

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

(21) **PI 1003217-7 A2**

(22) Data de Depósito: 08/04/2010
(43) Data da Publicação: 23/10/2012
(RPI 2181)



(51) *Int.Cl.:*
G06Q 20/38
H04L 9/32
H04L 29/06

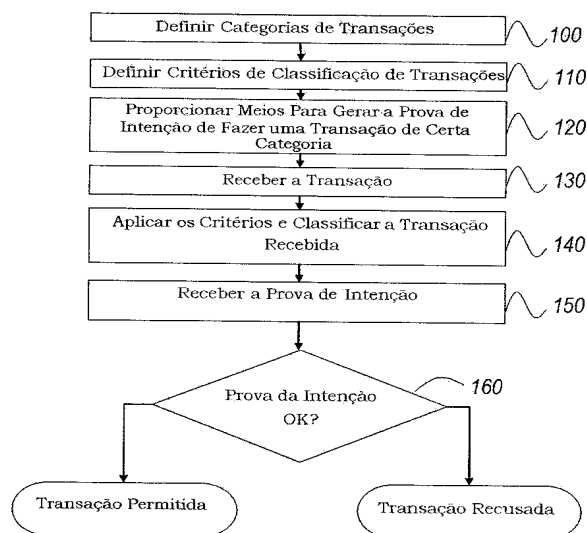
(54) Título: MÉTODOS E EQUIPAMENTO DE ASSEGURAMENTO DE TRANSAÇÕES ELETRÔNICAS E DE GERAÇÃO DE CÓDIGOS DINÂMICOS DE APROVAÇÃO DE CATEGORIA DE TRANSAÇÃO

(30) Prioridade Unionista: 23/10/2009 US 12604838

(73) Titular(es): Vasco Data Security Inc.

(72) Inventor(es): Dirk Marien , Frank Hoornaert

(57) Resumo: Métodos e Equipamento de Asseguramento de Transações Eletrônicas e de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação. A presente invenção relaciona-se com o campo de assegurar transações eletrônicas e, mais especificamente, com métodos para indicar e verificar a aprovação do nível de risco de uma transação e com equipamentos para gerar códigos de aprovação do nível de risco de transações. Num método de acordo com a invenção, as transações são classificadas num número limitado de categorias. Um usuário que submete uma transação a um servidor é solicitado também a gerar e submeter um código dinâmico de aprovação de categoria de transação para a transação submetida. Do lado do servidor é gerado um valor de verificação correspondente para a transação recebida. Num método alternativo de acordo com a invenção, às transações são atribuídos um dentre um número limitado de níveis de risco. Um usuário que submete uma transação a um servidor é solicitado também a gerar e submeter um código dinâmico de aprovação de nível de risco para a transação submetida. No lado do servidor, um valor de verificação correspondente é gerado para a transação recebida. O código dinâmico de aprovação de nível de risco recebido é verificado no lado do servidor comparando-o com o valor de verificação gerado. Também são descritos um token de segurança para assegurar transações eletrônicas adaptadas para gerar códigos dinâmicos de aprovação de categoria de transação e um token de segurança para assegurar transações eletrônicas adaptado para gerar códigos dinâmicos de aprovação de nível de risco.



“Métodos e Equipamento de Asseguramento de Transações

Eletrônicas e de Geração de Códigos Dinâmicos

de Aprovação de Categoria de Transação”

Relatório Descritivo

5 Dispositivo de segurança compacto com capacidade de aprovação de nível de risco de transação.

Campo Técnico

10 A presente invenção relaciona-se com o campo de assegurar transações eletrônicas e, mais especificamente, com métodos para indicar e verificar a aprovação do nível de risco de uma transação e com equipamentos para gerar códigos de aprovação do nível de risco de transações.

Técnica Antecedente

15 *Tokens* fortes de autenticação são um tipo de *tokens* de segurança que é bem conhecido na técnica. Eles permitem a provedores de serviço e aplicativos autenticarem o possuidor do *token*, proporcionando senhas dinâmicas que poderiam apenas ser geradas com conhecimento de um segredo ou chave que é compartilhada entre o servidor de autenticação empregado pelo provedor de serviço ou aplicativo, por um lado, e o *token* de autenticação, por outro lado. Para gerar senhas dinâmicas, o *token* de autenticação forte aplica um algoritmo criptográfico ao segredo compartilhado e uma variável dinâmica, por exemplo, compreendendo um ou mais de um valor de contador, um valor que representa o tempo presente e um desafio aleatório. Normalmente a senha dinâmica pode ser usada apenas uma vez, aumentando
25 muito, deste modo, o nível de segurança com respeito a senhas estáti-

cas. Os *tokens* fortes de autenticação são populares, especialmente para assegurar aplicativos tais como Internet *banking*, porque oferecem um nível muito mais alto de segurança do que as senhas estáticas combinadas com uma elevada conveniência do usuário.

5 Outro tipo de *tokens* de segurança são *tokens* de assinatura de transação. Esses *tokens* de assinatura de transação permitem que provedores de serviços e aplicativos verifiquem a aprovação da transação pelo possuidor do *token* e a integridade dos dados de transação, proporcionando assinaturas eletrônicas na transação que apenas
10 poderiam ser geradas com o conhecimento de um segredo ou chave que fosse compartilhada entre o servidor de autenticação empregado pelo provedor de serviços e aplicativos, por um lado, e o *token* de autenticação, por outro lado. Para gerar assinaturas eletrônicas, o *token* de assinatura de transação aplica um algoritmo criptográfico ao segredo
15 compartilhado e aos dados da transação. Em alguns casos, o *token* de assinatura de transação pode incluir também o valor de uma variável dinâmica no cálculo da assinatura eletrônica como medida contra ataques de repetição.

Para verificar a validade da senha dinâmica ou assinatura eletrônica gerada pelo *token* de segurança, o servidor de autenticação
20 realiza o mesmo cálculo ou um cálculo complementar ao *token* de segurança para obter um valor de verificação usando a sua própria cópia do segredo compartilhado e seu valor localmente mantido do contador, o tempo presente, o desafio que submeteu ao usuário final ou
25 os dados relevantes relacionados com a transação. O servidor compara, então, o valor de verificação que gerou com a senha dinâmica ou a assinatura eletrônica recebida a partir do usuário. A autenticação ou a aprovação da transação é bem sucedida, se a senha dinâmica gerada pelo *token* ou a assinatura eletrônicas submetida pelo usuário final
30 combina com o valor de verificação gerado pelo servidor de autentica-

ção.

Os *tokens* de assinatura de autenticação e transação fortes típicos têm uma tela para comunicar as credenciais geradas tais como senhas de uma vez ou assinaturas eletrônicas ao usuário final e um botão ou teclado para pedir a geração de uma nova credencial e/ou introduzir desafios, dados de transação, Códigos PIN etc. Outro meio de comunicação conhecido inclui saída audível, interfaces de USB e interfaces sem fio. Outros meios de entrada conhecidos incluem sensores ópticos, interfaces de USB e interfaces sem fio.

Alguns *tokens* de segurança exigem que o usuário introduza um código PIN para realizar certas ações tais como gerar uma assinatura eletrônica. Em alguns casos, o usuário submete também ao servidor de autenticação uma senha estática, além da senha dinâmica gerada por um *token* de autenticação forte tal como uma contra-medida contra o uso fraudulento de *tokens* perdidos ou roubados.

Alguns *tokens* de segurança são capazes de gerar tanto senhas dinâmicas como assinaturas eletrônicas.

Alguns *tokens* de segurança são dispositivos de hardware dedicados cuja função única ou principal é gerar senhas dinâmicas e assinaturas eletrônicas, enquanto outros *tokens* são dispositivos que têm capacidades de computação de propósito geral (por exemplo, Computadores Pessoais, Assistentes Digitais Pessoais, telefones celulares) que processam software que emula as funções de autenticação forte de hardware dedicado e *tokens* de assinatura de transações e que frequentemente oferecem a geração de senhas dinâmicas e assinaturas eletrônicas meramente como uma funcionalidade adicional além de outras funcionalidades. O último tipo de *token* é, às vezes, chamado de *token* de software.

Numa primeira classe de *tokens* fortes de assinatura de autenticação e transação, o segredo é embutido numa memória interna ao *token* propriamente, que é tipicamente tornada inacessível ao mundo externo. Numa segunda classe de *tokens* fortes de assinaturas de autenticação e transação, o *token* é capaz de receber um componente externo que transporta um segredo, tal como um cartão inteligente, e de cooperar com este componente externo para gerar e proporcionar senhas dinâmicas e assinaturas eletrônicas.

A faixa de produtos vendidos por Vasco Data Security sob a marca DIGIPASS contém vários exemplos de *tokens* de segurança conforme descritos acima.

Revelação da Invenção

Problema Técnico

Embora ofereça um aperfeiçoamento enorme na segurança, quando comparado com as senhas estáticas, o uso de senhas dinâmicas geradas por *tokens* de autenticação forte não resolve todos assuntos de segurança associados a transações eletrônicas remotas. Por exemplo, por meio de um ataque de homem real no meio em tempo real (MITM), atacantes podem conseguir pegar senhas dinâmicas válidas e usa-las para seus próprios propósitos abomináveis, por exemplo, realizar transações fraudulentas. Nesse MITM, um atacante pode substituir dados de transação fraudulentos pelos os dados de transação real, por exemplo, no caso de uma transferência de dinheiro, o atacante pode substituir o número para a conta recebedora pretendida pelo número de uma conta sob controle do atacante e pode levantar uma quantidade baixa de dinheiro a ser transferida por uma quantidade mais alta de dinheiro a ser transferida.

Os *tokens* de assinatura de transação oferecem uma

solução para este problema, visto que as assinaturas eletrônicas que geram estão matematicamente ligadas aos dados de transação com que estão associadas. Se um atacante alterar ou substituir os dados de transação autêntica por dados fraudulentos, a verificação da assinatura eletrônica pelo servidor de verificação falhará. Um caminho típico para proporcionar dados de transação para um *token* de autenticação forte é deixar o usuário introduzir os dados de transação manualmente no teclado do *token*. Introduzir os dados de transação no seu teclado de *token* assim como também no seu PC de cliente pode ser visto por alguns usuários como muito incômodo. Também um *token* capaz de gerar assinaturas eletrônicas em geral exige um meio para introduzir os dados de transação. Tipicamente, um meio de entrada de *tokens* de assinatura de transação compreende um teclado, que torna um *token* de assinatura de transação típico maior do que um *token* de autenticação forte típico que apenas gera senhas dinâmicas e que, portanto, apenas precisa de uma interface mínima com o usuário (um botão único e, às vezes, até nenhum botão mesmo, é suficiente em geral).

O que é necessário é um método para certificar transações eletrônicas que ofereça um nível de segurança superior ao que é oferecido apenas por senhas dinâmicas, ao mesmo tempo em que oferece a mesma conveniência de usuário de senhas dinâmicas e que possam ser de preferência implementadas usando dispositivos de segurança que tenham um fator de forma que seja tão compacto quanto aquele de um *token* de autenticação forte ordinário capaz de gerar senhas dinâmicas.

Solução Técnica

A presente invenção é baseada na visão de que um nível significativamente mais alto de segurança do que aquele oferecido por senhas dinâmicas tradicionais pode ser atingido, se, por um lado, as transações puderem ser classificadas num número relativamente

pequeno de grupos distintos, tendo cada grupo certo nível de risco associado a ele e se, por outro lado, existir um modo para que o servidor verifique sem ambiguidade que o usuário realmente pretendeu fazer uma transação com aquele nível de risco particular.

5 Uma maneira para que os usuários indiquem o seu intento ao servidor de executar uma transação correspondendo a certo nível de risco é submeter ao servidor, junto com os dados de transação, um código de aprovação de nível de risco de transação que corresponde ao nível de risco do grupo a que transação pertence, de forma que o
10 código de aprovação de nível de risco de transação possa ser verificado pelo servidor.

A presente invenção é ainda baseada na visão de que os códigos de aprovação de nível de risco de transação podem ser vantajosamente gerados por um dispositivo confiado sob controle do usuário e
15 que, se o número de níveis de risco for relativamente pequeno, então, esse dispositivo exige apenas uma interface simples com o usuário para permitir a um usuário indicar com apenas algumas interações que nível de risco uma aprovação de nível de risco precisa ser gerado.

Para melhorar o nível de segurança, os códigos de aprovação de nível de risco de transação são de preferência impossíveis de
20 prever. Preferivelmente, deve ser duro para qualquer atacante obter ou gerar códigos válidos de aprovação de nível de risco de transação para uma dada transação. Uma maneira de gerar códigos de aprovação de nível de risco de transação impossível de prever envolve o uso de
25 um algoritmo criptográfico parametrizado com um ou mais valores secretos. De preferência pelo menos um destes segredos é direta ou indiretamente associado ao usuário. Numa modalidade, um segredo usado na geração de códigos de aprovação de nível de risco é compartilhado com um servidor de verificação. O algoritmo criptográfico pode
30 compreender um algoritmo simétrico tal como um algoritmo simétrico

de criptografia ou de decodificação (por exemplo, DES ou AES) ou pode compreender uma função de uma só via tal como uma função de *hash* (por exemplo, MD5 ou membros da família de SHA de funções de *hash*).

O algoritmo criptográfico pode também compreender a geração de um código de autenticação de mensagem ou um código de autenticação de mensagem chaveado por *hash*. Além do nível de risco para o qual um código de aprovação é gerado, o algoritmo de geração de código de aprovação de nível de risco pode também levar em conta o valor de uma variável dinâmica tal como o valor de um contador ou um valor relacionado com o tempo, a fim de prevenir ataques de retomada. Numa modalidade, o geração de código de aprovação de nível de risco compreende aplicar um algoritmo criptográfico a um segredo, uma variável dinâmica e um valor que representa o nível de risco. Noutra modalidade, a geração de código de aprovação de nível de risco compreende selecionar um segredo a partir de um conjunto de segredos com base no nível de risco e aplicar um algoritmo criptográfico ao segredo selecionado e uma variável dinâmica. Ainda noutra modalidade, a geração de código de aprovação de nível de risco compreende selecionar um algoritmo criptográfico a partir de um conjunto de algoritmos criptográficos com base no nível de risco e aplicar o algoritmo criptográfico selecionado a um segredo e uma variável dinâmica. Ainda noutra modalidade, a geração de código de aprovação de nível de risco compreende selecionar valores para um ou mais parâmetros a partir de um conjunto de valores para estes parâmetros respectivos com base no nível de risco e usar os valores dos parâmetros selecionados, quando se aplica um algoritmo de geração de código de aprovação nível de risco a um segredo e uma variável dinâmica. Numa modalidade específica, estes parâmetros podem incluir o comprimento do código de aprovação de nível de risco a ser gerado ou que bits devem ser selecionados a partir de uma *string* binária onde esta *string* binária pode incluir, por exemplo, um criptograma.

