele introduziu está é incorreto e pedir-lhe que reintroduza o seu Número de Identificação Pessoal; retornando à fase 9, etapa 2 (440)

10 (fase 9) introduzir um Número de Identificação Pessoal (440) pelo usuário em seu navegador de rede ou WAP;

enviar uma mensagem (450) a partir do dispositivo terminal móvel para dito servidor de rede do referido centro de autorização e processamento para transferir o citado Número de Identificação Pessoal;

15 receber o Número de Identificação Pessoal (460) a partir de dito usuário pelo servidor de rede do centro de autorização e processamento e transferi-lo para o referido centro de autorização e processamento;

20 enviar uma mensagem (470) a partir do servidor de rede do citado centro de autorização e processamento para dito centro de autorização e processamento para transferir o referido Número de Identificação Pessoal; e proceder para a fase 8, última etapa (430).

22 - Produto de Programa de Computador Contendo Código de Programa, que está na forma de um meio legível em máquina com um
25 código de programa nele armazenado ou na forma de um sinal propagável ou não radioativo, **caracterizado** por que compreende uma representação de código de programa, em que o referido código de programa



é disposto para realizar um método de acordo com uma das Reivindicações precedentes, quando executado num microcontrolador, sistema de computador, *notebook*, assistente de dados pessoais, telefone inteligente, depois de operação de carga de uma estrutura de dados numa
5 memória funcional ou principal de um computador ou uma pluralidade de computadores de uma rede de computadores ou operando num cliente numa rede cliente-servidor.

23 - Meio Legível em Computador, caracterizado por que nele está armazenada uma estrutura de dados, executando a referida estrutura
10 de dados o citado método de acordo com uma das Reivindicações precedentes depois de uma operação de carga de dita estrutura de dados numa memória funcional ou principal de um computador ou uma pluralidade de computadores de uma rede de computador.

24 - Sinal de Dados Modulados ou Sinal de Dados de Computador, caracterizado por que é corporificado num portador de ondas que
15 consiste em instruções executáveis para execução de um método num sistema de computador de uma rede de computadores ou uma pluralidade de computadores de uma rede de computadores de acordo com qualquer das Reivindicações precedentes.

25 - Sistema Para Permuta de Dados de Transações, que compreende:

um usuário (1);

um computador pessoal (2) do referido Usuário (1) tendo uma conexão de Internet (4) para a Internet (5);

25 um telefone móvel (3) tendo uma conexão móvel (17) para

uma rede de telefone móvel (16);

uma loja de rede virtual (7) de um comerciante tendo

uma conexão de Internet (6) para a citada Internet (5); e

um centro de autorização e processamento (8)

tendo uma primeira conexão (12) para dita Internet (5),

tendo uma segunda conexão (13) para a referida rede de
5 telefone móvel e

tendo uma terceira conexão (14) para uma Instituição
financeira 15,

caracterizado por que o citado centro de autorização e
processamento (8) está contendo um servidor de rede (9), um portal de
10 rede móvel (10) e um servidor de dados (11).

26 - Participante em Sistema, segundo uma das Reivindicações
precedentes, **caracterizado** por que o referido participante pode receber
e processar informações entrantes, enviar e passar informações de
saída, adequado para o respectivo padrão de interface usado no respec-
15 tivo modo de comunicação.

27 - Participante em Sistema, de acordo com a Reivindicação 26,
caracterizado por que executa ou contribui para um método de uma
das Reivindicações precedentes num aplicativo distribuído sobre o
sistema de parceiros.

20 **28 - Participante em Sistema**, de acordo com a Reivindicação 26,
caracterizado por que o uso do referido modo de comunicação é otini-
zado para a largura de faixa, características de canal e propagação,
incluindo encriptação de dados e uma conexão de participantes ponto-
a-ponto ou ponto-para-multipontos.

