



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

**(21) PI 1100931-4 A2**



\* B R P I 1 1 0 0 9 3 1 A 2 \*

(22) Data de Depósito: 14/03/2011  
(43) Data da Publicação: 07/01/2014  
(RPI 2244)

**(51) Int.Cl.:**  
**G06Q 20/38**

**(54) Título:** MÉTODO E SISTEMA PARA VALIDAR  
UMA TRANSAÇÃO, TERMINAL E PROGRAMA  
TRANSACIONAIS CORRESPONDENTES

**(30) Prioridade Unionista:** 23/03/2010 FR 1052095

**(73) Titular(es):** Compagnie Industrielle Et Financiere D' Ingenierie  
Ingenico

**(72) Inventor(es):** David Naccache, Eric Brier

**(57) Resumo:** MÉTODO E SISTEMA PARA VALIDAR  
TRANSAÇÃO, TERMINAL E PROGRAMA TRANSACIONAIS  
CORRESPONDENTES

A invenção refere-se a um método para validar uma transação em um terminal transacional, a transação sendo associada a um usuário. De acordo com a invenção, tal método compreende uma etapa para decodificar um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados.

## “MÉTODO E SISTEMA PARA VALIDAR TRANSAÇÃO, TERMINAL E PROGRAMA TRANSACIONAIS CORRESPONDENTES”

### 1.Campo da invenção

5 O campo da invenção é o da validação de transações efetuadas por um usuário em um terminal transacional.

Mais especificamente, a invenção refere-se a sistemas de validação que permitem aos usuários executar uma ação predeterminada, como, por exemplo, um pagamento, de maneira rápida e prática.

### 2.Técnica anterior

10 Um sistema conhecido, muito usado para validar transações é o que associa um código secreto e pessoal a um usuário, código esse que ele usa quando, por exemplo, deve acessar um lugar ou validar uma transação através de um terminal de pagamento eletrônico.

Uma desvantagem deste sistema reside no fato de que o código secreto pode ser roubado do usuário, permitindo assim que um indivíduo fraudulento usurpe a identidade do usuário e aja em seu lugar. Outra desvantagem reside no fato de que o usuário deve lembrar seu código para validar uma transação.

Existem também sistemas para autenticar um usuário, que incluem a biometria, comumente utilizada para identificar e/ou autenticar usuários na base de características físicas individuais e que permite que a validação de transações se torne segura.

20 Entretanto, uma desvantagem destes sistemas de autenticação biométricos da técnica anterior reside no fato de que eles são lentos quando usados para referir um grande número de usuários (por exemplo, para controlar o acesso a um sistema ferroviário subterrâneo em uma grande aglomeração urbana ou para autenticar o usuário de um cartão bancário).

25 Na verdade, a duração da etapa de verificação, durante a qual a decisão de autenticação apropriada é tomada, depende do número de usuários referidos no sistema de autenticação. Quanto maior o número de usuários referidos, maior o número de comparações potenciais que devem ser feitas para se determinar ou não determinar a autenticação do usuário.

30 Há, portanto, necessidade de uma técnica para superar estas desvantagens dos sistemas de validação de transações da técnica anterior.

35 A invenção pode ser aplicada especialmente a dispositivos móveis, tais como telefones celulares, sistemas GPS portáteis, assistentes digitais pessoais (PDAs), computadores portáteis e todos os outros aparelhos, a seguir aqui designados como dispositivos móveis, cuja finalidade é comunicar-se através de uma rede de telecomunicações móvel e possuir ou ser a fonte de um segmento de informação em locais precisos e aproximados e estar geralmente dentro do alcance dos seus donos.

A invenção aplica-se também, em pelo menos uma modalidade, a dispositivos de verificação de transações chamados “terminais transacionais” a seguir, como, por exemplo, terminais de pagamento e verificação de identidade, fechaduras eletrônicas, caixas registradoras e terminais de controle de acesso, terminais de transporte público, etc. Estes dispositivos são projetados para comunicar-se através de uma rede de telecomunicações e têm uma localização precisa ou aproximada conhecida dos seus gerentes.

### 3. Objetivos da invenção

A invenção visa especialmente a superar estas desvantagens da técnica anterior.

Mais especificamente, é um objetivo da invenção, em pelo menos uma das suas modalidades, prover uma técnica para validar uma transação associada a um usuário, técnica esta que é rápida e confiável no caso de um sistema usado para referir um grande número de usuários de modo a permitir ao usuário executar uma ação, tal como um pagamento.

É, portanto, um objetivo da invenção prover uma técnica desta espécie, que é também ergonômica para o usuário.

É outro objetivo da invenção prover uma técnica desta espécie, que custa pouco e é fácil de implementar.

### 4. Sumário da invenção

A invenção propõe uma solução inédita sem todas estas desvantagens da técnica anterior sob a forma de um método para validar uma transação em um terminal transacional, a transação sendo associada a um usuário.

De acordo com a invenção, tal método compreende uma etapa para decodificar um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados.

Assim, a invenção recorre a uma abordagem inédita e inventiva para validar uma transação, associada a um usuário, em um terminal transacional que usa o dispositivo móvel do usuário (seu telefone celular, por exemplo) para enviar uma mensagem de validação que compreende um código de validação gerado pelo terminal transacional. Assim, o usuário executa uma ação para validar a transação lendo um código exibido pelo terminal transacional e copiando-o em uma mensagem de validação em seu telefone celular. O usuário em seguida transmite esta mensagem de validação, através do seu telefone celular, para uma entidade de uma rede de telecomunicações à qual o seu telefone celular está conectado e à qual o terminal transacional está também conectado.