Uma modalidade preferida da presente invenção inclui um método para certificar transações eletrônicas compreendendo as etapas de:

- definir um número limitado de categorias de transação;
- 5 • definir critérios para classificar cada transação possível numa destas categorias de transação;
- receber uma transação a partir de um usuário;
- aplicar os critérios acima a uma transação recebida e atribuir uma transação recebida a uma das categorias acima;
- 10 • proporcionar meios para que um usuário gere uma prova de sua intenção de fazer uma transação que pertence a uma certa categoria;
- receber a partir de um usuário prova de sua intenção de fazer uma transação que pertence a certa categoria;
- 15 • verificar para uma transação recebida a prova correspondente da intenção do usuário de fazer uma transação que pertence à mesma categoria que a transação recebida.

Em algumas modalidades, as categorias de transação podem ter sido definidas de um modo implícito. Em outras modalidades, os critérios para classificar transações podem ser codificados implicitamente como um fluxo de programa do aplicativo.

Outra modalidade preferida da presente invenção inclui um método para assegurar transações eletrônicas compreendendo as etapas de:

- 25 • armazenar critérios, para posterior recuperação, para classi-

ficar transações num número limitado de categorias de transação

- receber uma transação a partir de um usuário;
- aplicar os critérios acima a uma transação recebida e atribuir uma transação recebida a uma das categorias acima;
- proporcionar meios para que um usuário gere uma prova de sua intenção de fazer uma transação que pertence a certa categoria;
- receber a partir de um usuário prova de sua intenção de fazer uma transação que pertence a certa categoria;
- verificar, para uma transação recebida, a prova correspondente da intenção do usuário de fazer uma transação que pertence à mesma categoria que a transação recebida.

De preferência, as categorias de transação são significativas para o usuário ordinário e os critérios para classificar as transações nestas categorias podem ser automaticamente aplicados pelo servidor de verificação e podem também ser facilmente aplicados pelo usuário ordinário. De preferência, o número de categorias de transação ou níveis de risco é de pelo menos dois e menos do que seis.

Numa modalidade, os critérios para classificar transações incluem critérios relacionados ao risco que estas transações representam. Noutra modalidade, os critérios para classificar transações incluem critérios para estimar a suscetibilidade à fraude das transações.

Em algumas modalidades, algumas etapas do método podem ser realizadas por um sistema de computador. Este sistema de computador pode compreender um computador de servidor. Pode

também compreender um banco de dados e pode também compreender um Módulo de Segurança de Hardware (HSM) para realizar certas operações criptográficas.

Uma modalidade específica da presente invenção compreende um método para assegurar um aplicativo de Internet *banking*. Nesta modalidade, os critérios de classificação podem compreender o tipo de transação (os exemplos de tipos de transação podem incluir: recuperação de informações tais como informações do saldo de conta, operações de investimento tais como comércio de mercadorias, transferências de dinheiro, configuração de conta tais como atualizações de informações de endereço). Outros critérios de classificação que podem ser usados incluem a quantidade de dinheiro envolvido (por exemplo, a quantidade de dinheiro a ser transferida ou investida) em que caso podem ser definidos certos limites (por exemplo, para distinguir entre transações de transferência de dinheiro com uma quantidade baixa e alta de dinheiro a ser transferida) ou a propriedade das contas envolvidas na transação (por exemplo, se a conta para a qual o dinheiro deveria ser transferido é possuída pelo usuário ou é possuída por outra pessoa) ou o padrão histórico das transações do usuário (por exemplo, se a conta para a qual o dinheiro tem de ser transferido já foi usada antes pelo usuário para transferir dinheiro).

Em outras modalidades, outros tipos de aplicativos com outros tipos de transações podem ser assegurados pela presente invenção. Esses aplicativos podem incluir qualquer aplicativo remotamente acessível e essas transações podem incluir qualquer interação entre um usuário e o sistema remoto que implique uma mudança no estado do sistema. Um exemplo desse sistema poderia ser uma ferramenta tal como um *Firewall* por meio do qual o usuário é um operador dessa ferramenta e por meio do qual as transações incluem ações para administrar a ferramenta. Neste exemplo, algumas transações tais como,

por exemplo, monitoração de tráfego ou recuperação de estatísticas podem ser consideradas transações de risco baixo, enquanto outras transações tais como, por exemplo, mudar a configuração do *Firewall* incluindo abertura ou fechamento de certas portas podem ser consideradas transações de alto risco.

Numa modalidade preferida da invenção, um código de aprovação de nível de risco de transação é verificado por um servidor de validação usando um valor de referência de verificação. Numa modalidade, o referido valor de referência de verificação é gerado usando o mesmo algoritmo ou um algoritmo semelhante ao que era usado para gerar o código de aprovação de nível de risco. Noutra modalidade, o valor de referência de verificação é gerado usando um segredo que é direta ou indiretamente associado ao usuário ou um dispositivo de segurança usado pelo usuário para gerar o código de aprovação de nível de risco. Numa modalidade específica, este segredo é recuperado a partir de um banco de dados. Noutra modalidade específica, este segredo é gerado usando um segredo-mestre e um valor que é direta ou indiretamente associado ao usuário ou um dispositivo de segurança usado pelo usuário para gerar o código de aprovação de nível de risco. Ainda noutra modalidade, o valor de referência de verificação é comparado ao código de aprovação de nível de risco recebido a partir do usuário e o código de aprovação de nível de risco é validado com sucesso se ele coincidir com o valor de referência de verificação, de acordo com algum critério de comparação. Numa modalidade específica, o critério de comparação pode exigir que ambos os valores sejam iguais.

Outra modalidade preferida da presente invenção inclui um equipamento de segurança para gerar códigos de aprovação do nível de risco de transações. O equipamento de segurança para gerar códigos de aprovação do nível de risco de transações tem, de preferência, um fator de forma compacta e uma interface simples com o usuário exigin-

do poucas interações do usuário. A interface com o usuário compreende, de preferência, meios de entrada que permitem ao usuário selecionar o nível de risco apropriado e instruir o equipamento de segurança a gerar um código de aprovação de nível de risco correspondente. A interface com o usuário compreende também, de preferência, meios de saída para comunicar, por exemplo, códigos de aprovação de nível de risco gerados.

Numa modalidade, os meios de entrada podem, por exemplo, compreender um ou mais botões ou uma roda de polegar.

Numa modalidade particular, o usuário seleciona o nível de risco apropriado pressionando ou empurrando um botão ou uma combinação específica de botões associados àquele nível de risco. Noutra modalidade particular, o usuário seleciona o nível de risco apropriado rolando uma lista de etiquetas, representando cada etiqueta um nível de risco particular. Numa modalidade específica, o usuário rola esta lista repetidamente empurrando um botão. Noutra modalidade específica, o usuário seleciona o nível de risco apropriado pressionando depressa várias vezes um botão específico por meio do que o número de vezes que o botão foi apertado indica que nível de risco o usuário pretende selecionar. Ainda noutra modalidade particular, o usuário rola a lista usando uma roda de polegar. Ainda noutra modalidade particular, o usuário instrui o equipamento de segurança a gerar um código de aprovação de nível de risco para um nível de risco selecionado apertando um botão ou empurrando uma roda de polegar. Ainda noutra modalidade específica, o equipamento de segurança gera automaticamente um código de aprovação de nível de risco para um nível de risco atualmente selecionado depois de certo tempo de espera durante o qual o usuário não seleciona outro nível de risco.

Noutra modalidade, a interface do usuário do equipamento de segurança compreende meios de saída para comunicar um código

de aprovação de nível de código gerado para o usuário ou para indicar que nível de risco está atualmente selecionado. Este meio de saída pode compreender, por exemplo, uma tela ou meios para gerar sinais audíveis que podem incluir fala sintetizada ou fragmentos de voz gravados. Em algumas modalidades, o nível de risco atualmente selecionado é indicado usando etiquetas. Estas etiquetas podem ser numéricas ou podem compreender palavras. Numa modalidade específica, estas etiquetas podem referir-se diretamente ao nível de risco. Noutra modalidade específica, estas etiquetas podem referir-se a certas características das transações associadas a um nível de risco particular que são facilmente discerníveis e significativas para o usuário.

Numa modalidade, o equipamento de segurança tem o fator de forma de um *token* de autenticação forte. Noutra modalidade, o equipamento de segurança tem o fator de forma de um cartão de crédito.

Numa modalidade, um segredo usado na geração do código de aprovação de nível de risco está armazenado com segurança no equipamento de segurança. Noutra modalidade, um segredo usado na geração do código de aprovação de nível de risco está armazenado num segundo equipamento que pode ser acessado pelo equipamento de segurança. Este segundo equipamento pode ser, por exemplo, um cartão inteligente. Ainda noutra modalidade, pelo menos uma parte do algoritmo para gerar um código de aprovação de nível de risco é realizada por um segundo equipamento que pode ser acessado pelo equipamento de segurança. Este segundo equipamento pode ser, por exemplo, um cartão inteligente.

Efeitos Vantajosos

Uma vantagem importante da presente invenção é que pode oferecer um nível significativamente mais alto de segurança do que

a segurança oferecida pelo uso de *tokens* de autenticação fortes tradicionais que geram senhas dinâmicas (e *a fortiori* o nível de segurança oferecido pelo uso de senhas estáticas), mas, a um custo e com um nível de conveniência para o usuário que é bem parecido ao custo e à

5 conveniência destes *tokens*.

Isto é ilustrado no exemplo seguinte. Um aplicativo de Internet *banking* típico pode suportar principalmente dois tipos de transações: visualizar informações de conta tais como o saldo e a história de transações, por um lado, e fazer transferências de dinheiro,

10 por outro lado. Este aplicativo pode ser assegurado por senhas estáticas, isto é, os usuários devem autenticar eles mesmos antes que tenham permissão para efetuar uma transação proporcionando uma senha estática. A prática mostrou que as senhas estáticas proporcionam um nível completamente inadequado de segurança. Realmente, foi

15 mostrado repetidamente que as senhas estáticas são demasiadamente vulneráveis a todos os tipos de ataques incluindo ataques de *phishing* em que os atacantes obtêm senhas válidas que eles subsequenteiramente podem usar para propósitos fraudulentos. O uso de *tokens* de autenticação forte que geram senhas dinâmicas proporciona um nível muito

20 mais alto de segurança, visto que estas senhas dinâmicas são tipicamente usadas apenas uma vez e - no caso particular de *tokens* baseadas no tempo - têm um período de validade muito limitado. Contudo, existem ataques mais sofisticados por meio dos quais são obtidas senhas válidas e usadas quase em tempo real dentro de seu período de

25 validade. Um exemplo desse ataque é um Ataque de Homem no Meio (MITMA) em que um atacante conseguiu interceptar e manipular as comunicações entre o usuário e o aplicativo de tal forma que o atacante consegue capturar as credenciais de autenticação do usuário (incluindo quaisquer senhas dinâmicas) e/ou consegue substituir os dados reais

30 da transação pelos dados fraudulentos de transação do atacante. Em muitos casos tais como um MITMA, exige-se que o usuário seja um

pouco desajeitado para checar, por exemplo, se o URL do sítio do aplicativo é correto e se o certificado SSL/TLS do site é válido. Infelizmente, os usuários na vida real muito freqüentemente se comportam de forma bastante descuidada e não notam ou ignoram anomalias que deveriam alertá-los de que algo suspeito está ocorrendo ou são suficientemente crédulos para ficarem facilmente seguros para aceitar estas anomalias e introduzir as suas credenciais de autenticação. Uma vez que os atacantes tenham obtido um conjunto válido de credenciais de autenticação, eles podem realizar qualquer transação que normalmente apenas o usuário real deveria ser intitulado a fazer, por exemplo, transferindo dinheiro da conta do usuário para a conta do atacante.

A presente invenção torna esses ataques muito menos prováveis de terem sucesso. De acordo com a invenção, o aplicativo de Internet *banking* do exemplo pode dividir todas as transações em três grupos, cada um dos quais com o seu próprio nível de risco associado:

- transações de visualização da conta: como é bastante improvável que um atacante possa beneficiar-se financeiramente às custas do usuário legítimo a partir dessa transação de visualização de conta, este grupo de transações representa um risco bastante baixo.
- Transferências de dinheiro para um parceiro presumivelmente confiável: estes parceiros presumivelmente confiáveis podem incluir, por exemplo, aqueles parceiros a quem o usuário já transferiu dinheiro antes ou companhias de utilidades bem conhecidas. Como esses parceiros presumivelmente confiáveis são improváveis de coincidir com atacantes, estas transações podem ser consideradas como de risco médio.
- Outras transferências de dinheiro: como transações fraudulentas são prováveis de serem transferências de dinheiro para

um parceiro obscuro que é desconhecido do usuário legítimo, estas transações são melhor consideradas como de alto risco.

Os usuários legítimos são providos de pequenos dispositivos de segurança que são capazes de gerar três tipos de códigos de aprovação de nível de risco: códigos de aprovação nível de risco baixo, códigos de aprovação de nível de risco médio e códigos de aprovação nível de risco alto. Quando os usuários quiserem fazer uma transação, o aplicativo exige que eles proporcionem um código de aprovação apropriado correspondendo ao nível de risco da transação.