82

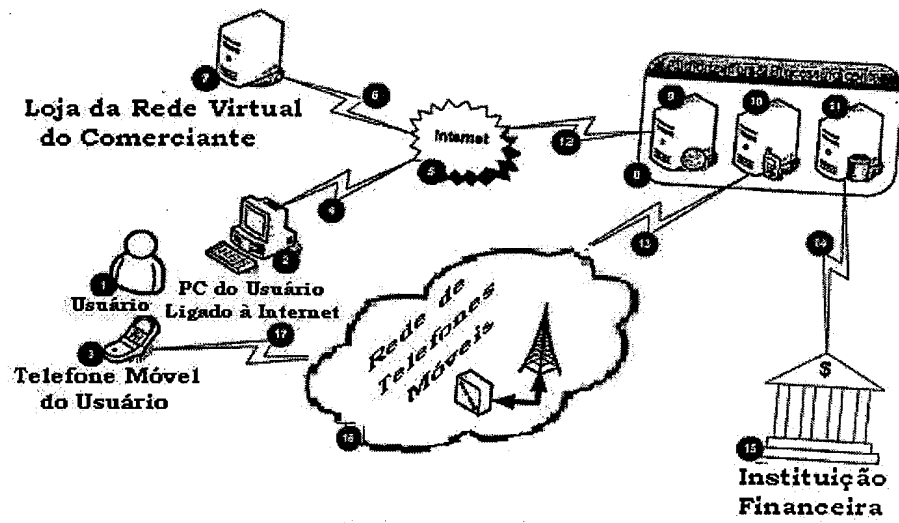


Figura 2

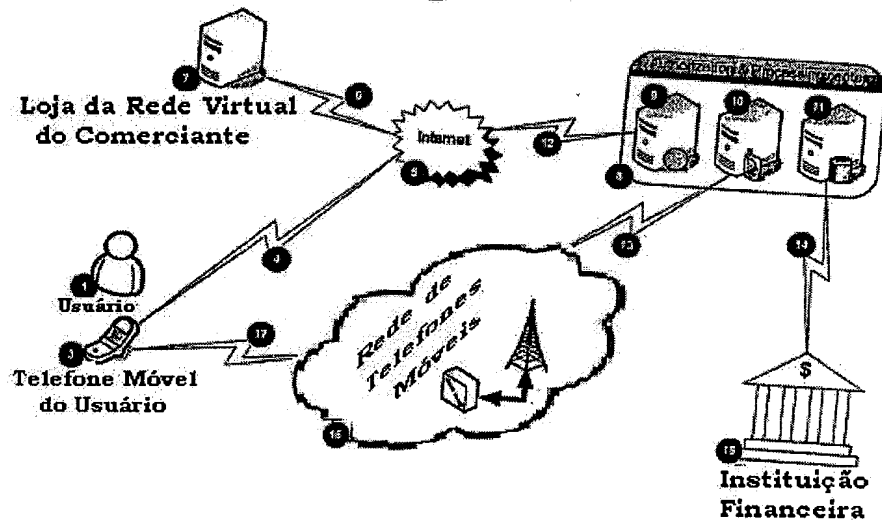