Esta rede de comunicações pode incluir em primeiro lugar uma rede móvel à qual o telefone celular do usuário está conectado e, se necessário, o terminal transacional quando é do tipo móvel (equipado com um cartão SIM, por exemplo) e uma rede cabeada à qual o

terminal transacional está conectado se não for do tipo móvel.

De acordo com uma característica específica da invenção, o método compreende etapas para:

- 5                   • receber um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados;
- identificar uma estação base de uma rede de telecomunicações móvel à qual o dispositivo móvel do usuário é conectado;
- 10               • decodificar o código de validação que transmite pelo menos um segmento de informação que representa um identificador do terminal transacional;
- validar a transação quando o terminal transacional identificado estiver na zona de cobertura da estação base identificada à qual o dispositivo móvel do usuário está conectado.

15               Assim, o método da invenção usa a possibilidade de localizar o dispositivo móvel de um usuário, como, por exemplo, um telefone celular, para validar uma transação efetuada por um terminal transacional e associa ao usuário em questão.

                  O princípio geral da invenção é baseado no envio, pelo dispositivo móvel do usuário, de um código de validação usado tanto para localizar o usuário através do seu dispositivo móvel quanto identificar o terminal transacional no qual a transação é efetuada. Assim, a  
20               transação é validada quando puder ser determinado que o usuário está verdadeiramente localizado nas proximidades do terminal transacional em questão.

                  Esta proximidade é determinada em primeiro lugar através da localização do dispositivo móvel e em segundo lugar através de um segmento de informação que representa o  
25               terminal transacional, contido no código de validação, e de um segmento de informação para localizar o terminal transacional conhecido do sistema de validação.

                  De acordo com uma primeira modalidade, com o terminal transacional sendo móvel e conectado a uma estação base da rede de comunicações móveis, o sistema de validação  
30               pode identificar o terminal transacional localizado nas proximidades do dispositivo móvel do usuário.

                  De acordo com uma segunda modalidade, por exemplo quando o terminal móvel é conectado a uma rede de comunicações cabeada, é transmitido para o sistema de validação um segmento de informação que localiza o terminal transacional.

                  Em particular, a mensagem de validação é do tipo SMS ou MMS.

35               Assim, o envio do código de validação pelo usuário é rápido na medida em que ele tem que enviar apenas uma SMS.

                  De preferência, o código de validação é um código curto que pode ser rapidamente

digitado.

De acordo com um aspecto específico da invenção, a etapa de decodificação transmite adicionalmente um segmento de informação que representa a transação.

Assim, o código de validação, quando decodificação, pode identificar também a transação a ser validada, como, por exemplo, pelo fornecimento de um “número de ordem”, isto é, um número referente à ordem na qual as transações são efetuadas pelo terminal transacional.

Classicamente, o terminal transacional transmite informações sobre as transações efetuadas e em progresso, especialmente o valor associado a cada transação, que, ela mesma, é identificada por um número de ordem.

Assim, o valor da transação associada ao número de ordem pode ser facilmente determinado pelo sistema de validação e pode estar associado ao usuário que efetua a transação.

De acordo com uma característica da invenção, o identificado do terminal transacional corresponde ao resultado de uma função  $f(x,y)$  que permite que um identificador único seja associado a um terminal transacional como uma função da sua localização  $(x,y)$ .

Por exemplo, a função pode ser escrita da seguinte maneira:  $f(x,y) = axv + u$ , com:

- $a$  e  $b$  sendo dois números inteiros, de modo que  $b \geq a$  e  $n = a \times b$ , onde  $n$  representa o número de identificadores diferentes a serem distribuídos para o terminal transacional;

- $w = E[x/a] \text{ mod } 2$ ;

- $u = x \text{ mod } a$ ;

- $v = (y + wxE[b/2]) \text{ mod } b$ , com  $E[.]$  sendo a parte de número inteiro; e

- $d = \text{Min} (b, \sqrt{a^2 + \frac{b^2}{4}})$  a distância mínima entre dois terminais transacionais

distintos.

De acordo com uma modalidade da invenção, o método compreende também uma etapa para receber um código confidencial, introduzido preliminarmente pelo usuário no terminal transacional e transmitido pelo terminal transacional concomitantemente com a transmissão do código de validação pelo dispositivo móvel do usuário.

Assim, a validação da transação é também submetido à verificação de um código confidencial associado ao usuário e introduzido no terminal transacional no momento da transação.

Assim, uma verificação dupla pode ser implementada para validar uma transação uma vez que é necessário que o usuário tanto introduza um código confidencial único associado a ele quanto use seu telefone celular para validar a transação.

Assim, se uma pessoa mal intencionada consegue saber o código confidencial do

usuário, mas não tem seu telefone celular, a transação não pode ser validada.

De maneira semelhante, se uma pessoa mal intencionada consegue roubar o telefone celular do usuário, mas não conhece seu código confidencial, a transação não pode ser validada.

5 De acordo com outro aspecto da invenção, a mensagem de validação inclui um código confidencial.

Assim, a validação da transação está também sujeita à introdução de um código confidencial na mensagem de validação que contém o código de validação, reforçando-se assim a segurança da transação.

10 De acordo com uma modalidade alternativa, o método inclui também uma etapa para selecionar a operadora telefônica junto à qual o dispositivo móvel do usuário está registrado.

Assim, a implementação da invenção não está limitada a uma única operadora telefônica. Esta etapa de introdução ocorre no terminal transacional, por exemplo depois que 15 várias escolhas tenham sido propostas pelo terminal transacional.

Por exemplo, o terminal transacional pode ser um terminal de pagamento móvel conectado à rede de telecomunicações.