Como consequência, um atacante que, de alguma maneira, obteve um código de aprovação de risco baixo válido, por exemplo, por meio de um ataque MITMA, não pode usar aquele código de aprovação de nível de risco baixo para injetar uma transação fraudulenta que tem as características de uma transação de nível de risco médio ou alto. Em outras palavras, ainda que um atacante seja bem sucedido em montar um ataque MITMA contra certa sessão, o atacante será em geral capaz de apenas usar aquela sessão para fazer uma transação fraudulenta, se o usuário realmente gerar um código de aprovação de nível de risco alto. Na prática, a maioria das transações realizadas por usuários legítimos do aplicativo de Internet *banking* seriam transações de nível de risco baixo ou médio com as transações de nível de risco alto constituindo uma fração relativamente pequena da quantidade total de transações. Isso significa que a taxa de sucesso de ataques automaticamente será reduzida de modo significativo, visto que, na prática, a maioria das sessões de transação não pode mais ser usada por atacantes, visto que eles não produzirão um código de aprovação válido de nível de risco alto de que os atacantes precisam para poder injetar com sucesso as suas transações fraudulentas.

A invenção também fortalece a segurança do aplicativo de outro modo. Para montar um ataque MITMA bem sucedido ou de outra

forma obter credenciais de autenticação válidas, os atacantes normalmente têm que contar com certo descuido dos usuários legítimos, quando se conectam ao aplicativo. Esse descuido origina-se frequentemente do fato de que os usuários tendem a esquecer ou ignorar que mesmo uma conexão para fazer uma transação absolutamente inocente tal como visualizar o saldo de sua conta poderia potencialmente ser seqüestrada por um atacante para um tipo completamente diferente de transação. Também não pode ser esperado que os usuários típicos estejam sempre alerta para qualquer transação que queiram fazer. Todavia, é provável que os usuários típicos estejam muito vigilantes, quando fazem uma transação de nível de risco alto e tomem cuidado extra em verificar que nada suspeito está ocorrendo, quando lhes for pedidos que forneçam um código de aprovação de nível de risco alto. Como resultado, os atacantes serão muito menos bem sucedidos em montar um ataque MITMA contra uma sessão de transação de nível de risco alto ou, de outra forma, obter um código de aprovação de nível de risco alto.

Uma vantagem extra da invenção é que este nível mais alto de segurança não vem às custas de uma conveniência reduzida para o usuário. Por exemplo, numa modalidade, o dispositivo de segurança para gerar os códigos de aprovação de nível de risco poderia ter o mesmo fator de forma de um *token* de autenticação forte tradicional. O dispositivo de segurança poderia ser um dispositivo compacto pequeno com uma tela e um botão. Apertando o botão uma vez o usuário instrui o dispositivo a gerar um código de aprovação de nível de risco baixo. Pressionando rapidamente o botão duas vezes o usuário instrui o dispositivo a gerar um código de aprovação de nível de risco médio. Para instruir o dispositivo a gerar um código de aprovação de nível de risco alto, o usuário pressiona depressa o botão três vezes. Em outras palavras, usando um dispositivo com exatamente o mesmo fator de forma que um *token* de autenticação forte tradicional e com apenas

qualquer interação extra exigida do usuário, pode ser obtido um nível de segurança significativamente mais alto com respeito ao uso de *tokens* de autenticação forte tradicional que apenas gerem senhas dinâmicas. Noutra modalidade, o dispositivo de segurança tem três
5 botões, um para cada nível de risco diferente. O usuário instrui o dispositivo a gerar o código de aprovação de nível de risco apropriado apertando o botão correspondente. Em outras palavras, usando um dispositivo com um fator de forma compacto bem parecido com um *token* de autenticação forte tradicional e sem qualquer interação extra
10 exigida do usuário, pode ser obtido um nível de segurança significativamente mais elevado com respeito ao uso de *tokens* de autenticação forte tradicional que apenas gerem senhas dinâmicas.

As vantagens da invenção tornam-se particularmente evidentes, quando se considera dispositivos de segurança conformados
15 em cartão de crédito flexível. A tecnologia para produzir esses dispositivos não está ainda madura, exigindo componentes caros e resultando freqüentemente em problemas de rendimento e confiabilidade. Em particular, os botões para que os usuários proporcionem a entrada levantam problemas. Na prática, é bastante difícil produzir de maneira
20 confiável dispositivos de segurança conformados em cartões de crédito flexíveis com botões que respondam suficientemente aos pressionamentos de teclas do usuário. Uma porcentagem relativamente grande dos botões responde insuficientemente ou não responde mesmo. Isso significa que a presença de botões tem um efeito negativo no rendimento
25 e/ou conveniência do usuário de dispositivos de segurança conformados em cartões de crédito flexíveis. Cada botão extra agrava o problema. Como consequência, a produção de *tokens* de assinatura de transações conformados em cartões de crédito flexíveis com um teclado numérico compreendendo tipicamente pelo menos 10 botões tem um
30 rendimento muito baixo, que, em combinação com o alto custo de componentes torna-os proibitivamente caros. Todavia, a presente

invenção permite produzir dispositivos de aprovação de nível de risco conformados em cartões de crédito flexíveis que, ao mesmo tempo em que oferecem um nível de segurança significativamente mais alto do que os *tokens* de autenticação forte tradicional que apenas geram senhas dinâmicas, exigem apenas poucos botões e interações do usuário, tendo, deste modo, o mesmo custo ou semelhante ao de *tokens* de autenticação forte conformados em cartão de crédito flexível de um botão e oferecendo o mesmo nível de conveniência para o usuário ou semelhante.

Breve Descrição dos Desenhos

A **Figura 1a** ilustra um método de acordo com a presente invenção.

A **Figura 1b** ilustra outro método de acordo com a presente invenção.

A **Figura 1c** ilustra ainda outro método de acordo com a presente invenção.

A **Figura 1d** ilustra ainda outro método de acordo com a presente invenção.

A **Figura 2a** ilustra um método para gerar códigos de aprovação de categorias de transações dinâmicas de acordo com uma modalidade da invenção.

A **Figura 2b** ilustra um método alternativo de gerar um código de aprovação de nível de risco de acordo com outra modalidade da invenção.

A **Figura 2c** ilustra outro método de gerar um código de aprovação de nível de risco de acordo ainda com outra modalidade da

invenção.

A **Figura 3a** ilustra um equipamento de segurança para gerar códigos de aprovação de nível de risco de acordo com uma modalidade da invenção.

5 A **Figura 3b** ilustra outro equipamento de segurança para gerar códigos de aprovação de nível de risco de acordo com uma modalidade da invenção.

10 A **Figura 3c** ilustra ainda outro equipamento de segurança para gerar códigos de aprovação de nível de risco de acordo com uma modalidade da invenção.

A **Figura 4a** ilustra um fator de forma particular de um equipamento de segurança para gerar códigos de aprovação de nível de risco.

15 A **Figura 4b** ilustra outro fator de forma de um equipamento de segurança para gerar códigos de aprovação de nível de risco.

A **Figura 4c** ilustra ainda outro fator de forma de um equipamento de segurança para gerar códigos de aprovação de nível de risco.

20 A **Figura 4d** ilustra ainda outro fator de forma de um equipamento de segurança para gerar códigos de aprovação de nível de risco.

A **Figura 4e** ilustra um fator de forma mais de um equipamento de segurança para gerar códigos de aprovação de nível de risco.

Uma modalidade preferida do método da presente invenção para assegurar transações eletrônicas, conforme ilustrado na **Figura 1a**, compreende as etapas de:

- 5 • definir um número limitado de categorias de transação (etapa **100**);
- definir critérios para classificar cada transação possível em uma destas categorias de transação (etapa **110**);
- 10 • proporcionar meios para um usuário gerar uma prova de sua intenção de fazer uma transação que pertence a certa categoria (etapa **120**);
- receber uma transação a partir de um usuário (etapa **130**);
- aplicar os critérios acima a uma transação recebida e atribuir uma transação recebida a uma das categorias acima (etapa **140**);
- 15 • receber a partir de um usuário prova de sua intenção de fazer uma transação que pertence a certa categoria (etapa **150**);
- verificar, para uma transação recebida, a prova correspondente da intenção do usuário de fazer uma transação que pertence à mesma categoria que a transação recebida (etapa **160**).
- 20

Outra modalidade do método da presente invenção para assegurar transações eletrônicas, conforme ilustrado na **Figura 1b**, compreende as etapas de:

- 25 • definir critérios para segmentar as transações numa pluralidade de categorias (etapa **111**);

- associar um nível de risco a cada uma destas categorias (etapa **115**);
- proporcionar aos usuários meios para gerar códigos de aprovação de nível de risco de transação (etapa **121**);
- 5 • receber a partir dos usuários dados da transação (etapa **131**);
- aplicar os critérios definidos para as transações recebidas para determinar para as transações recebidas os níveis de risco correspondentes (etapa **141**);
- 10 • receber a partir dos usuários códigos de aprovação do nível de risco de transação associados às transações (etapa **151**);
- calcular valores de referência de verificação para as transações recebidas em base dos níveis de risco correspondentes determinados (etapa **164**);
- 15 • comparar, para as transações recebidas, os códigos de aprovação de nível de risco recebidos com os valores de referência de verificação calculados correspondentes de acordo com algum critério de comparação (etapa **165**); e
- 20 • fazer uma aprovação das transações recebidas dependente da comparação dos códigos de aprovação de nível de risco correspondentes recebidos com os valores de referência de verificação calculados correspondentes (etapa **166**).

Ainda outra modalidade do método da presente invenção para assegurar transações eletrônicas, conforme ilustrado na **Figura**
25 **1c**, compreende as etapas de:

- armazenar critérios, para recuperação mais adiante, para

classificar transações num número limitado de categorias de transação (etapa **115**);

- proporcionar meios para que um usuário gere uma prova de sua intenção de fazer uma transação que pertence a certa categoria (etapa **122**);
- receber uma transação a partir de um usuário (etapa **132**);
- aplicar os critérios acima a uma transação recebida e atribuir uma transação recebida a uma das categorias acima (etapa **142**);
- receber a partir de um usuário prova de sua intenção de fazer uma transação que pertence a certa categoria (etapa **152**);
- verificar para uma transação recebida a prova correspondente da intenção do usuário de fazer uma transação que pertence à mesma categoria que a transação recebida (etapa **162**).

Ainda outra modalidade do método da presente invenção para assegurar transações eletrônicas, conforme ilustrado na **Figura 1d**, compreende as etapas de:

- proporcionar aos usuários meios de gerar códigos de aprovação de nível de risco de transação com base num nível de risco de uma transação particular fora de um conjunto de níveis de risco plurais associados a diferentes transações (etapa **123**);
- receber a partir de usuários os dados da transação de (etapa **133**);

- aplicando critérios definindo níveis de risco diferentes para as transações recebidas para determinar para as transações recebidas os níveis de risco correspondente (etapa **143**);
- 5 • receber a partir dos usuários os códigos de aprovação de nível de risco de transação associados às transações (etapa **153**);
- calcular valores de referência de verificação para as transações recebidas com base nos níveis de risco correspondentes determinados (etapa **167**);
- 10 • comparar para as transações recebidas os códigos de aprovação de níveis de risco recebidos com os valores de referência de verificação calculados correspondentes de acordo com algum critério de comparação (etapa **168**); e
- 15 • fazer uma aprovação das transações recebidas dependentes da comparação dos códigos de aprovação de nível de risco correspondentes recebidos com os valores de referência de verificação calculados correspondentes (etapa **169**).

Numa modalidade da invenção a prova da intenção do usuário de fazer uma transação que pertence a certa categoria compreende um código dinâmico de aprovação de categoria de transação. 20 Noutra modalidade da invenção, a prova da intenção do usuário de fazer uma transação que pertence a certa categoria compreende um código de aprovação de nível de risco de transação. Ainda noutra modalidade, um código de aprovação de nível de risco de transação 25 compreende um código dinâmico de aprovação.

A **Figura 2a** ilustra um método preferido de acordo com a invenção de gerar códigos dinâmicos de aprovação compreendendo as etapas de:

- obter um indicador da categoria da transação (etapa **210**);
- capturar o valor de pelo menos uma variável dinâmica (etapa **220**);
- recuperar um ou mais valores secretos (etapa **230**);
- 5 • combinar criptograficamente o referido indicador de categoria de transação, o citado valor dinâmico e ditos um ou mais valores secretos (etapa **240**); e
- transformar o resultado da referida combinação criptográfica num código dinâmico de aprovação (etapa **250**).

10 Numa modalidade, o indicador da categoria de transação pode compreender um indicador de nível de risco. Noutra modalidade, a variável dinâmica pode ser o tempo relacionado. Numa modalidade específica, a variável dinâmica compreende o valor de um relógio de tempo real. Ainda noutra modalidade, a variável dinâmica compreende

15 o valor de um contador. Ainda noutra modalidade, a combinação criptográfica do indicador, o valor dinâmico e um ou mais valores secretos compreende a geração de um criptograma usando uma combinação matemática do indicador e o valor dinâmico e usando um algoritmo criptográfico que é parametrizado com o citado um ou mais

20 valores secretos.

Um método alternativo de acordo com a invenção para gerar códigos dinâmicos de aprovação é ilustrado na **Figura 2b** e compreende as etapas de:

- obter um indicador da categoria de transação (etapa **210**);
- 25 • capturar o valor de pelo menos uma variável dinâmica (etapa **220**);

- recuperar um conjunto de valores secretos (etapa **231**);
- seleccionar pelo menos um valor secreto fora do conjunto recuperado de valores secretos com base no valor do indicador da categoria de transação (etapa **235**);
- 5 • criptograficamente combinar o referido indicador, o citado valor dinâmico e dito valor secreto seleccionado (etapa **241**); e
- transformar o resultado da referida combinação criptográfica num código dinâmico de aprovação (etapa **250**).

10 Ainda outro método de acordo com a invenção de gerar códigos dinâmicos de aprovação é ilustrado na **Figura 2c** e compreende as etapas de:

- obter um indicador da categoria de transação (etapa **210**);
- capturar o valor de pelo menos uma variável dinâmica (etapa **220**);
- 15 • recuperar o valor de um segredo-mestre (etapa **232**);
- derivar um valor secreto a partir do segredo-mestre recuperado e o indicador da categoria de transação (etapa **236**);
- criptograficamente combinar o referido indicador, o citado valor dinâmico e dito valor secreto derivado (etapa **242**); e
- 20 • transformar o resultado da referida combinação criptográfica num código dinâmico de aprovação (etapa **250**).