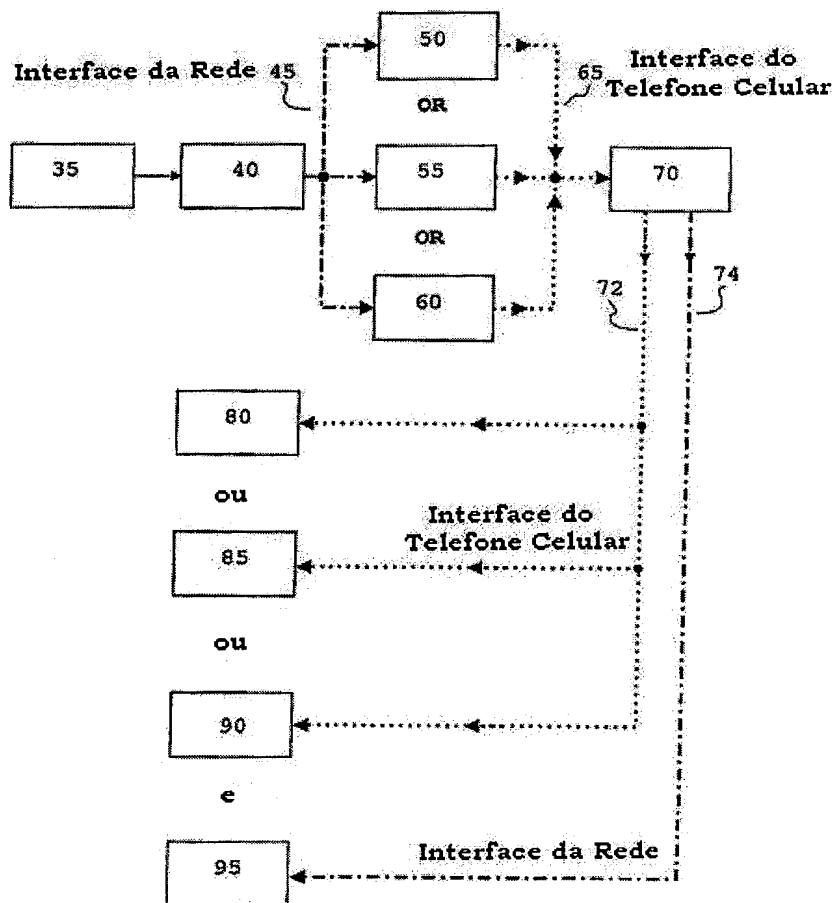
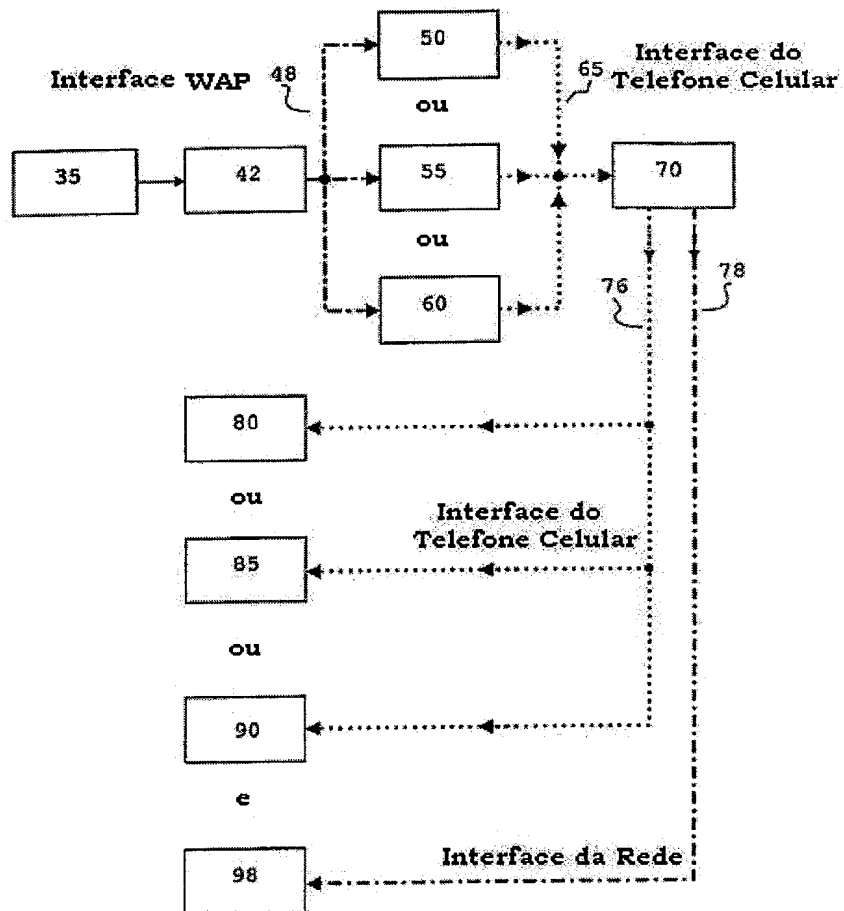