Em particular, o terminal transacional é conectado à estação base.

20 De acordo com uma característica específica da invenção, o método compreende também uma etapa para a transmissão do código de validação pela entidade da rede de telecomunicações para o terminal transacional, e a etapa para decodificar o código de validação é implementada dentro do terminal transacional.

A invenção refere-se também a um sistema para validar uma transação em um terminal transacional, a transação estando associada a um usuário.

25 De acordo com a invenção, o sistema compreende um dispositivo para decodificar um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados.

30 A invenção refere-se também a um terminal transacional que compreende um dispositivo para gerar um código de validação na base de pelo menos um segmento de informação que representa um identificador do terminal transacional e um dispositivo para exibir o código de validação gerado no dispositivo de exibição do terminal transacional.

35 Outro aspecto da invenção refere-se a um produto de programa de computador passível de transferência de uma rede de comunicações e/ou gravado em uma portadora passível de leitura por computador e/ou executável por um processador, que compreende instruções de código de programa para implementar o método para validar uma transação

conforme descrito acima.

#### 5. Lista de figuras

Outras características e vantagens da invenção aparecerão mais claramente com a descrição seguinte de uma modalidade específica apresentada por meio de um exemplo  
5 simples, ilustrativo e não restritivo e com os desenhos anexos, nos quais:

- A Figura 1 apresenta o contexto para implementar o método para validar uma transação de acordo com a invenção;

- As Figuras 2 e 3 mostram as etapas principais de uma modalidade específica do método de acordo com a invenção.

#### 10 6. Descrição de uma modalidade da invenção

##### *6.1 Princípio geral*

O princípio geral da invenção conta com a utilização do dispositivo móvel do usuário (seu telefone celular, por exemplo) para transmitir uma mensagem de validação gerada e exibida pelo terminal transacional, tornando possível tanto localizar o usuário através do seu  
15 dispositivo móvel quanto identificar o terminal transacional no qual a transação é efetuada. Assim, a transação é validada quando puder ser determinado que o usuário está verdadeiramente localizado nas proximidades do terminal transacional em questão.

Esta proximidade é determinada em primeiro lugar através da localização do dispositivo móvel e em segundo lugar através de um segmento de informação que representa o terminal transacional, contido no código de validação, e através de um segmento de informação, conhecido do sistema de validação, para localizar o terminal transacional.  
20

Uma das características principais das redes de telecomunicações móveis é que um dispositivo móvel, qualquer que possa ser, é permanentemente coberto por uma estação base ou uma estação transceptora base (BTS).

25 Quando um aparelho sai da zona de cobertura de uma estação base, ele é transferido para outra estação base. Esta transferência é feita em ordem, de modo a se aperfeiçoar a qualidade do sinal.

Em outras palavras, a operadora de telecomunicações tem conhecimento em tempo real da posição geográfica aproximada de um dispositivo móvel na rede de telecomunicações móveis: o dispositivo móvel está situado na zona de cobertura da estação base à qual ele está anexado.  
30

O método da invenção faz geralmente uso desta localização. O método da invenção torna possível usar um dispositivo móvel possuído por um usuário em primeiro lugar como um vetor para validar a transação através de uma mensagem de validação que compreende um código de validação e em segundo lugar como um dispositivo para localizar o  
35 usuário.

Além disso, o método da invenção funciona qualquer que seja o tipo de dispositivo

móvel possuído pelo usuário; o usuário não precisa ter um dispositivo móvel de última geração ou um dispositivo muito sofisticado disponível de modo a beneficiar-se das vantagens apresentadas pela invenção.

5 De maneira semelhante, um terminal transacional também se comunica através de uma rede de telecomunicações cabeada ou móvel dependendo do tipo de terminal transacional, permitindo assim a localização geográfica precisa ou aproximada pela operadora da rede de telecomunicações.

10 O método da invenção faz geralmente uso desta localização do terminal transacional para verificar que o usuário, localizado através do seu dispositivo móvel, está nas proximidades do terminal transacional, que é também localizado.

Tais sistemas podem ser usados para fazer pagamentos de maneira simples, sem que seja necessário que o usuário use um cartão bancário ou tenha um dispositivo móvel particular disponível.

15 Tais sistemas podem ser também usados para controlar o acesso a um edifício, uma firma, uma zona geográfica, um show, um evento, uma instalação ou um meio de transporte em uma grande aglomeração e referir assim um número muito grande de usuários.

A seguir, para ilustrar o método de acordo com a invenção, consideraremos um sistema desta espécie usado para validar um pagamento em um centro de compras.

20 Com referência à Figura 1, é apresentado um contexto técnico geral para se implementar o método da invenção. Uma estação base (SB1) é conectada, através de uma rede de telecomunicações (R1), a um servidor de validação (SRV-VALID). A estação base possui uma zona de cobertura dentro da qual terminais transacionais (TT1 a TT7) e um dispositivo móvel (DM1) são identificados e conectados.

25 O servidor de validação (SRV-VALID) é situado, por exemplo, na rede de telecomunicações gerida pela operadora de telefonia do usuário. O servidor de validação nesta modalidade específica da invenção, pode ser um centro de comutação de serviços móveis (MSC) ou um registrador de locais de visitante (VLR) ou um registrador de locais nativos (HLR).

30 Em uma alternativa, o servidor de validação é situado dentro do terminal transacional. Neste caso, a operadora de telefonia se comunica com o terminal transacional de modo a enviar a ele todas as informações necessárias para validar a transação.