Numa modalidade, a etapa de derivar um valor secreto a partir do segredo-mestre recuperado e o indicador de categoria de transação compreende combinar criptograficamente o segredo-mestre e

o indicador de categoria de transação. Numa modalidade específica, combinar criptograficamente compreende usar uma criptografia ou algoritmo de decodificação que atua sobre dados relacionados ao indicador da categoria de transação e parametrizado com o segredo-mestre.

- 5 Noutra modalidade específica, combinar criptograficamente compreende dados relacionados ao indicador de categoria de transação e o segredo-mestre.

Numa modalidade os meios de gerar códigos de aprovação de nível de risco de transação compreendem um equipamento de
10 segurança. Um equipamento de segurança para gerar códigos de aprovação de nível de risco é freqüentemente provido na forma de um equipamento manual, alimentado por bateria com meios de saída tais como uma tela para transferir códigos de aprovação e outras informações para o usuário. Freqüentemente, o equipamento tem um ou mais
15 botões ou outros meios de entrada para disparar a geração de código de aprovação do nível de risco de transação e/ou selecionar o nível de risco apropriado para o qual um código de aprovação deve ser gerado.

Numa modalidade preferida do equipamento da presente invenção, conforme ilustrada em **Figura 3a**, o equipamento é um *token*
20 de segurança **300** para gerar códigos dinâmicos de aprovação de categoria de transação. O *token* de segurança **300** compreende tipicamente uma armazenagem de chave secreta **310**, uma fonte de variabilidade **320**, um agente criptográfico **330**, um agente de transformação **340**, uma interface de entrada **350**, uma interface de saída **360** e uma fonte
25 de energia **370**.

A armazenagem de chave secreta **310** armazena uma ou mais chaves secretas – de preferência, num modo seguro – que pode ser usado na geração de códigos dinâmicos de aprovação. A armazenagem de chave secreta **310** pode compreender uma memória volátil, tal como
30 a memória de um processador ou microcontrolador já presente no

token, ou um componente de memória separada de acesso aleatório (RAM), por meio do qual esta memória é permanentemente alimentada por uma bateria para impedir a perda dos dados armazenados. Alternativamente, a armazenagem da chave secreta **310** pode ser uma
5 memória persistente tal como um componente de memória flash.

A fonte de variabilidade **320** proporciona uma variável dinâmica que pode compreender um tempo-relacionado valor ou um valor de contador. A fonte de variabilidade **320** pode compreender um relógio de tempo real ou um contador. O contador pode ser automati-
10 camente incrementado toda a vez em que for gerado um código dinâmico de aprovação.

O agente criptográfico **330** pode ser um processador ou microcontrolador apropriadamente programado ou hardware dedicado tal como um Circuito Integrado Específico do Aplicativo (ASIC) ou
15 Conjunto Ordenado de Pórtico de Campo Programável (FPGA).

Também o agente de transformação **340** pode ser um processador ou microcontrolador apropriadamente programado ou um hardware dedicado tal como um Circuito Integrado Específico do Aplicativo (ASIC) ou um Conjunto Ordenado de Pórtico de Campo Programável
20 (FPGA).

O agente criptográfico **330** e o agente de transformação **340** podem ser implementados na mesma plataforma de hardware ou numa plataforma de hardware diferente.

A interface de entrada **350**, que pode compreender um
25 dispositivo de interface humana ou uma interface máquina a máquina, permite ao usuário instruir o *token* a gerar um código dinâmico de aprovação ou selecionar uma categoria de transação ou um nível de risco para o qual um código dinâmico de aprovação deve ser gerado. O

dispositivo de interface humana pode compreender um ou mais botões. O dispositivo de entrada de interface humana pode também ou alternativamente compreender uma roda de polegar.

Os códigos dinâmicos de aprovação gerados podem ser proporcionados para a interface de saída de usuário final através de **360**. Noutra modalidade, o *token* inclui uma interface de saída do código de aprovação **360**, tal como um dispositivo de interface humana ou uma interface máquina a máquina, adaptada para dar saída a um código dinâmico gerado de aprovação. O dispositivo de saída de interface humana pode compreender um dispositivo de saída visual, tal como uma tela, ou um dispositivo de saída audível, tal como uma fonte de fala sintetizada. O código dinâmico de aprovação a que é dada saída pelo dispositivo de saída de interface humana pode ser comunicado ao usuário como uma *string* ou seqüência de símbolos interpretáveis pelas pessoas humanas.

A interface máquina a máquina da interface de entrada **350** ou da interface de saída **360** pode compreender uma interface de USB, *Ethernet*, *serial* ou outra interface protegida ou um *Bluetooth*, WiFi, celular ou outra interface sem fio.

A fonte de energia **370** proporciona a energia exigida pelos outros componentes. A fonte de energia **370** pode compreender uma bateria, uma célula de fotografia voltaica, uma célula de combustível, um elemento termoeletrico, um agente adaptado para capturar a energia ambiente ou qualquer outra fonte de energia que seja compatível com os requisitos de energia dos outros componentes e o custo global e requisitos fator de forma do *token* de segurança **300**.

O *token* de segurança **300** opera tipicamente como se segue. Por meio da interface de entrada **350**, o usuário seleciona uma categoria de transação ou nível de risco apropriado e instrui o *token* a

gerar um código dinâmico de aprovação correspondente. O agente criptográfico **330** combina criptograficamente uma ou mais chaves recuperadas a partir de armazenagem de chave secreta **310** com o valor de uma variável dinâmica proporcionado pela fonte de variabilidade **320** e um indicador da categoria de transação ou nível de risco selecionado pela interface de entrada do usuário através de **350**. O agente de transformação **340** transforma o resultado da combinação criptográfica num código dinâmico de aprovação. O *token* dá saída ao código dinâmico de aprovação gerado por meio da interface de saída **360**.

10 Numa modalidade, estes componentes são dispostos sobre um substrato tal como um PCB. Em outras modalidades, estes componentes são alojados numa concha protetora que pode ser de plástico. Ainda noutras modalidades, estes componentes são embutidos num meio laminado.

15 Ainda outra modalidade, conforme ilustrada na **Figura 3b**, alguns destes componentes podem ser incorporados num dispositivo físico (**301**), enquanto outros componentes podem ser incorporados num segundo dispositivo (**302**) por meio do que são gerados os códigos dinâmicos de aprovação de categoria de transação pelos dois dispositivos juntos em co-operação fechada. Alguns destes componentes podem ser divididos sobre ambos os dispositivos. Por exemplo, o primeiro dispositivo (**301**) pode compreender uma primeira parte do agente criptográfico **330**, enquanto o segundo dispositivo (**302**) pode compreender uma segunda parte do agente criptográfico **330**. O mesmo pode ser verdade para o agente de transformação **340** ou a fonte de variabilidade **320**. Numa modalidade particular, conforme ilustrada na **Figura 3c**, o primeiro dispositivo (**301**) pode compreender um leitor de cartão inteligente sem conexão alimentado por uma bateria (**370**), com uma interface de saída (**360**) compreendendo uma imagem, compreendendo
25 uma interface de entrada (**350**) um botão, um relógio de tempo real
30

(321) proporcionando um valor de tempo relacionado, um microprocessador (341) para realizar operações criptográficas e/ou de transformação e uma interface de cartão inteligente (355) para se comunicar com um cartão inteligente inserido; enquanto o segundo dispositivo (302) pode ser um cartão inteligente que compreende uma memória secreta (310), um microprocessador (331) para operações criptográficas e um contador (322) para proporcionar um valor de contador. Por exemplo, um leitor de cartão inteligente sem conexão e um cartão inteligente inserido podem gerar em conjunto um código dinâmico de aprovação como segue. Por meio de um ou mais botões no leitor, o usuário seleciona uma categoria de transação ou um nível de risco e instrui o leitor a gerar um código dinâmico de aprovação para a categoria de transação ou nível de risco selecionado. O leitor comunica-se com o cartão inteligente inserido pela interface do cartão inteligente por meio de comandos de cartão inteligente. Com estes comandos de cartão inteligente, o leitor comunica um valor que representa a categoria de transação ou nível de risco selecionado para o cartão inteligente e instrui o cartão inteligente a gerar um criptograma usando esse valor. O processador criptográfico do cartão inteligente gera um criptograma usando o valor recebido que representa a categoria de transação ou o nível de risco selecionado, um contador que mantém e que automaticamente incrementa todo a vez em que gera um criptograma e uma chave secreta que ele armazena em sua memória segura não volátil. O cartão inteligente envia o criptograma gerado e o valor de contador que foi usado de volta para o leitor. O microprocessador do leitor seleciona um grupo de bits do criptograma e o valor do contador e transforma a cadeia binária resultante numa sequência de dígitos decimais ou uma sequência de outros símbolos interpretáveis pelas pessoas humanas. O leitor dá saída a esta sequência de dígitos ou outros símbolos em sua tela. Numa variante desta modalidade, o cartão inteligente meramente armazena um valor secreto e retorna uma chave secreta para o leitor e o processador do leitor gera o criptograma.

A **Figura 4a** ilustra uma modalidade particular de um equipamento de segurança de acordo com a invenção compreendendo um *token* **401** para gerar códigos dinâmicos de aprovação. A sua interface de saída compreende uma tela **461**. A sua interface de entrada compreende vários botões **451**, um para cada categoria de transação ou nível de risco diferente. No exemplo ilustrado, o *token* tem três botões, porque suporta a geração de códigos dinâmicos de aprovação para três categorias de transação ou níveis de risco de transação diferentes. Uma etiqueta ou símbolo indicando a categoria de transação ou nível de risco correspondente pode estar impressa no alojamento de plástico do *token* perto de cada botão ou os próprios botões. Quando o usuário apertar um botão, o *token* se energiza, gera um código dinâmico de aprovação para a categoria de transação ou nível de risco e dá saída ao código dinâmico de aprovação gerado em sua tela.

A **Figura 4b** ilustra outra modalidade particular de um equipamento de segurança de acordo com a invenção compreendendo um *token* **402** para gerar códigos dinâmicos de aprovação. A sua interface de saída compreende uma tela **462**. A sua interface de entrada compreende dois botões **452/453**. Um botão **452** permite ao usuário circular através de uma lista de categorias de transação ou níveis de risco suportados. Quando o usuário apertar este botão, o *token* seleciona a categoria de transação ou o nível de risco seguinte. O *token* indica que categoria de transação ou nível de risco é atualmente selecionada por meio de uma etiqueta ou símbolo apropriado que é exibido na tela **462**. Estas etiquetas podem incluir, por exemplo, baixo, médio, alto ou log -in, pague, pague alto. Se o usuário apertar o outro botão **453**, o *token* gera um código dinâmico de aprovação pelo código de categoria de transação ou nível de risco atualmente selecionado e dá saídas a este código dinâmico de aprovação gerado na sua tela **462**.

A **Figura 4c** ilustra ainda outra modalidade particular de

um equipamento de segurança de acordo com a invenção compreendendo um *token* **404** para gerar códigos dinâmicos de aprovação que têm o fator de forma de um cartão de crédito. A sua interface de saída compreende uma tela **464**. A sua interface de entrada compreende um

5 botão **454**. Se o usuário apertar o botão pelo menos uma vez, o *token* é energizado. O número de vezes em que o botão **454** foi apertado determina que categoria de transação ou nível de risco está atualmente selecionada. Por exemplo, apertando o botão **454** depressa duas vezes, a segunda categoria de transação ou nível de risco da lista de categorias

10 de transação ou nível de risco suportado é selecionada. Para selecionar a terceira categoria de transação ou nível de risco da lista, o usuário aperta depressa o botão **454** três vezes. O *token* indica que categoria de transação ou o nível de risco está atualmente selecionado, por meio de uma etiqueta ou símbolo apropriado que é exibido na tela **464**. Se o

15 usuário não apertar o botão **454** durante mais do que certo tempo pré-fixado, por 2 segundos, por exemplo, então o *token* gera um código dinâmico de aprovação pelo código da categoria da transação atualmente selecionada ou nível de risco e dá saída a este código dinâmico gerado de aprovação em sua tela **464**. Se, porém, o usuário apertar o

20 botão **454** dentro desse tempo pré-fixado, é selecionada outra categoria de transação ou nível de risco.

A **Figura 4d** ilustra ainda outra modalidade particular de um equipamento de segurança de acordo com a invenção compreendendo um *token* **405** para gerar códigos dinâmicos de aprovação. O

25 *token* **405** compreende uma interface de saída e uma de entrada. A sua interface de saída **460** pode compreender um conjunto de LEDs **467**. Pode também ou alternativamente compreender uma tela **465**. A sua interface de entrada compreende um botão **455**. O *token* **405** compreende, além disso, uma interface máquina a máquina de comunicação

30 **480** que pode, por exemplo, compreender um conector de USB e uma controladora de USB. Quando o *token* **405** é conectado a um computa-

dor hospedeiro por meio desta interface máquina a máquina de comunicação, um aplicativo no computador hospedeiro pode pedir que o *token* **405** gere um código dinâmico de aprovação para uma categoria de transação ou nível de risco proporcionado pelo computador hospedeiro. Por meio da interface de saída **460**, o *token* **405** indica ao usuário que categoria de transação ou nível de risco um código dinâmico de aprovação é solicitado. Por exemplo, o *token* pode ligar um LED específico que está associado a dada categoria de transação ou nível de risco ou pode mostrar certa etiqueta ou símbolo na tela **465**. Apertando o botão **455**, o usuário instrui o *token* **405** a gerar o código de aprovação solicitado. O *token* **405** gera, então, o código dinâmico de aprovação solicitado e comunica isto ao hospedeiro através da interface de comunicação **480**. O *token* **405** pode também compreender outro botão **456** que o usuário pode apertar para indicar que o pedido do computador hospedeiro deve ser recusado.