Figura 1

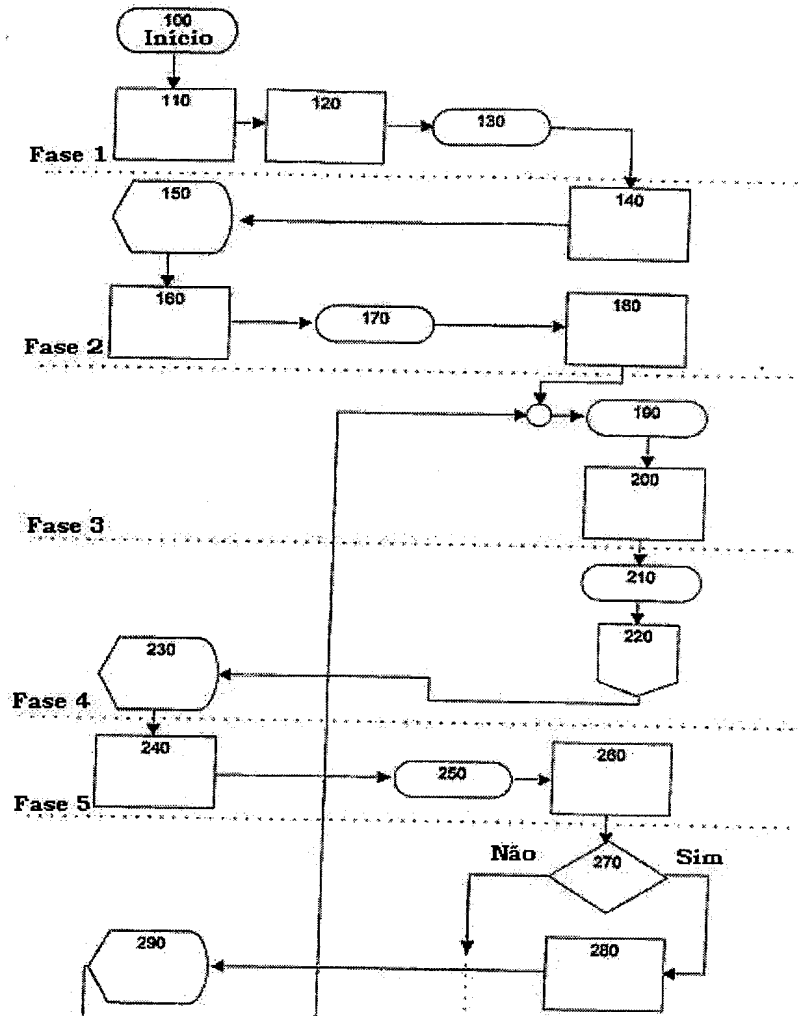
527

**Figura 3**