No contexto deste exemplo, supõe-se que o usuário U1 portador do dispositivo móvel DM1 deseja fazer uma compra e pagá-la usando o TT4 transacional. Naturalmente, este sistema pode ser implementado em outros casos, como, por exemplo, a validação de um  
35 acesso a uma zona de segurança.

As vantagens apresentadas pela invenção incluem as seguintes:

- não é necessário dar uma nova peça de equipamento ao usuário, que pode usar seu dispositivo móvel. Esta abordagem é, portanto, economicamente muito vantajosa.

- a invenção funciona com qualquer telefone que seja: não é necessário alterar o dispositivo móvel de alguém para o sistema funcionar. O simples fato de se ter um dispositi-  
5 vo móvel disponível é suficiente.

- o sistema é fácil de usar, o que o torna rapidamente pelos usuários.

- o sistema é seguro: para se poder agir de maneira fraudulenta, é necessário por um lado roubar o dispositivo móvel do usuário e, por outro lado, determinar seu código con-  
fidencial. A fraude é, portanto, altamente improvável.

10 - finalmente, as operadoras de telecomunicação estão sempre buscando maneiras de limitar a inconstância dos seus assinantes (em outras palavras, de criar lealdade nos assinantes), e o fato de se associar funções de pagamento com um dispositivo móvel é de uma natureza que reduz a inconstância e cria lealdade nos assinantes.

#### *6.2 Descrição de uma modalidade*

15 Com referência agora à Figura 2, serão apresentadas as etapas principais do método para validar uma transação de acordo com uma modalidade da invenção, na qual o terminal transacional é um terminal de pagamento usado para fazer compras e o dispositivo móvel é um telefone celular.

O método compreende uma primeira etapa 20 para gerar um código de validação por meio do terminal transacional, que exibe o código durante uma etapa de exibição 21.

Por exemplo, a exibição é feita na tela do terminal transacional propriamente dito ou em uma tela conectada ao terminal transacional, tal como a tela de uma caixa registradora em uma loja.

25 Este código de validação, que corresponde, por exemplo, a uma sequência de letras (AIYT, por exemplo), é gerado pelo terminal transacional, em particular a partir do seu próprio identificador.

No exemplo da Figura 1, tal identificador é um dígito, mas pode ser também um número atribuído, por exemplo de acordo com a modalidade específica da invenção descrita acima.

30 O usuário envolvido na transação deve em seguida introduzir este código de validação exibido pelo terminal transacional em seu próprio dispositivo móvel (seu telefone celular, por exemplo) em uma etapa de entrada 22.

De acordo com uma modalidade específica da invenção, o usuário introduz este código sob a forma de uma mensagem de validação do tipo SMS ou MMS, que ele então  
35 transmite para um servidor de validação, por exemplo através de um número curto do tipo "8000".

Este servidor de validação recebe este código em uma etapa de recepção 23 e o

decodifica em uma etapa de decodificação 24 de modo a validar a transação.

Se o servidor de validação for diretamente gerido pela operadora de telefonia do usuário, a mensagem de validação transmitida pelo usuário através do seu dispositivo móvel é diretamente recebida pelo servidor de validação.

5 Se o servidor de validação for gerido independentemente da operadora de telefonia do usuário, a operadora transmite a mensagem de validação para o servidor de validação juntamente com informações que localizam o dispositivo móvel do usuário. O servidor de validação é assim conectado à operadora de telefonia do usuário.

10 Com referência agora à Figura 3, são apresentadas as etapas principais da decodificação do código de validação e da decisão de validar a transação.

Em um primeiro estágio, em uma etapa 240 para identificar uma estação base, o servidor de validação pode associar uma estação base ao usuário, por exemplo *SB1* com referência à Figura 1, com a qual o usuário está conectado. Na verdade, a mensagem de validação recebida do dispositivo móvel do usuário permite que o servidor de validação localize o usuário através da estação base com a qual o dispositivo móvel está conectado.

15 De maneira semelhante, a partir da identificação desta estação base, o servidor de validação pode identificar os terminais transacionais que estão localizados na zona de cobertura desta estação base e estão, portanto, próximos do usuário. Na verdade, o servidor de validação, quer seja gerido diretamente pela operadora de telefonia do usuário, quer seja independente, mas conectado à operadora de telefonia do usuário, é capaz de conhecer cada estação base da rede de telecomunicações móvel e, portanto, quando os terminais transacionais são móveis, o servidor de validação pode conhecer os que estão conectados a cada estação base da rede de telecomunicações móvel.

25 Assim, a posição geográfica do terminal transacional pode ser automaticamente inferida do fato de que uma dada estação base assume o controle dele (isto supõe que o terminal transacional tem um cartão SIM, o que é muito comum). Isto é importante porque uma implementação desta espécie destrói qualquer noção de coordenadas geográficas. O fato de que os telefones celulares estão no campo de uma estação base que cobre também um terminal transacional significa que os telefones celulares estão nas proximidades do terminal transacional em questão. Isto é suficiente para que o servidor de validação identifique o terminal ou terminais transacionais localizados nas proximidades do usuário, conforme descrito acima.

35 De maneira semelhante, o servidor de validação é capaz de conhecer os terminais transacionais conectados a uma rede cabeada e, portanto, entre estes terminais, o servidor de validação é capaz de conhecer os que estão na zona de cobertura da estação base identificada (ver a seguir). Para isto, pode-se planejar que o servidor de validação gere uma lista de terminais transacionais conectados à rede cabeada e localizados nas zonas de co-

bertura das estações base.

Assim, os terminais transacionais potencialmente usados na transação a ser validada são identificados pelo servidor de validação a partir da localização do dispositivo móvel do usuário.

5 Em um segundo estágio, o servidor de validação pode identificar com precisão o terminal transacional, usando o código de validação recebido.