A **Figura 4e** ilustra mais uma modalidade particular de um equipamento de segurança de acordo com a invenção que compreende um *token* **402** para gerar códigos dinâmicos de aprovação. A sua interface de saída compreende uma tela **466**. A sua interface de entrada compreende uma roda de polegar **457**. Numa modalidade, a sua interface de entrada pode também compreender um botão **453**. Girando a roda de polegar **457**, o usuário pode circular através de uma lista de categorias de transação ou níveis de risco suportados. O *token* indica que categoria de transação ou nível de risco está atualmente selecionado por meio de uma etiqueta ou símbolo apropriado que é exibido na tela **466**. Estas etiquetas podem incluir, por exemplo, baixo, médio, alto ou *log in*, pague, pague alto. Numa modalidade, o usuário instrui o *token* a gerar um código dinâmico de aprovação para o código da categoria de transação ou nível de risco atualmente selecionado apertando a roda de polegar. Noutra modalidade o usuário aperta o botão **453** para fazê-lo. O *token* dá saída ao código dinâmico de apro-

vação gerado em sua tela **466**.

Embora várias modalidades da presente invenção tenham sido descritas acima, deve ficar entendido que elas foram apresentadas por via de exemplo apenas e não por limitação. Deste modo, o alcance e o escopo da presente invenção não devem ser limitados por nenhuma das modalidades exemplificativas acima descritas, mas, devem ser apenas definidas de acordo com as Reivindicações seguintes e seus equivalentes.

“Métodos e Equipamento de Asseguramento de Transações

Eletrônicas e de Geração de Códigos Dinâmicos

de Aprovação de Categoria de Transação”

Reivindicações

5 **1 - Método de Asseguramento de Transações Eletrônicas, caracteri-**
 zado por que compreende as etapas de: armazenar critérios para classi-
ficar transações numa pluralidade de categorias de transação; propor-
cionar meios para que pelo menos um usuário gere uma prova da
intenção do referido usuário fazer uma transação que pertence a uma
10 das citadas categorias de transação; receber pelo menos uma transação
a partir de pelo menos um usuário; aplicar ditos critérios a uma transa-
ção recebida e atribuir a referida transação recebida a uma da citada
pluralidade de categorias de transação; receber a partir de pelo menos
uma prova do usuário de dita intenção do usuário de fazer uma transa-
15 ção que pertence a uma das referidas categorias de transação; e verifi-
car se a citada prova de dita intenção do usuário é válida para a catego-
ria de transação da referida transação recebida.

2 - Método de Asseguramento de Transações Eletrônicas, de acordo
com a Reivindicação 1, **caracterizado** por que compreende, além disso,
20 gerar um valor de referência de verificação; em que a referida prova da
citada intenção do usuário compreende um código dinâmico de aprova-
ção de categoria de transação; e em que a citada verificação se dita
prova da citada intenção do usuário é válida compreende comparar o
referido código dinâmico de aprovação de categoria de transação com o
25 citado valor de referência de verificação.

3 - Método de Asseguramento de Transações Eletrônicas, de acordo
com a Reivindicação 2, **caracterizado** por que o referido meio de gerar
uma prova de intenção compreende um equipamento de segurança

adaptado para gerar um código dinâmico de aprovação de categoria de transação em que o citado equipamento de segurança que gera um código dinâmico de categoria de transação compreende combinar criptograficamente um indicador de categoria de transação, um valor dinâmico e um valor de segredo; e em que dito gerador de valor de referência de verificação compreende combinar criptograficamente um indicador de categoria de transação para a referida transação recebida, um valor dinâmico e um valor de segredo.

4 - Método de Asseguramento de Transações Eletrônicas, de acordo

com a Reivindicação 2, **caracterizado** por que compreende, além disso, associar pelo menos um de uma pluralidade de níveis de risco a cada uma das referidas categorias de transação; em que a citada prova de dita intenção do usuário compreende uma prova do referido usuário de fazer uma transação tendo um dos citados níveis de risco; em que dito meio de gerar uma prova de intenção compreende um equipamento de segurança adaptado para gerar um código dinâmico de aprovação de nível de risco em que o referido equipamento de segurança que gera um código dinâmico de nível de risco compreende combinar criptograficamente um indicador de nível de risco, um valor dinâmico e um valor de segredo; e em que o citado gerador de valor de referência de verificação compreende combinar criptograficamente um indicador de nível de risco com dita transação recebida, um valor dinâmico e um valor de segredo.

5 - Método de Geração de Códigos Dinâmicos de Aprovação de

Categoria de Transação, **caracterizado** por que compreende as etapas de: obter um indicador de categoria de transação; capturar o valor de pelo menos uma variável dinâmica; recuperar um ou mais valores secretos; aplicar um algoritmo para gerar um código dinâmico de aprovação usando o referido indicador de categoria de transação, o citado valor variável dinâmico e dito um ou mais valores secretos;

compreendendo o referido algoritmo as etapas de determinar com o citado um ou mais valores secretos recuperados uma chave criptográfica secreta, combinar criptograficamente pelo menos dito valor da variável dinâmica e a referida chave criptográfica secreta e transformar o resultado da citada combinação criptográfica num código dinâmico de aprovação.

6 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 5, **caracterização** por que a referida determinação de uma chave criptográfica secreta compreende selecionar uma chave criptográfica secreta fora dos citados valores secretos com base no valor do indicador da categoria de dita transação.

7 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 5, **caracterização** por que a referida recuperação de um ou mais valores secretos compreende recuperar o valor de um segredo-mestre e em que a citada determinação de uma chave criptográfica secreta compreende derivar uma chave criptográfica secreta a partir de dito valor da referida chave mestra usando o valor do citado indicador da categoria da transação.

8 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 5, **caracterização** por que o referido indicador de categoria de transação compreende um indicador de nível de risco.

9 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 5, **caracterização** por que a referida variável dinâmica é relacionada com o tempo.

10 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 9, **caracteri-**

zação por que o referido valor de variável dinâmica compreende o valor de um relógio de tempo real.

11 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 5, **caracteri-**

5 **zação** por que o referido valor de variável dinâmica compreende o valor de um contador.

12 - Método de Geração de Códigos Dinâmicos de Aprovação de Categoria de Transação, de acordo com a Reivindicação 5, **caracteri-**

10 **zação** por que a referida combinação criptográfica do citado valor variável dinâmico e dita chave secreta criptográfica compreende gerar um criptograma usando uma combinação matemática do referido valor de variável dinâmica e o citado indicador de categoria de transação e usando um algoritmo criptográfico que é parametrizado com dita chave secreta criptográfica.

15 **13 - Equipamento de Asseguramento de Transações Eletrônicas**, adaptado para gerar códigos dinâmicos de aprovação, **caracterizado** por que compreende uma armazenagem de chave secreta para armazenar um ou mais valores secretos, uma fonte de variabilidade para proporcionar um valor de variável dinâmica, uma interface de entrada
20 adaptada para ativar a seleção de um valor de um indicador de categoria de transação ou indicador de nível de risco a partir de um conjunto limitado de categorias de transação ou valores de indicador de nível de risco suportado, um agente criptográfico adaptado para combinar criptograficamente uma chave secreta com o referido valor de variável
25 dinâmica e a citada categoria de transação ou valores de indicador de nível de risco, um agente de transformação para transformar o resultado da dita combinação criptográfica num código dinâmico de aprovação e uma interface de saída para dar saída ao referido código dinâmico de aprovação.

14 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 13, **caracterizado** por que a referida fonte de variabilidade compreende um relógio de tempo real.

15 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 13, **caracterizado** por que a referida fonte de variabilidade compreende um contador.

16 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 13, **caracterizado** por que a referida interface de entrada compreende uma interface máquina a máquina e por que a citada seleção de um valor de um indicador de categoria de transação ou indicador de nível de risco compreende o processamento de dados recebidos através da citada interface de máquina a máquina.

17 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 13, **caracterizado** por que a referida interface de entrada compreende um dispositivo de interface humana e por que a citada seleção de um valor de um indicador de categoria de transação ou indicador de nível de risco compreende a interação do usuário com dito dispositivo de interface humana.

18 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 17, **caracterizado** por que o referido dispositivo de interface humana compreende um ou mais botões e por que a citada interação do usuário com dito dispositivo de interface humana compreende usar pelo menos um dos referidos botões.

19 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 17, **caracterizado** por que o referido dispositivo de interface humana compreende uma roda de polegar e por que a citada interação do usuário com dito dispositivo de interface humana compreende o uso da referida roda de polegar.

20 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 13, **caracterizado** por que compreende um primeiro dispositivo energizado por uma fonte de energia contida no primeiro dispositivo e incluindo a referida interface de entrada e interface de saída e incluindo um segundo dispositivo a citada armazenagem de chave secreta; incluindo, além disso, dito segundo dispositivo dispositivos de entrada e de saída para receber e remeter sinais a partir de e para o referido primeiro dispositivo, incluindo, além disso, o citado primeiro dispositivo dispositivos de entrada e de saída para receber e remeter sinais para dito segundo dispositivo.

21 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido primeiro dispositivo compreende pelo menos uma parte do citado agente de transformação.

22 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido primeiro dispositivo compreende pelo menos uma parte do citado agente criptográfico.

23 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido primeiro dispositivo compreende pelo menos uma parte da citada fonte de variabilidade.

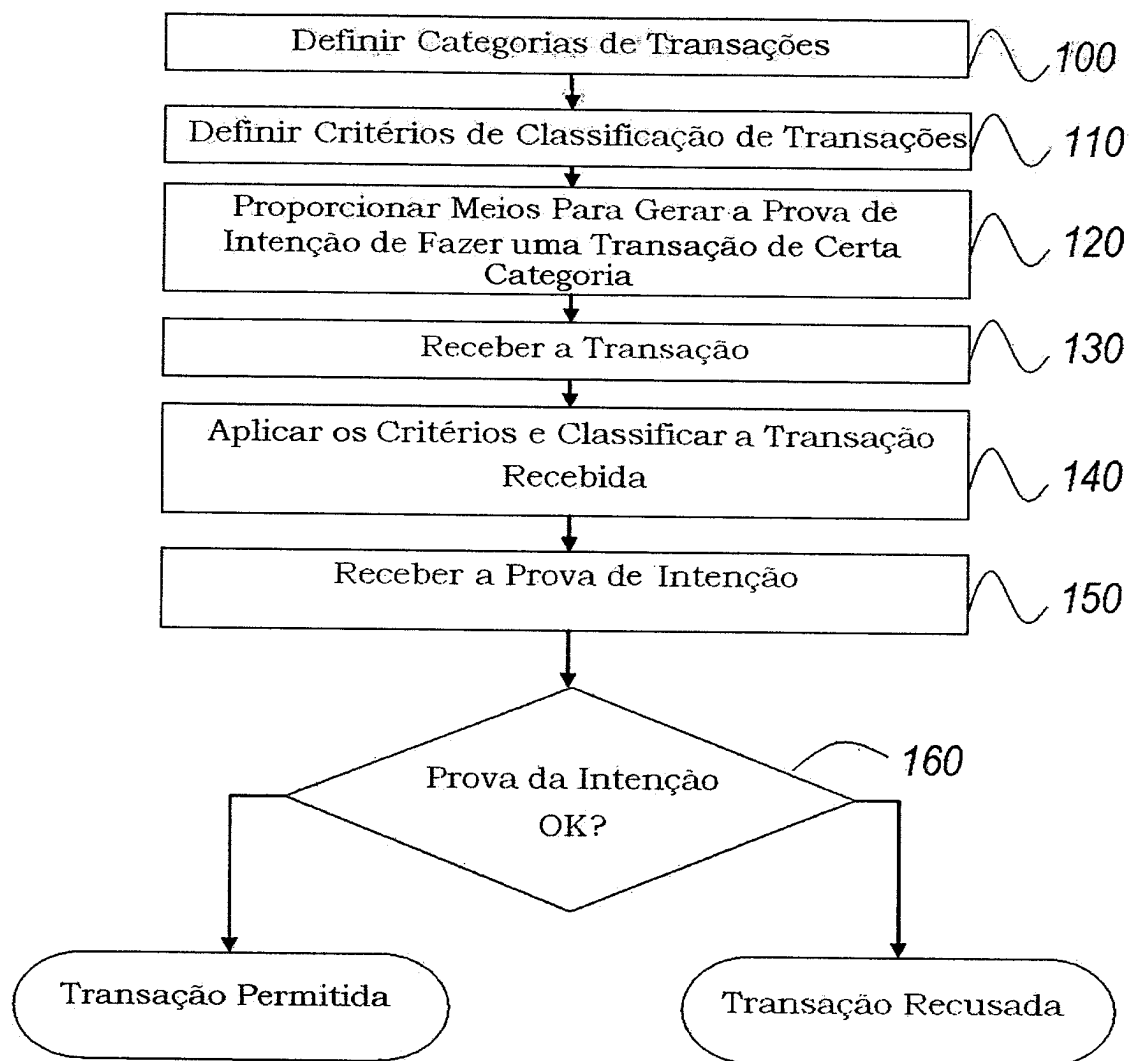
24 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido segundo dispositivo compreende pelo menos uma parte do citado agente de transformação.