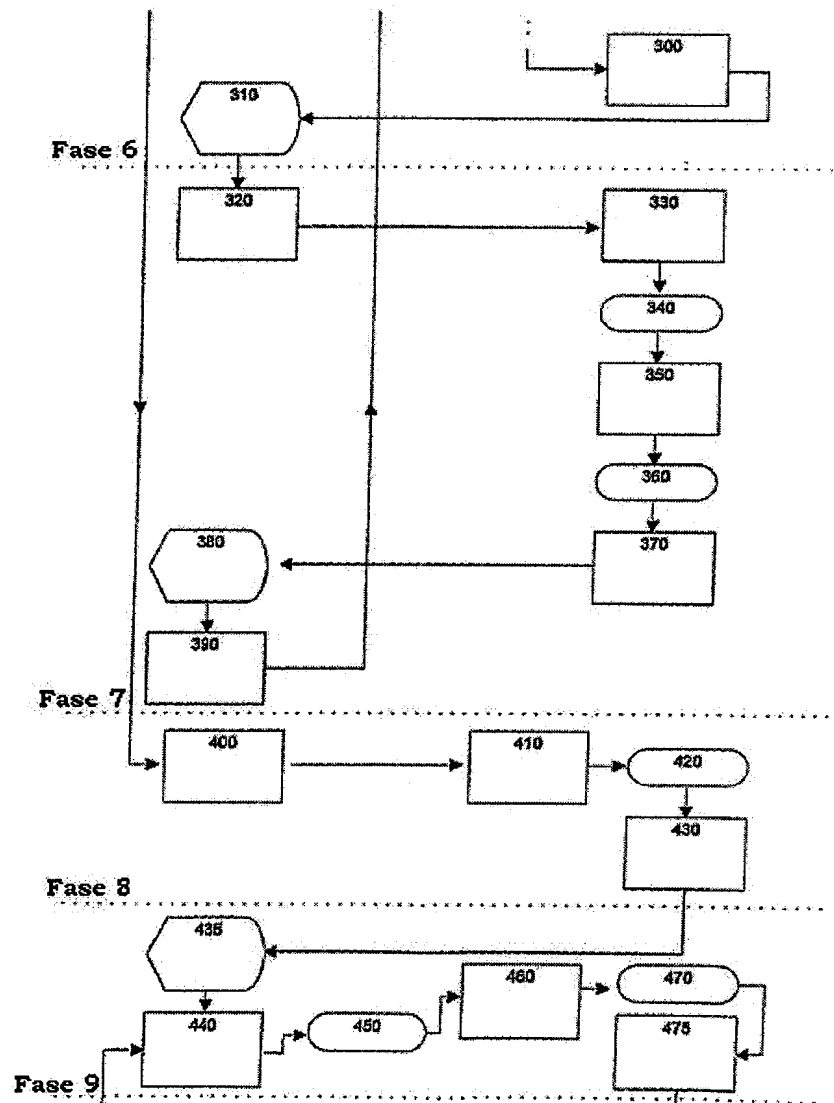
54

**Figura 4**

557

**Figura 9**

56