Na verdade, de acordo com uma variante específica desta modalidade da invenção, o código de validação recebido pelo servidor de validação corresponde a uma concatenação de dois elementos, que representam respectivamente um identificador do terminal transacional e a transação.

10 Por exemplo, este código de quatro letras (AIYT) pode ser dividido da seguinte maneira:

- um número  $N$  corresponde a um identificador do terminal transacional que implementa a transação a ser validada;

15 • um número  $Q$  representa a transação aberta a ser validada, por exemplo um número de transação que representa uma das transações que aguardam conclusão efetuadas pelo terminal transacional que implementa a transação a ser validada.  $Q$  é tipicamente um número inteiro pequeno, por exemplo um número inteiro cujo valor varia de 0 a 9 uma vez que há raramente mais de nove clientes diante de um terminal transacional em um dado ponto no tempo. Uma vez que tenha sido validada uma transação que tem um dado número  $Q$ , este valor de  $Q$  é reciclado pelo terminal transacional para outras transações.

20 De acordo com um aspecto específico da invenção, os terminais transacionais são identificados por um identificador único  $N$  que corresponde, por exemplo, ao resultado de uma função  $f$  usada para associar um identificador único a um terminal transacional como uma função da sua localização  $(x,y)$  (ver a seguir para um método para atribuir um identificador a um terminal transacional).

Assim, conforme mostrado na Figura 1, vários terminais transacionais podem ter o mesmo identificador se a rede de telecomunicações for considerada como um todo, mas um identificador único se for considerada a zona de cobertura de uma estação base.

30 Com este número  $N$  extraído do código de validação recebido, e a identificação preliminar da estação base, o servidor de validação pode, portanto, identificar de maneira única o terminal transacional envolvido na transação a ser validada, durante uma etapa 241 para identificar o terminal transacional.

35 Em seguida, a etapa 25 para validar a transação consiste em verificar que o número  $Q$  da transação corresponde verdadeiramente a uma transação aberta (em progresso) pelo terminal transacional que foi identificado preliminarmente, e em seguida associar a soma da transação com o usuário e validar a transação convencionalmente (por exemplo de-

pois da verificação do saldo na conta do usuário).

Na verdade, de acordo com a invenção, o servidor de validação é capaz de conhecer todas as transações feitas pelos terminais transacionais localizados na rede de telecomunicações e pode verificar que a transação número  $Q$  é efetivamente uma transação que foi aberta (em progresso) pelo terminal transacional identificado preliminarmente.

Por exemplo, os terminais transacionais enviam ao servidor de validação (quando ele é diretamente gerido pela operadora de telefonia do usuário) informações sobre as transações feitas em cada um deles.

Em outro caso, os terminais transacionais transmitem informações sobre as transações feitas em cada um deles para sua operadora de telefonia (ou, mais especificamente, para a operadora de telefonia do comerciante que os utiliza). Se esta operadora de telefonia for diferente da operadora de telefonia do usuário, as operadoras se comunicam uma com a outra para permitir a validação da transação.

De acordo com uma modalidade da invenção, planeja-se que o terminal transacional transmita esta informação para uma operadora escolhida pelo usuário. Assim, a informação pode ser diretamente transmitida para a operadora do usuário. Para isto, o método de acordo com uma modalidade da invenção compreende uma etapa para identificar uma operadora de comunicações. Por exemplo, o terminal transacional oferece ao usuário uma escolha entre diversas operadoras (por exemplo, Operadora No. 1: número = 1, Operadora No. 2: número = 2,...). Em seguida, o usuário introduz o número que corresponde à sua operadora no terminal transacional, de modo que o terminal transacional e o comerciante conheça o servidor de validação para o qual as informações sobre as transações devem ser transmitidas.

Se esta verificação de que o número  $Q$  da transação corresponde verdadeiramente a uma transação aberta (em progresso) pela terminal transacional identificado preliminarmente for positiva, então o servidor de validação tem as seguintes informações disponíveis para validar a transação;

- a transação a ser validada No.  $Q$  está sendo implementada em um terminal transacional  $TTx$  (verificação possível por meio do código de validação decodificado);
- o dispositivo móvel  $DMy$  do usuário é identificado e localizado;
- a estação base  $STBz$  à qual  $DMy$  está conectado é identificada e localizada;
- o terminal transacional  $TTx$  é localizado na zona de cobertura da estação base  $STBz$  a partir do código de validação decodificado. O servidor de validação pode, portanto, validar a transação pela execução subsequente, por exemplo, das seguintes operações:
- debitar o valor da transação No.  $Q$  da conta do usuário;
- creditar o valor associado ao terminal transacional  $TTx$ ;

- enviar uma validação de transação ao terminal transacional *TTx*.

Como complemento, quando da recepção desta validação do servidor de validação, o terminal transacional pode enviar um bilhete que representa a transação ao usuário e fechar assim a transação.

5 Além do método de validação descrito acima, a invenção refere-se também a um sistema de validação que compreende um dispositivo para implementar o método descrito acima.

### *6.3 Outras características e características complementares*

#### *6.3.1. Introdução do código confidencial*

10 De acordo com uma característica específica da invenção, uma etapa adicional para introduzir um código confidencial no terminal transacional é executada pelo usuário. Esta operação de introdução é uma medida de segurança adicional usada para assegurar que o usuário tenha verdadeiramente esta informação disponível para ele.

15 O código confidencial introduzido pelo usuário no terminal transacional é em seguida transmitido pelo terminal transacional para o servidor de validação ou para a operadora de telefonia do usuário, que é ela mesma conectada ao servidor de validação. Neste caso, o terminal transacional deve conhecer a operadora de telefonia em questão.