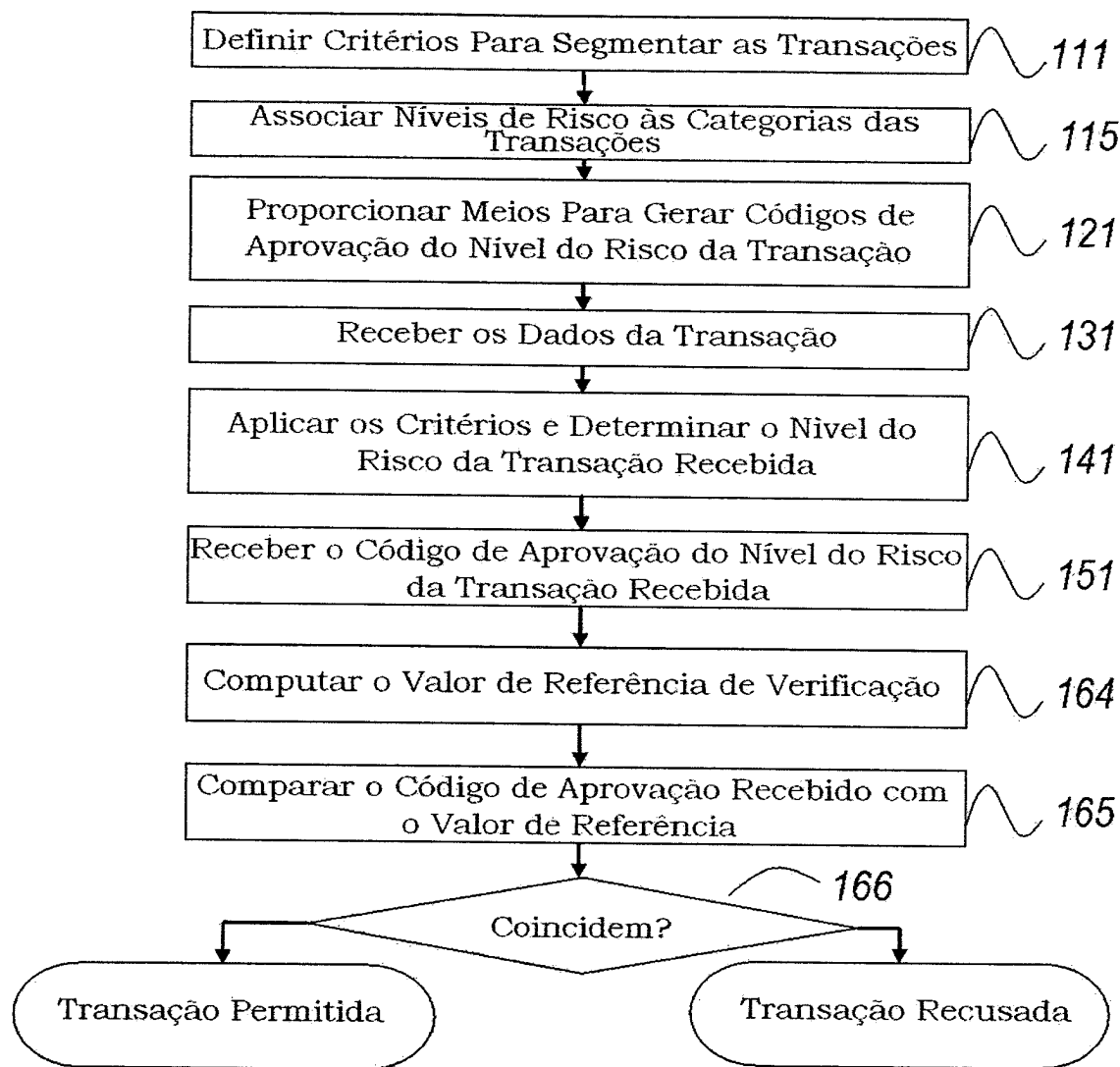
25 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido se-

gundo dispositivo compreende pelo menos uma parte do citado agente criptográfico.

26 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido segundo dispositivo compreende pelo menos uma parte da citada fonte de variabilidade.

27 - Equipamento de Asseguramento de Transações Eletrônicas, de acordo com a Reivindicação 20, **caracterizado** por que o referido segundo dispositivo compreende um cartão inteligente e os dispositivos de entrada e de saída do citado primeiro dispositivo compreendem uma interface de cartão inteligente.

**Figura 1A**

**Figura 1B**

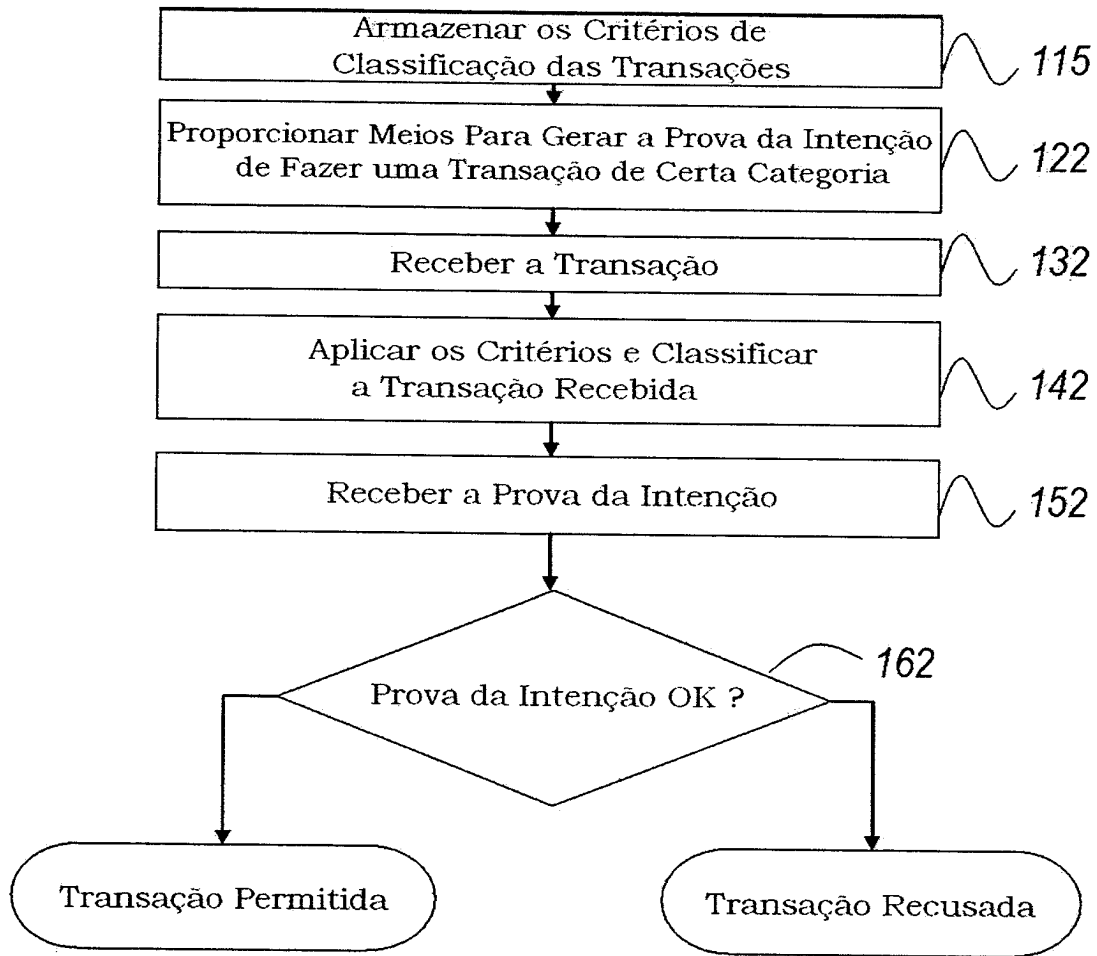
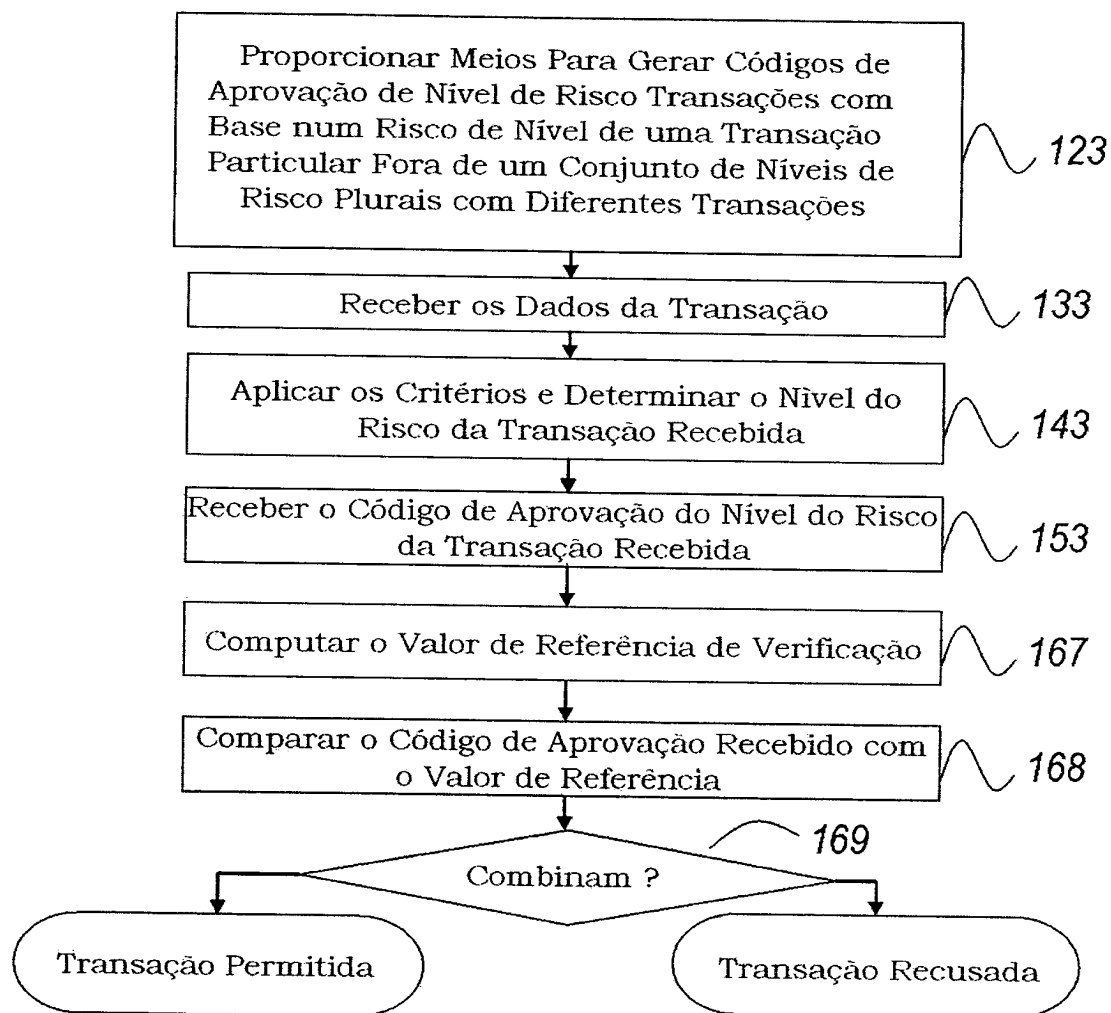
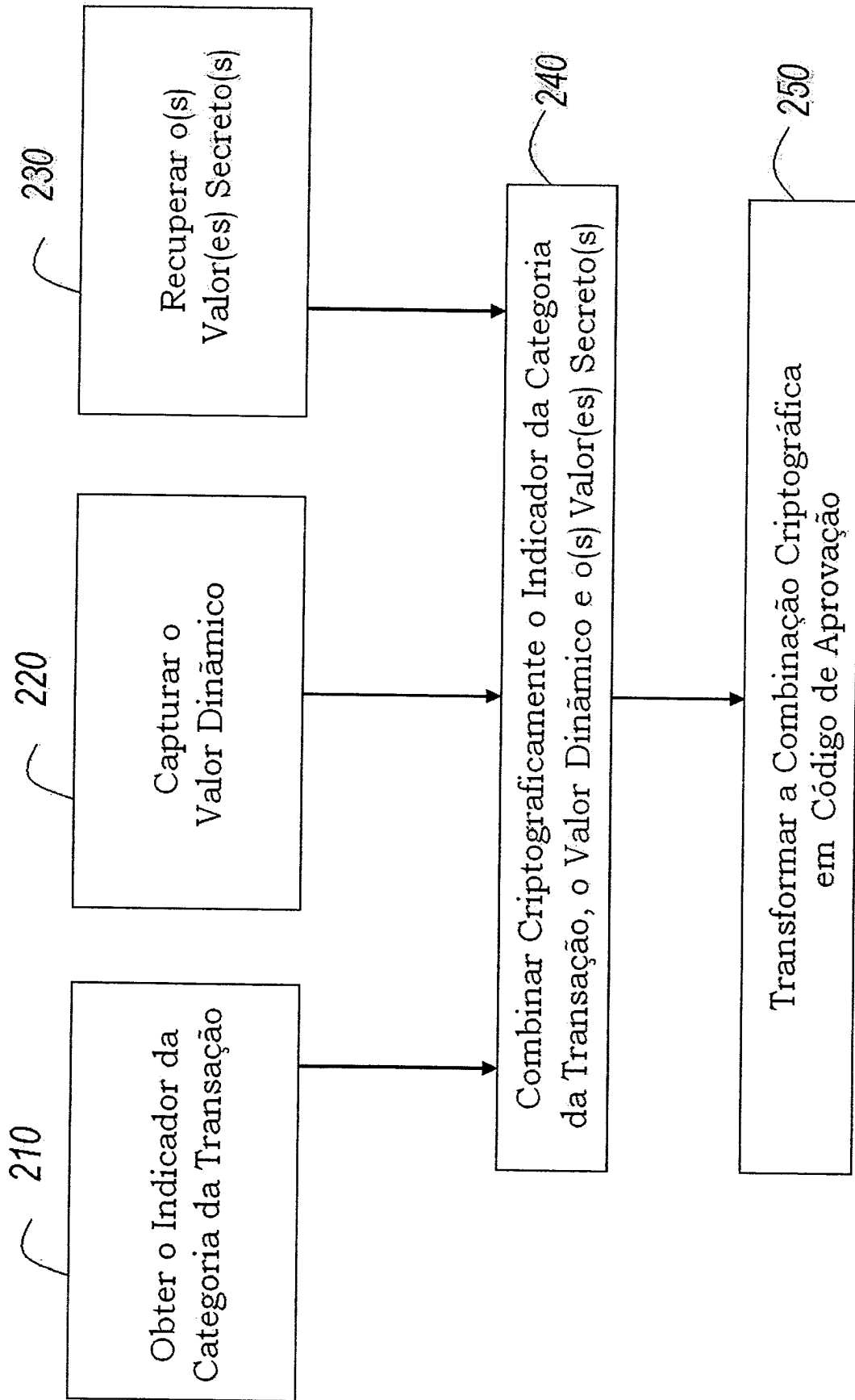
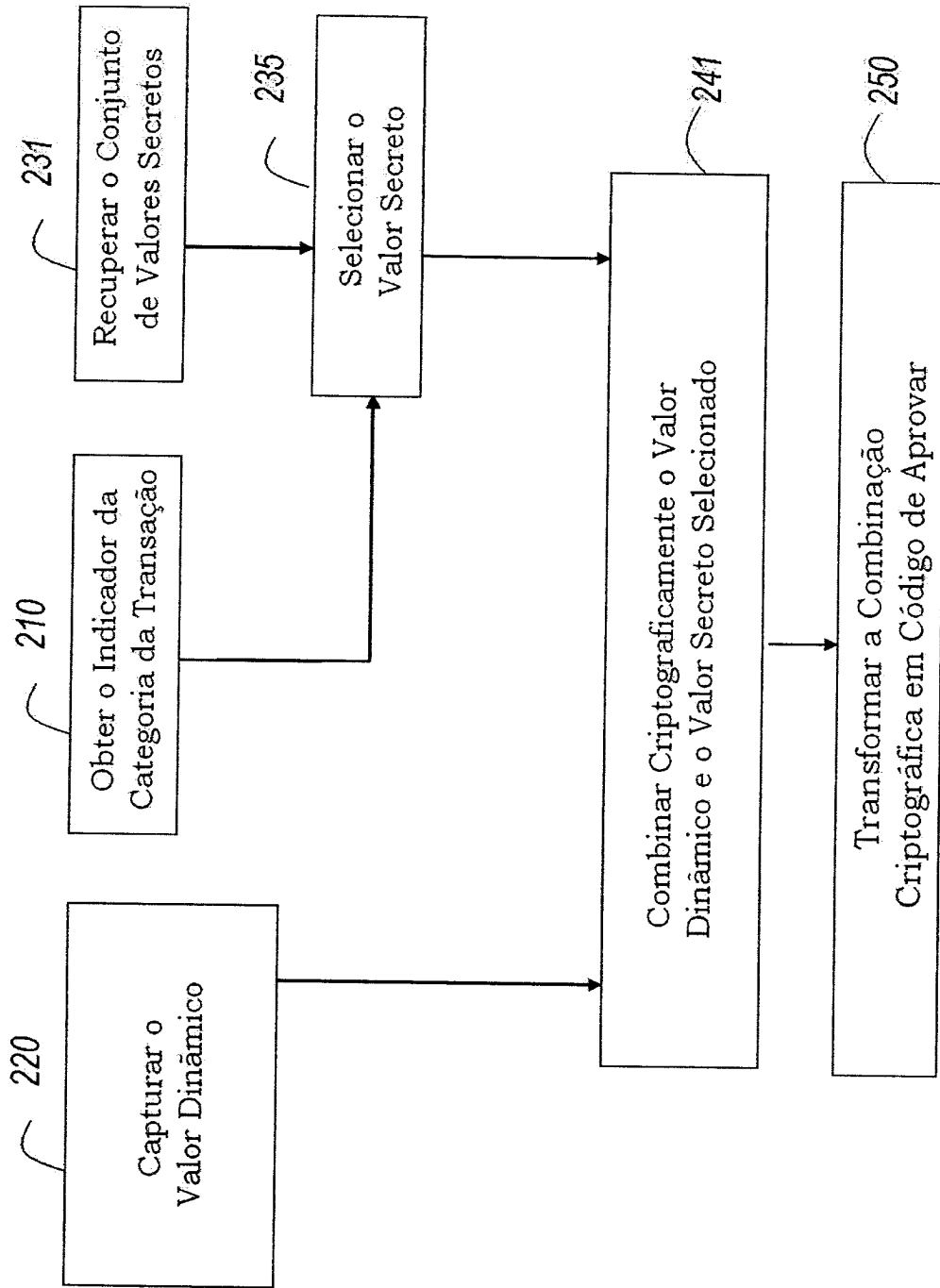