**Figura 5b**

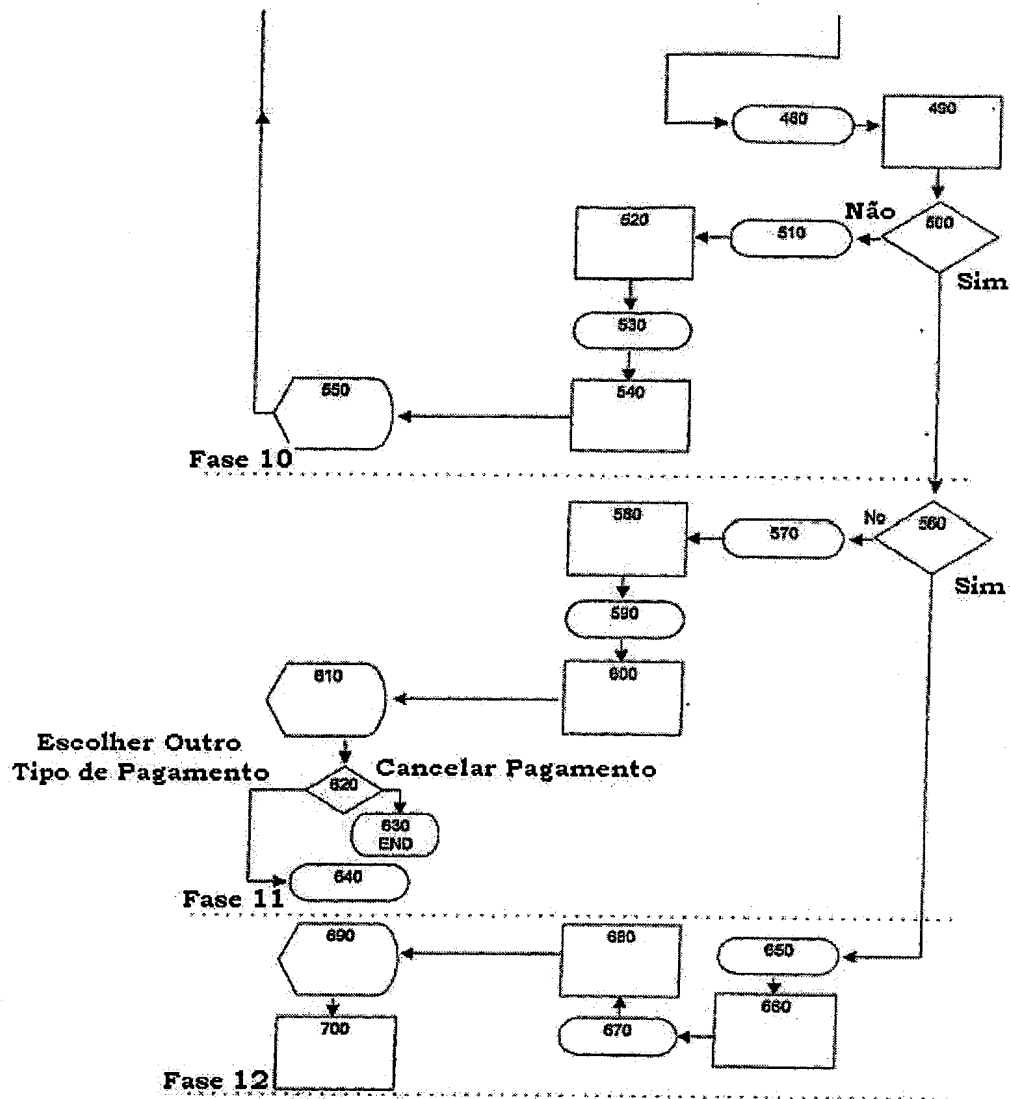


Figura 5c

SP