20 Para isto, o método de acordo com uma modalidade da invenção compreende uma etapa para identificar uma operadora de comunicações, conforme descrito acima. Por exemplo, o terminal transacional dá ao usuário uma escolha entre diferentes operadoras (por exemplo, Operadora No. 1: número = 1, Operadora No. 2: número = 2,...). O usuário introduz então o número correspondente à sua operadora no terminal transacional, de modo que o terminal transacional e o comerciante conheçam o servidor de validação para o qual o código confidencial introduzido pelo usuário deve ser transmitido.

25 Contempla-se, por exemplo, fazer com que esta introdução de um código confidencial seja obrigatória se a transação ultrapassar uma determinada soma que pode ser transformada em parâmetro de acordo com o usuário, por exemplo durante uma fase preliminar de registro junto ao servidor de validação.

30 Uma medida de segurança adicional pode ser obtida travando-se o dispositivo móvel do usuário de maneira convencional após determinado período de inatividade.

35 Outra medida de segurança pode consistir em tornar a introdução de um código confidencial obrigatória de modo a permitir o envio da mensagem de validação (que contém o código de validação) ao servidor de validação ou mais uma vez incluir um código confidencial no corpo da mensagem de validação. Assim, se o dispositivo móvel do usuário for roubado por alguém mal intencionado, este último não poderá usar o dispositivo móvel para validar uma transação se não conhecer o código confidencial a ser inserido na mensagem de validação.

### 6.3.2 Atribuição de um identificador a um terminal transacional

De acordo com uma característica específica da invenção, o identificador único atribuído a cada terminal transacional localizado na zona de cobertura de uma estação base é determinado levando-se em conta a localização do terminal transacional, isto é, sua posição  
5  $(x,y)$ .

Considera-se, portanto, uma função  $f(x,y)$  que transmite um número único para um terminal transacional como uma função da sua localização, de modo que:  $f = a \times v + u$ .

Por construção, a função  $f(x,y)$  transmite um número inteiro que varia na faixa de 0 a  $n-1$ ,  $n$  representando o número de identificadores diferentes que podem ser atribuídos aos  
10 terminais transacionais a serem considerados.

Considera-se também:

- dois números inteiros  $a$  e  $b$ , de modo que  $b \geq a$  e  $n = a \times b$ ;
- $w = E[x/a] \text{ mod } 2$ ;
- $u = x \text{ mod } a$ ;
- 15 •  $v = (y + wxE[b/2]) \text{ mod } b$ , com  $E[.]$  sendo a parte de número inteiro.

A função  $f(x,y)$  sendo periódica, a distância mínima  $d$  entre dois pontos que têm o mesmo valor de  $f$ , isto é, dois terminais transacionais localizados em dois lugares diferentes, pode ser obtida por um deslocamento de “ $b$  passos” ou pegadas verticalmente (ao longo de  $y$ ) ou por um deslocamento de “ $a$  passos” horizontalmente (ao longo de  $x$ ) e “ $b/2$  passos”  
20 verticalmente (ao longo de  $y$ ).

Por exemplo, pode-se escrever:  $d = \text{Min} (b, \sqrt{a^2 + \frac{b^2}{4}})$ , que pode ser otimizada por uma relação  $a/b$  próxima de  $\frac{\sqrt{3}}{2}$ .

Por exemplo, se se procurasse atribuir números de quatro dígitos (para facilidade dos usuários finais) aos terminais transacionais, então seria apropriado escolher  $a=93$  e  
25  $b=107$ , obtendo-se  $n=9951$  e uma distância de 107 passos entre dois terminais transacionais com o mesmo identificador.

A partir deste método, que atribui valores a todos os pontos do plano infinito, é fácil adaptar um mapeamento finito. Na verdade, uma vez que a construção é periódica, qualquer ponto de partida é apropriado e pode ser usado para manter a distância de 107 passos entre  
30 dois terminais transacionais com o mesmo identificador.

### 6.3.3 Características complementares

Em uma modalidade específica da invenção, quando o usuário é um assinante de um grupo estrangeiro (OE) que tem um convênio de itinerância com uma operadora nacional (ON), a implementação da invenção é quase idêntica. Na verdade, a presença de um assi-

nante estrangeiro na zona de cobertura da estação base de uma operadora nacional é um segmento de informação conhecido da operadora nacional. Assim, a localização do dispositivo móvel do usuário assim como a identificação do terminal transacional podem ser feitas conforme aqui descrito. Apenas as etapas para a validação apropriada da transação, no que se refere, por exemplo, a cheques no saldo na conta do usuário, podem exigir, por exemplo, câmbios com um servidor estrangeiro na cobrança pelo gerenciamento da conta do usuário.

## REIVINDICAÇÕES

1. Método para validar uma transação em um terminal transacional, a transação estando associada a um usuário,

5       **CARACTERIZADO** pelo fato de que compreende uma etapa para decodificar um código de validação gerado preliminarmente e exibido pelo terminal transacional de acordo com a reivindicação 14, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados.

10       2. Método para validar, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende as etapas para:

- 15           • receber um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados;
- identificar uma estação base de uma rede de telecomunicações móvel à qual o dispositivo móvel do usuário é conectado;
- decodificar o código de validação que transmite pelo menos um segmento de informação que representa um identificador do terminal transacional;
- 20           • validar a transação quando o terminal transacional identificado estiver na zona de cobertura da estação base identificada à qual o dispositivo móvel do usuário está conectado.

3. Método para validar, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a mensagem de validação é do tipo SMS ou MMS.