Figura 1C

**Figura 1D**

**Figura 2A**

**Figura 2B**

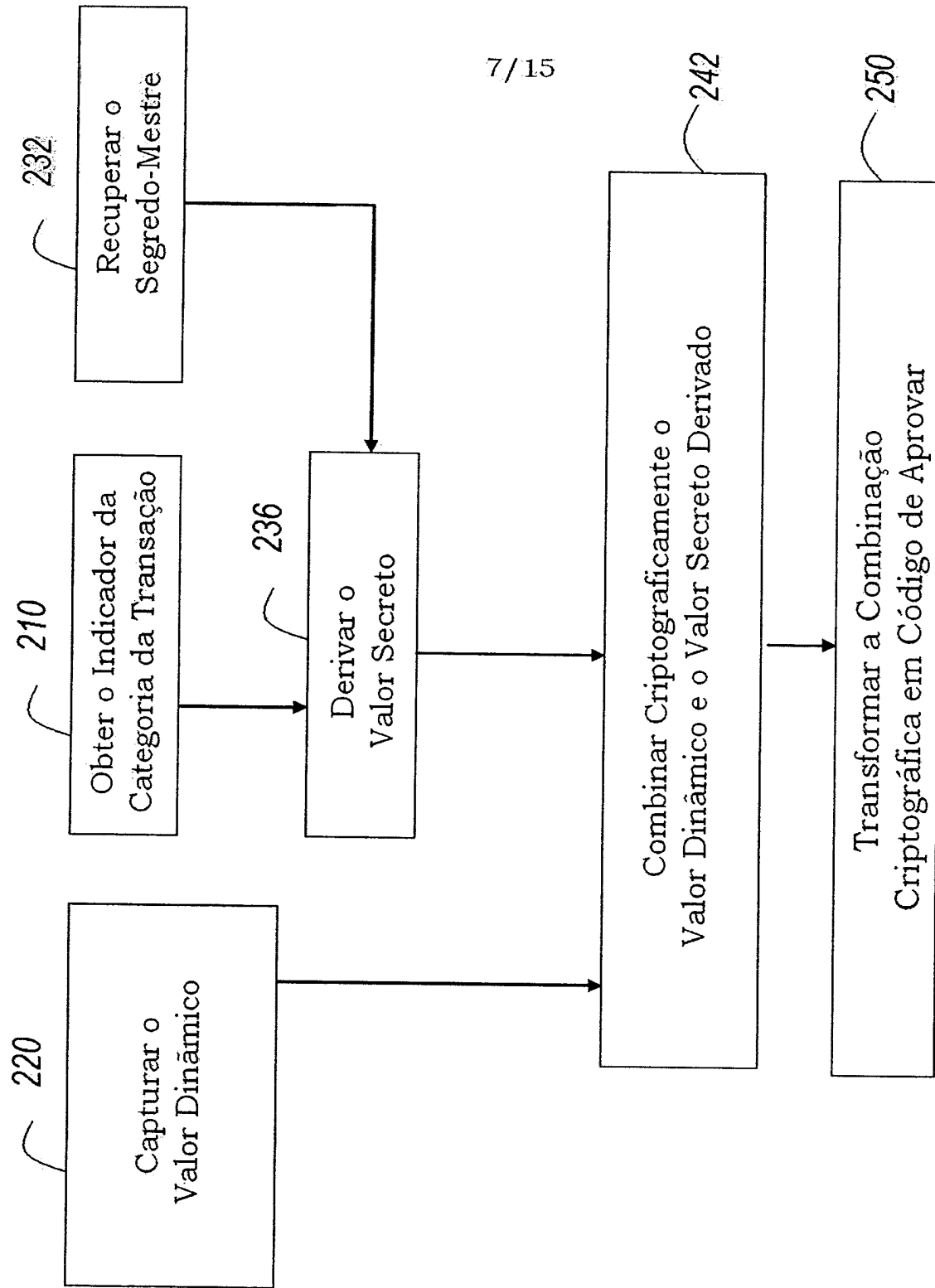
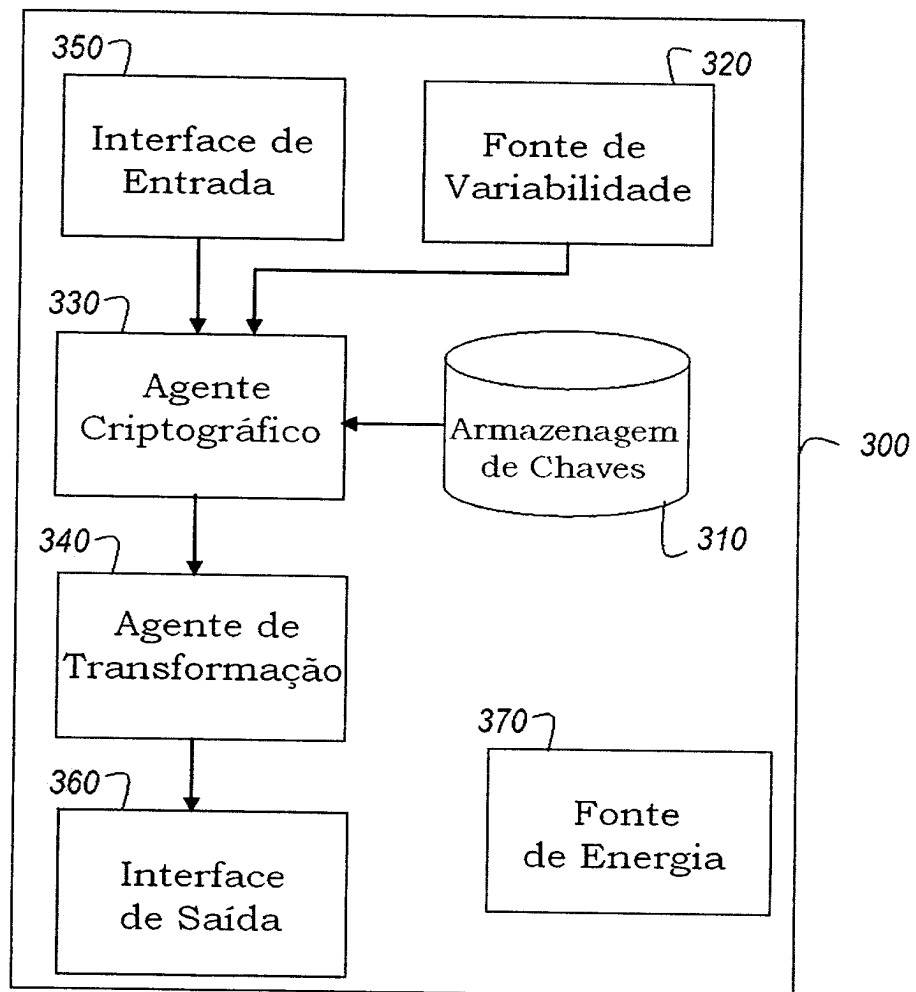
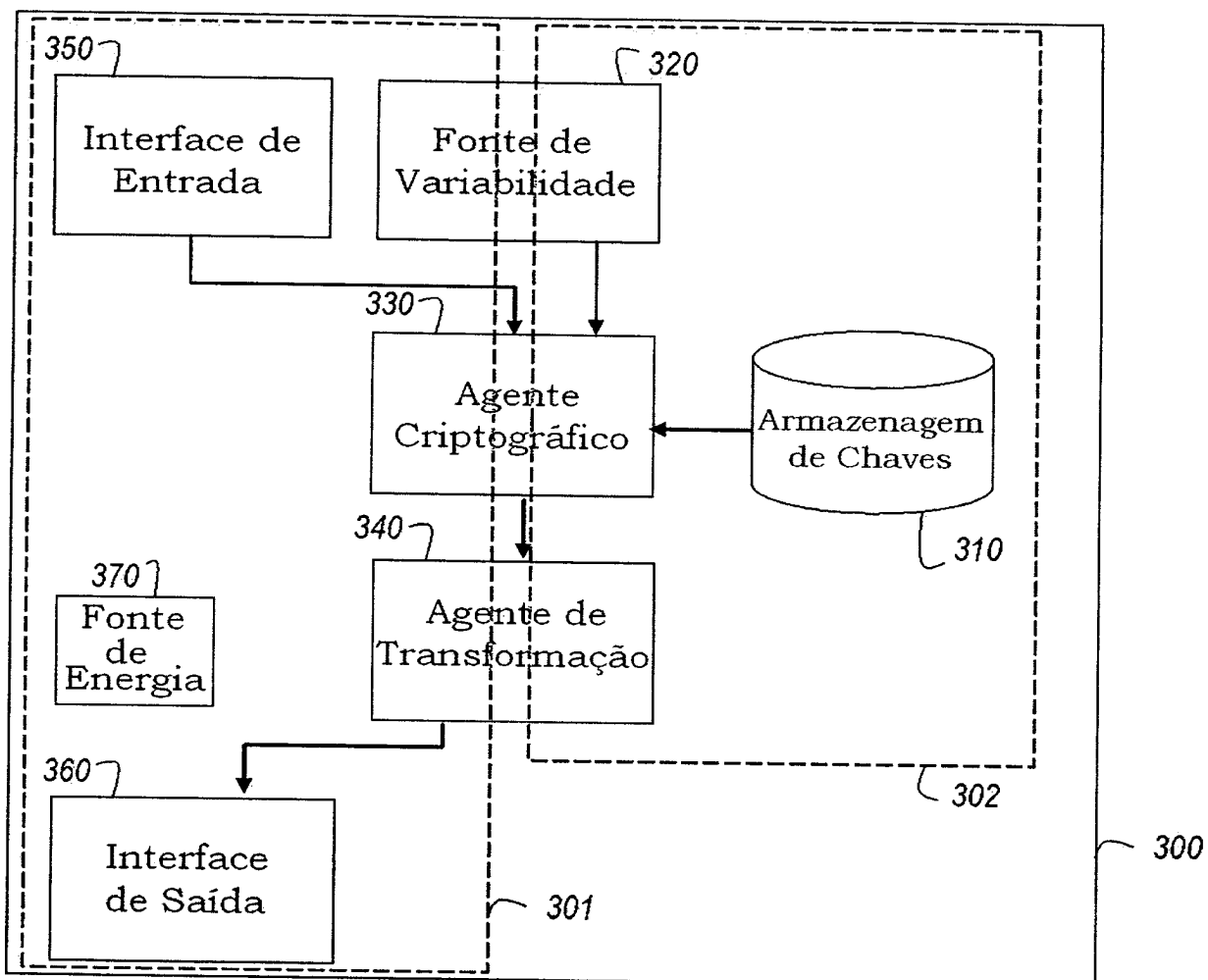