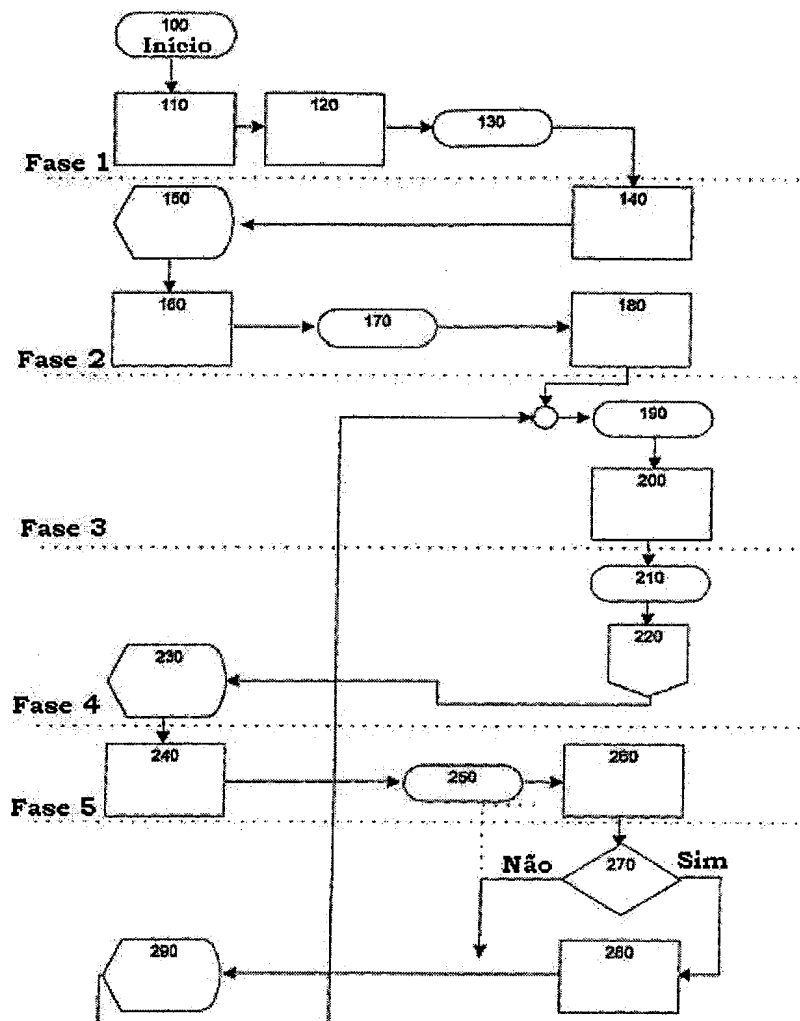
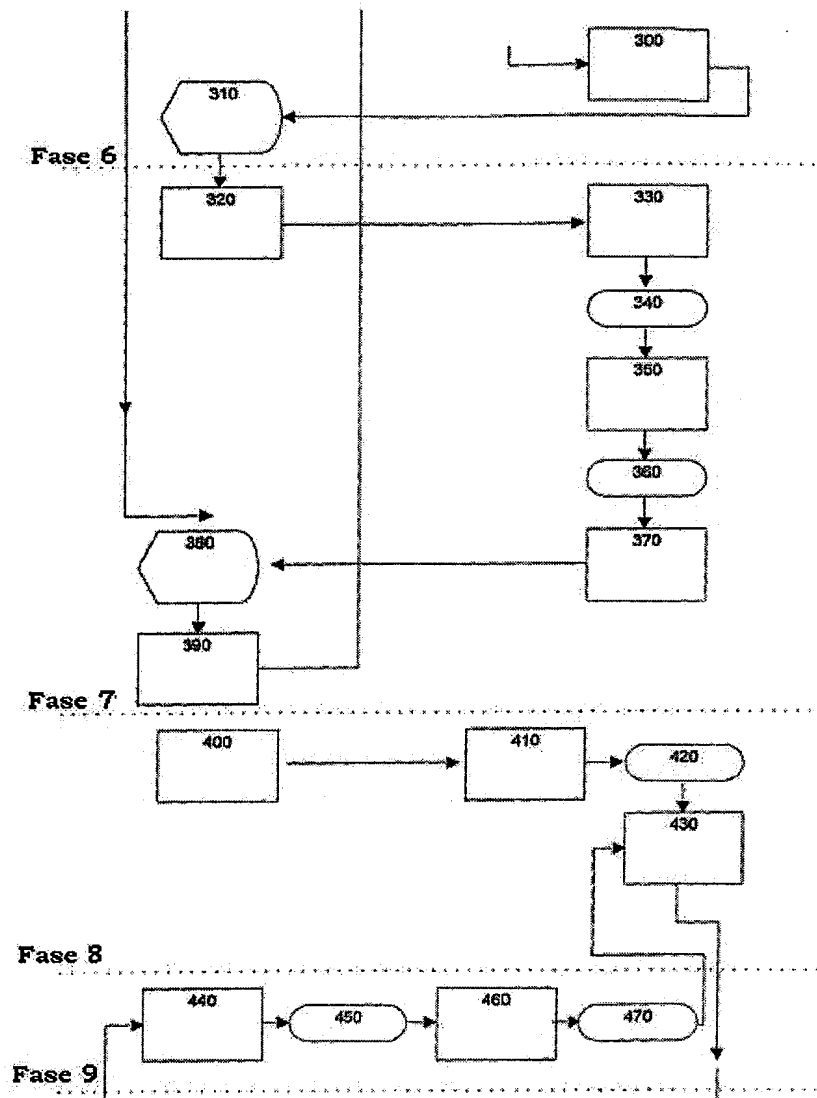