25       4. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 3, **CARACTERIZADO** pelo fato de que a etapa de decodificação também transmite um segmento de informação que representa a transação.

30       5. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 4, **CARACTERIZADO** pelo fato de que o identificador do terminal transacional corresponde ao resultado de uma função  $f(x,y)$  que permite que um identificador único seja associado a um terminal transacional como uma função da sua localização  $(x,y)$ .

6. Método para validar, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a função pode ser escrita da seguinte maneira:  $f(x,y) = ax + by + u$ , com:

- 35           •  $a$  e  $b$  sendo dois números inteiros, de modo que  $b \geq a$  e  $n = a \times b$ , onde  $n$  representa o número de identificadores diferentes a serem distribuídos para o terminal transacional;
- $w = E[x/a] \bmod 2$ ;

- $u = x \text{ mod } a$ ;
- $v = (y + wxE[b/2]) \text{ mod } b$ , com  $E[.]$  sendo a parte de número inteiro; e
- $d = \text{Min} (b, \sqrt{a^2 + \frac{b^2}{4}})$  a distância mínima entre dois terminais transacionais distintos.

5           7. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 6, **CARACTERIZADO** pelo fato de que compreende também uma etapa para receber um código confidencial, introduzido preliminarmente pelo usuário no terminal transacional e transmitido pelo terminal transacional concomitantemente com a transmissão do código de validação pelo dispositivo móvel do usuário.

10           8. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 7, **CARACTERIZADO** pelo fato de que a mensagem de validação inclui um código confidencial.

15           9. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 8, **CARACTERIZADO** pelo fato de que inclui também uma etapa para selecionar a operadora telefônica junto à qual o dispositivo móvel do usuário está registrado.

            10. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 9, **CARACTERIZADO** pelo fato de que o terminal transacional é um terminal de pagamento móvel conectado à rede de telecomunicações.

20           11. Método para validar, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que o terminal transacional é conectado à estação base.

25           12. Método para validar, de acordo com qualquer uma das reivindicações de 1 a 11, **CARACTERIZADO** pelo fato de que compreende também uma etapa para a transmissão do código de validação pela entidade da rede de telecomunicações para o terminal transacional, e pelo fato de que a etapa para decodificar o código de validação é implementada dentro do terminal transacional.

            13. Sistema para validar uma transação em um terminal transacional, a transação estando associada a um usuário,

30           **CARACTERIZADO** pelo fato de que compreende um dispositivo para decodificar um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal transacional são conectados.

35           14. Terminal transacional **CARACTERIZADO** por compreender um dispositivo para gerar um código de validação na base de pelo menos um segmento de informação que representa um identificador do terminal transacional e um dispositivo para exibir o código de validação gerado no dispositivo de exibição do terminal transacional.

15. Produto de programa de computador passível de transferência de uma rede de comunicações e/ou gravado em uma portadora passível de leitura por computador e/ou executável por um processador, **CARACTERIZADO** pelo fato de que compreende instruções de código de programa para implementar o método para validar uma transação de acordo com pelo menos uma das reivindicações de 1 a 12.