Figura 2C

**Figura 3A**

**Figura 3B**

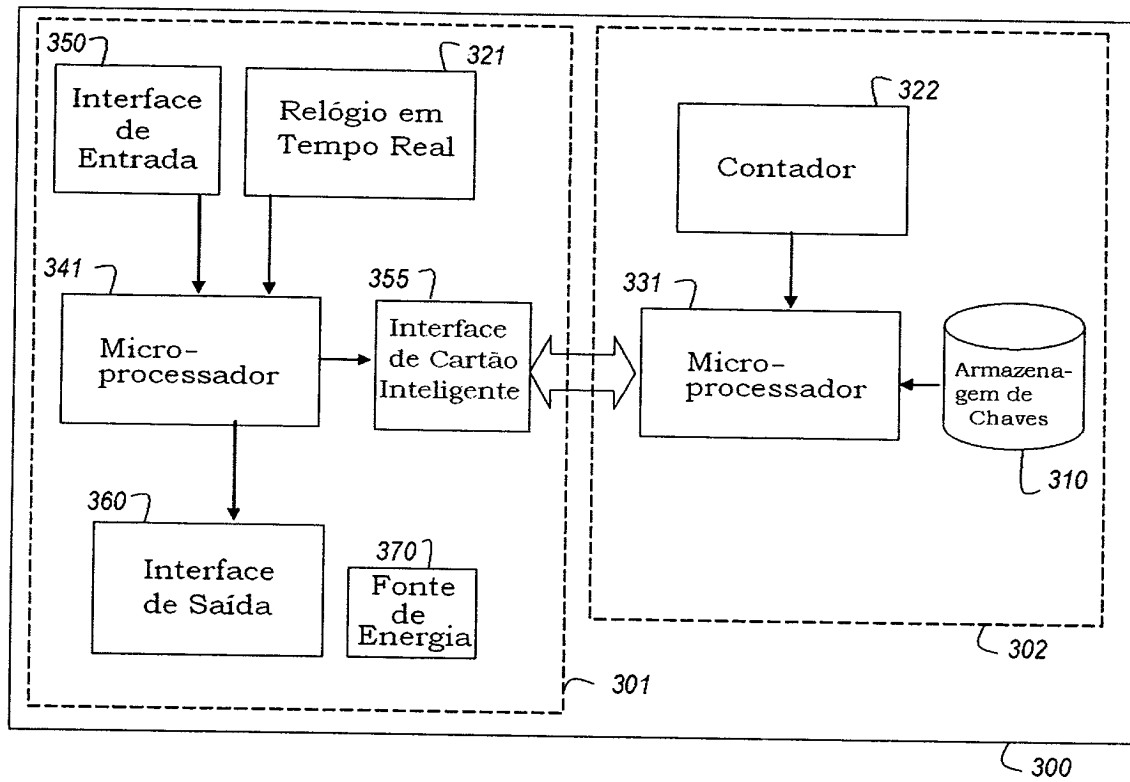


Figura 3C

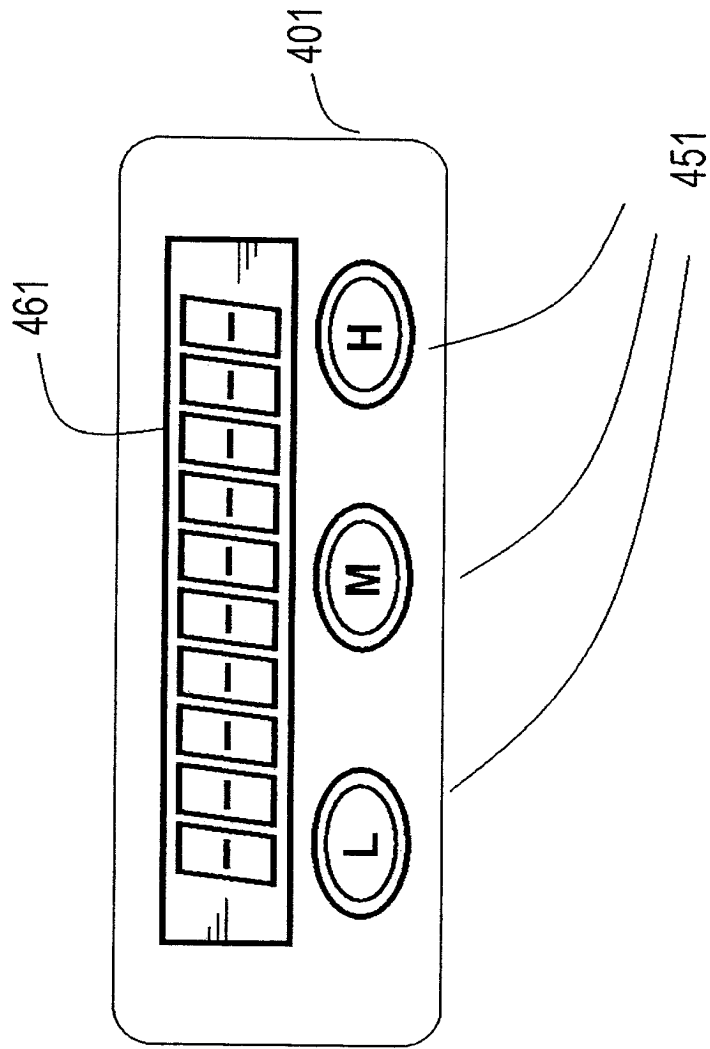


Figure 4A

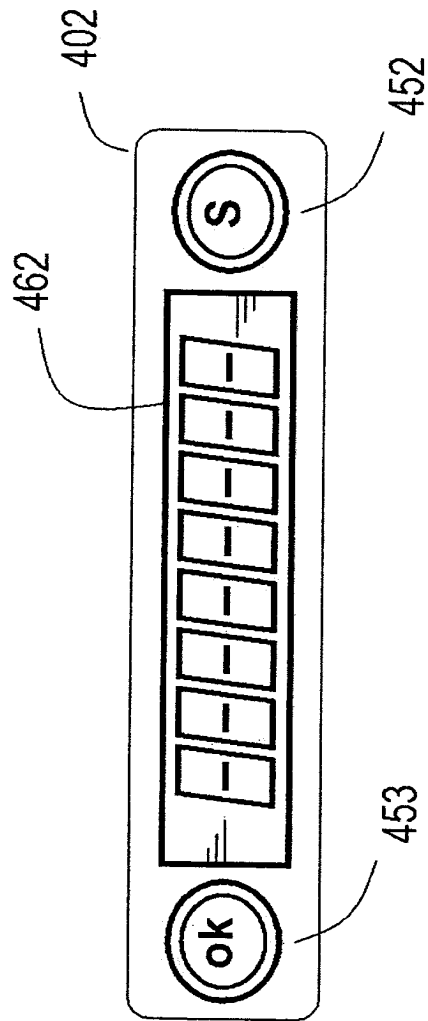


Figura 4B

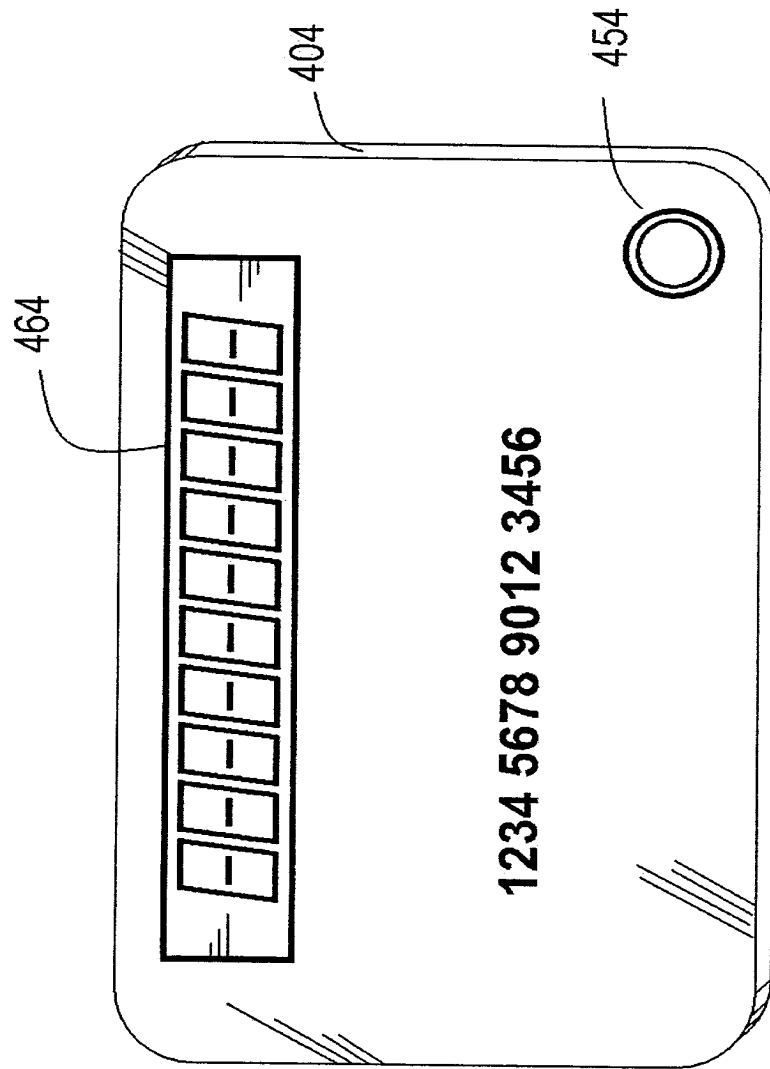


Figure 4C

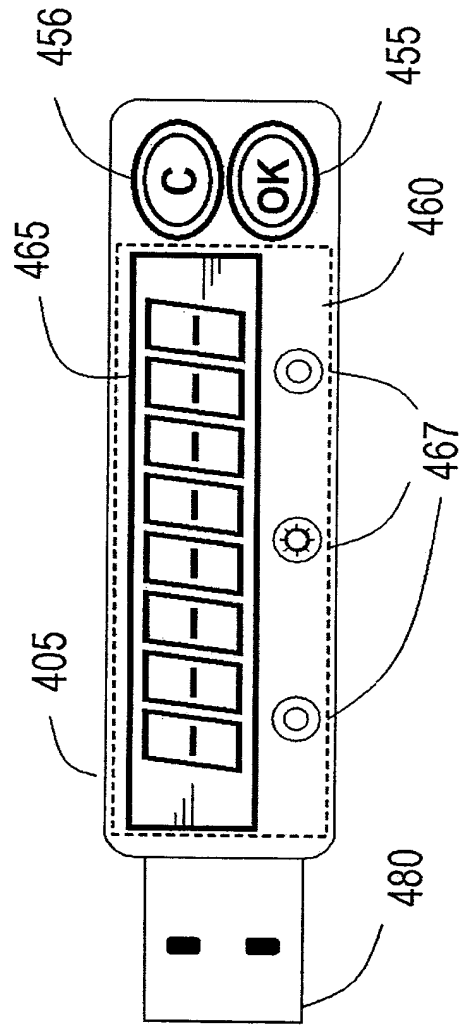


Figure 4D

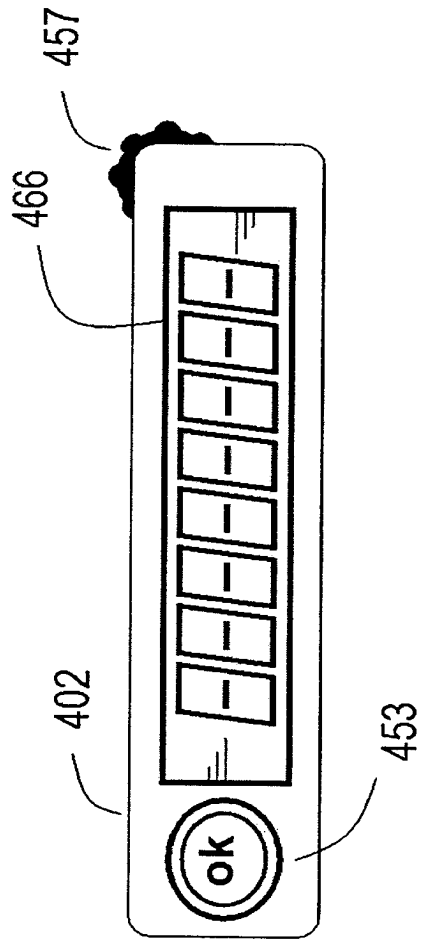


Figura 4E

“Métodos e Equipamento de Asseguramento de Transações

Eletrônicas e de Geração de Códigos Dinâmicos

de Aprovação de Categoria de Transação”

Resumo

5 A presente invenção relaciona-se com o campo de assegurar transações eletrônicas e, mais especificamente, com métodos para indicar e verificar a aprovação do nível de risco de uma transação e com equipamentos para gerar códigos de aprovação do nível de risco de transações. Num método de acordo com a invenção, as transações são

10 classificados num número limitado de categorias. Um usuário que submete uma transação a um servidor é solicitado também a gerar e submeter um código dinâmico de aprovação de categoria de transação para a transação submetida. Do lado do servidor é gerado um valor de verificação correspondente para a transação recebida. Num método

15 alternativo de acordo com a invenção, às transações são atribuídos um dentre um número limitado de níveis de risco. Um usuário que submete uma transação a um servidor é solicitado também a gerar e submeter um código dinâmico de aprovação de nível de risco para a transação submetida. No lado do servidor, um valor de verificação correspondente

20 é gerado para a transação recebida. O código dinâmico de aprovação de nível de risco recebido é verificado no lado do servidor comparando-o com o valor de verificação gerado. Também são descritos um *token* de segurança para assegurar transações eletrônicas adaptadas para gerar códigos dinâmicos de aprovação de categoria de transação e um *token*

25 de segurança para assegurar transações eletrônicas adaptado para gerar códigos dinâmicos de aprovação de nível de risco.