Figura 6A

59

**Figura 6B**

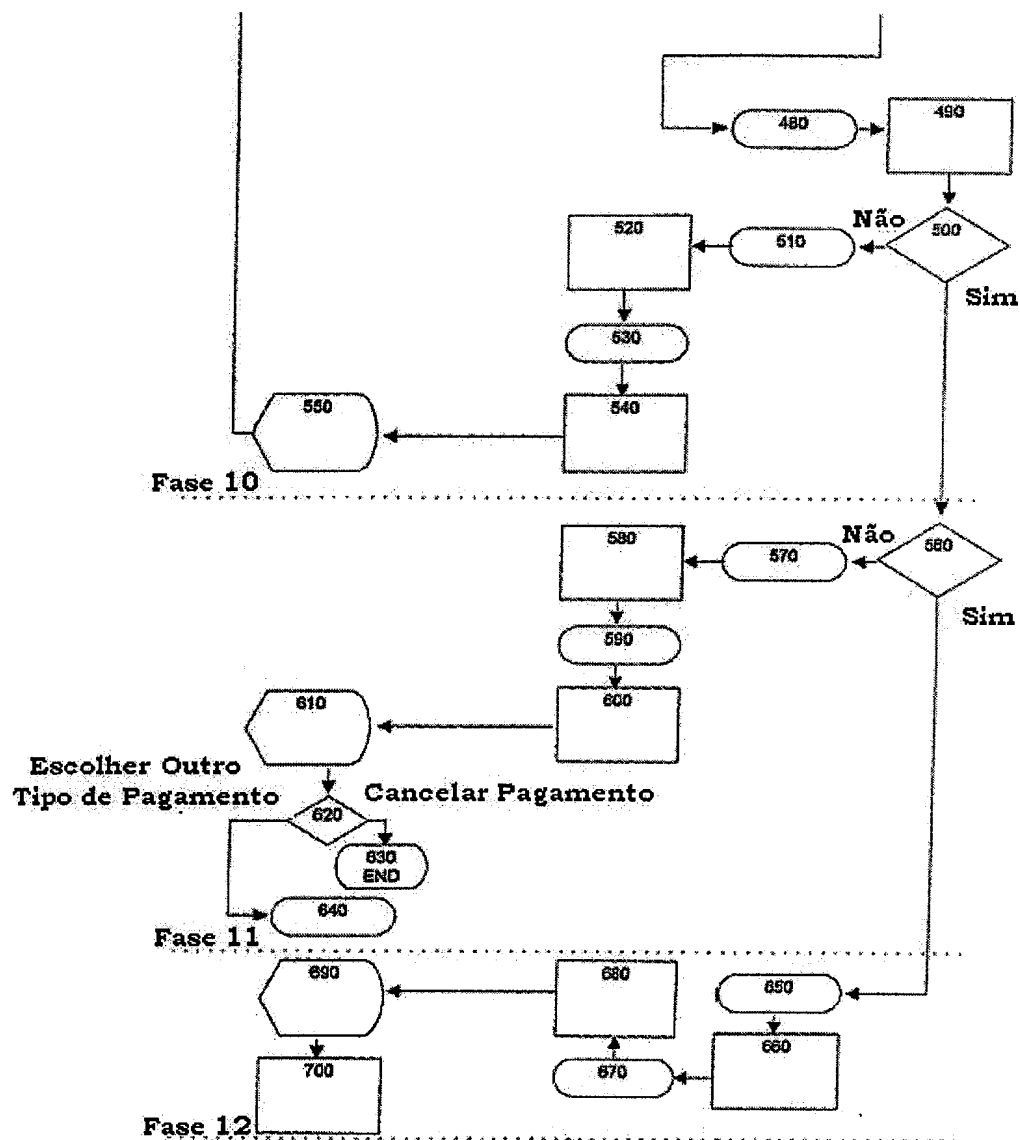


Figura 6c



“Dispositivo Terminal Móvel e Respectivos Métodos de Operação,

Loja de Rede de Comerciante, Centro de Autorização e

Processamento, Sistema de Parceiros Múltiplos, Clientes e

Servidores em Rede Cliente-Servidor e em Sistema de Parceiros

5 **Múltiplos, Produto de Programa de Computador Contendo Código**

de Programa, Meio Legível em Computador, Sinal de Dados

Modulados ou Sinal de Dados de Computador, Sistema de Permuta

de Dados de Transações e Participante”

Resumo

10 Esta invenção mostra um dispositivo terminal móvel (3)
que tem uma unidade de memória (3a) e um dispositivo de interface (3b)
que é conectável de modo liberável a um sistema de parceiros múltiplos
(7,9,15) e capaz de comunicação nele, em que a referida comunicação é
proporcionada por um terminal frontal formado pelo citado dispositivo
15 terminal móvel (3) em combinação com um dispositivo de computador
pessoal (2) e um terminal posterior formado por um parceiro do citado
sistema de parceiros múltiplos via modos de comunicação, sendo dita
comunicação adequada para executar transações de dados com requisi-
tos de segurança variantes, de tal modo que as partes complementares
20 ou partes dentro de uma aplicação distribuída, correndo dentro de um
sistema de parceiros múltiplos, são executadas dependentes de seus
requisitos de segurança atuais, em que a referida comunicação é usada
para permutar informações pelo uso dos citados modos de comunicação
de características diferentes e variantes (4, 6, 12, 17, 13) usando dife-
25 rentes canais de comunicação e padrões ou protocolos de interface
diferentes.