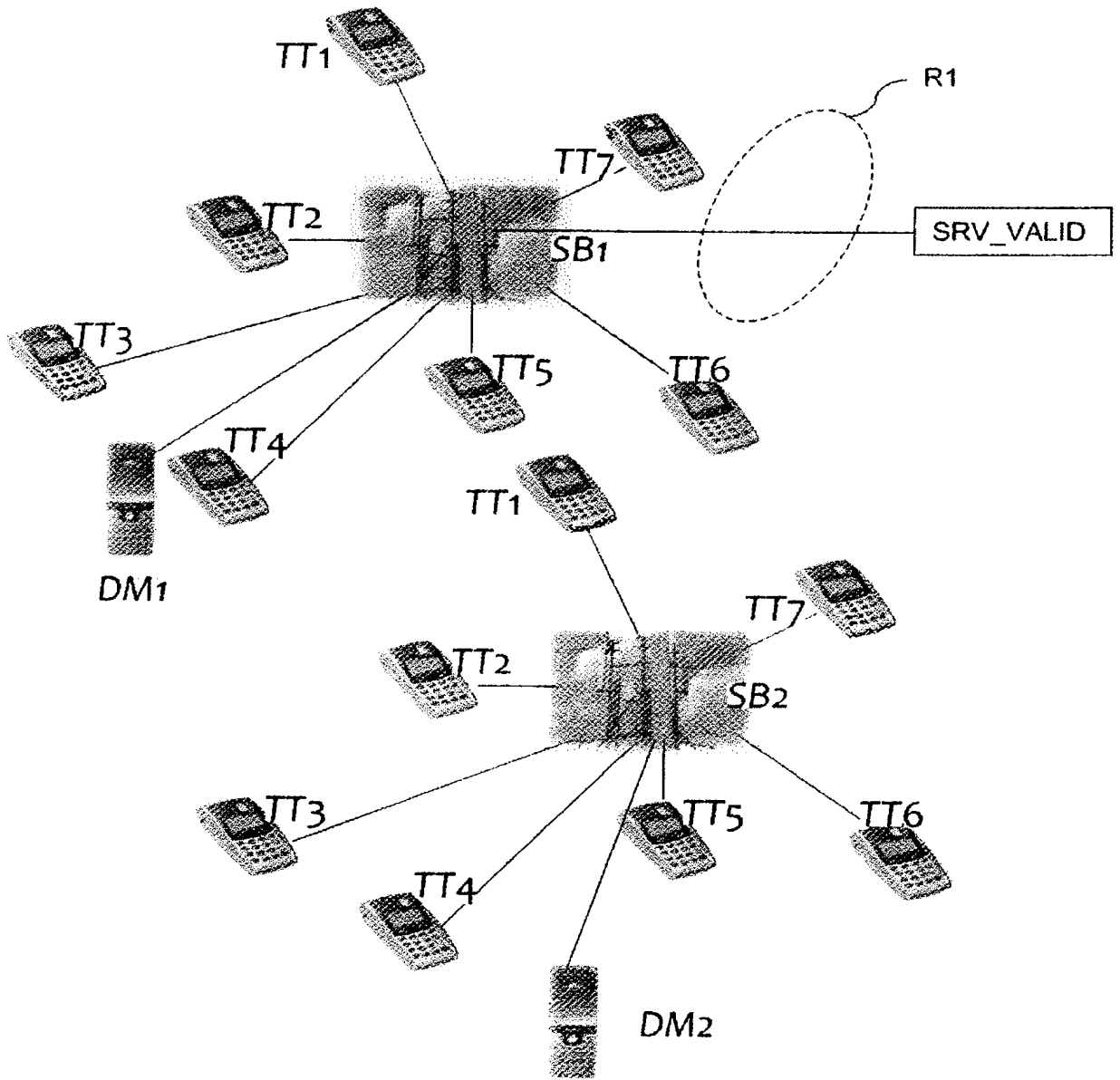


Figura 1

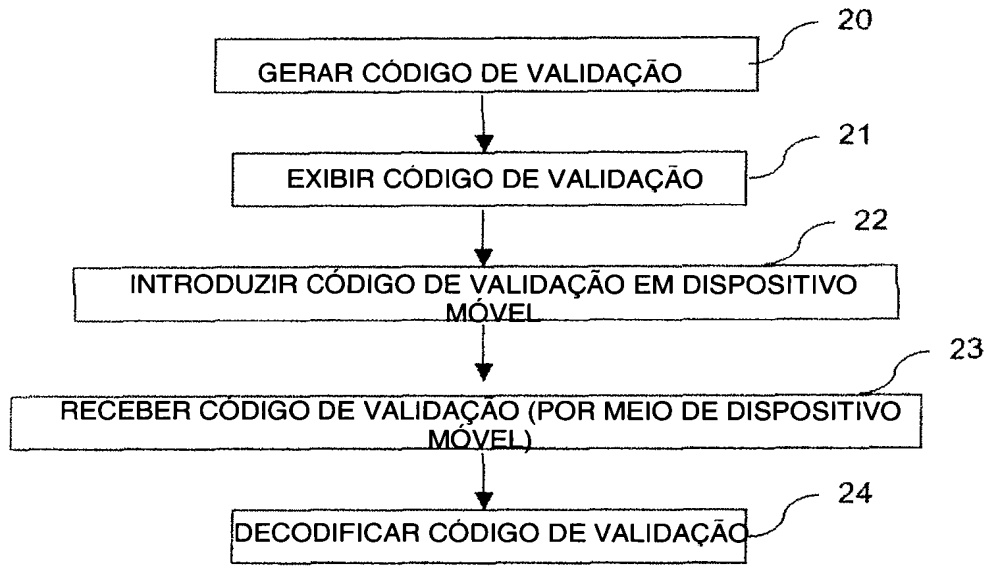


Figura 2

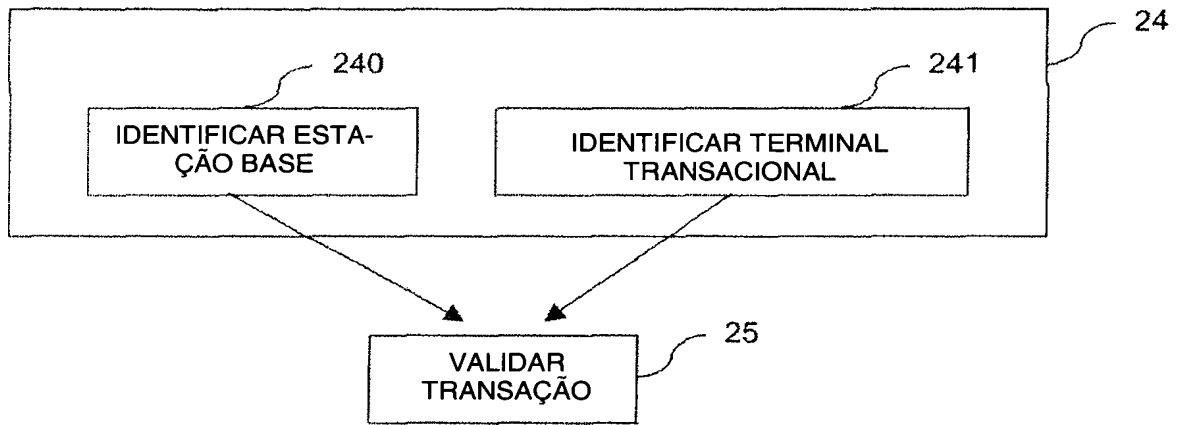


Figura 3

## RESUMO

### “MÉTODO E SISTEMA PARA VALIDAR TRANSAÇÃO, TERMINAL E PROGRAMA TRANSACIONAIS CORRESPONDENTES”

5 A invenção refere-se a um método para validar uma transação em um terminal transacional, a transação sendo associada a um usuário.

De acordo com a invenção, tal método compreende uma etapa para decodificar um código de validação gerado preliminarmente e exibido pelo terminal transacional, introduzido pelo usuário em uma mensagem de validação transmitida pelo dispositivo móvel do usuário para uma entidade de uma rede de telecomunicações à qual o dispositivo móvel e o terminal  
10 transacional são conectados.