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

(21) **PI0616470-6 A2**

BRPI0616470A2

(22) Data de Depósito: 28/09/2006
(43) Data da Publicação: 21/06/2011
(RPI 2111)

(51) Int.Cl.:
G06Q 99/00 2006.01

(54) Título: **LEITOR, CARTÃO, APARELHO, E, APARELHO LEITOR PARA REDUZIR UM TEMPO DE INTERAÇÃO PARA UMA TRANSAÇÃO SEM CONTATO, E PARA EVITAR UM ATAQUE DE INTERMEDIÁRIOS NA TRANSAÇÃO SEM CONTATO**

(30) Prioridade Unionista: 28/09/2005 US 60/721454, 19/07/2006 US 60/807775, 19/07/2006 US 60/807775, 28/09/2005 US 60/721454

(73) Titular(es): VISA INTERNATIONAL SERVICE ASSOCIATION

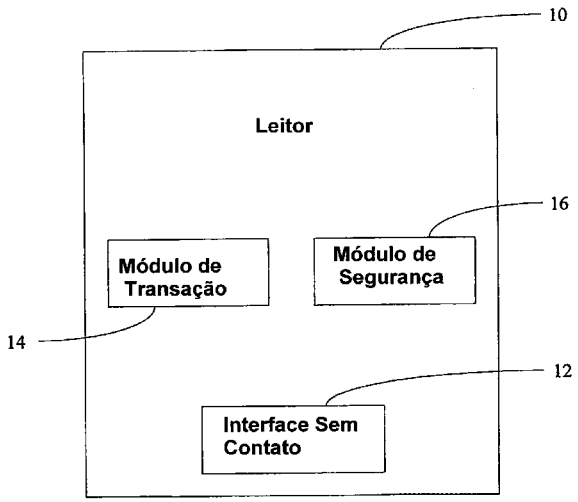
(72) Inventor(es): ANITA OCHIEANO, CAROLE OPPENLANDER, CHRISTIAN AABYE, CRAIG ALLEN GLENDENNING , JAGDEEP SINGH SAHOTA, KIM WAGNER, TRUDY HILL, WILLIAM CHI YUEN CHAN

(74) Procurador(es): Momsen, Leonardos & CIA.

(86) Pedido Internacional: PCT US2006038047 de 28/09/2006

(87) Publicação Internacional: WO 2007/038743de 05/04/2007

(57) Resumo: MÉTODO PARA AUMENTAR RESOLUÇÃO DE COR, E, ISPOSITIVO. A invenção relaciona-se a um método para aumentar resolução de cor e particularmente para obter resolução de 18 bits em um mostrador usando uma memória temporária de quadro de sistema de 16 bits por pixel. A invenção usa lógica para criar valores de pixel intermediários entre valores de cor de 16 bpp. A invenção propõe armazenar a imagem no memória temporária de quadro de sistema sempre com um número fixo de bits e usando Tremor de Difusão de Erro. Então, um filtro de pós-processamento é provido para prover a resolução de cor aumentada usando um maior número de bits por pixel como aceito pelo meio de exibição. A invenção também relaciona-se a um dispositivo explorando o método.



"LEITOR, CARTÃO, APARELHO, E, APARELHO LEITOR PARA REDUZIR UM TEMPO DE INTERAÇÃO PARA UMA TRANSAÇÃO SEM CONTATO, E PARA EVITAR UM ATAQUE DE INTERMEDIÁRIOS NA TRANSAÇÃO SEM CONTATO"

REFERÊNCIA CRUZADA PARA PEDIDOS RELACIONADOS

Este pedido reivindica o benefício da prioridade do Pedido de Patente dos Estados Unidos Provisório No. 60/721.454, depositado em 28 de Setembro de 2005, e Pedido de Patente dos Estados Unidos Provisório No. 60/807.775, depositado em 19 de Julho de 2006.

C. DECLARAÇÃO RELATIVA A ACORDOS DE PESQUISA DE PATROCÍNIO FEDERAL - NÃO APLICÁVEL

D. PARTES A JUNTAR AO ACORDO DE PESQUISA - NÃO APLICÁVEL

E. INCORPORAÇÃO DE MATERIAL SUBMETIDO EM CD - NÃO APLICÁVEL

F. FUNDAMENTOS

Este pedido descreve uma invenção que é relacionada, geralmente e em várias realizações, a um dispositivo, sistema e método para reduzir um tempo de interação para uma transação sem contato.

Tecnologias de comunicação sem contato e sem fio tem se tornado mais difundidas em anos recentes. Na industria de pagamento, pagamento sem contato tem um número de vantagens sobre ambas tecnologias de tira magnética tradicional e protocolos de pagamento baseados em contato de chip. Por exemplo, cartões de pagamento tradicionais são conhecidos por operar relativamente lentos, e cartões de tira magnética são conhecidos por não serem suficientemente seguros. Cada uma destas tecnologias requer adicionalmente um encaixe em um leitor de terminal que precisa ser mantido por um comerciante.

Pagamento sem contato não requer uma fenda de encaixe na qual inserir o cartão. O consumidor mantém controle sobre o cartão e meramente posiciona o cartão próximo ao leitor do terminal todas as vezes que for necessário. As especificações tradicionais adotadas pela industria de pagamento para pagamento com chip baseado em contato, geralmente requerem que o consumidor posicione o cartão próximo ao leitor de terminal por diferentes vezes e/ou por períodos estendidos de tempo, no sentido de completar uma transação. Com ambos comerciantes e consumidores desejando tempos de transação rápidos, transações sem contato executadas de acordo com especificações tradicionais deixam de satisfazer às exigências do mercado.

Comerciantes e consumidores estão também demandando que as transações sem contato sejam mais seguras. Embora cartões baseados em tira magnética sem contato emitidos mais recentemente possam ser mais seguros que cartões de tira magnética, tais cartões baseados em tira magnética sem contato são tipicamente projetados somente para transações em linha. Para transações sem contato fora de linha executadas de acordo com as especificações tradicionais, as transações podem ser susceptíveis a várias intromissões fora de linha, tipos de ataques geralmente referidos como ataques *de capa* (*"sleeve"*), ataques de *cavalo de Tróia*, etc.

Em um tipo de ataque *de capa*, um dispositivo intercepta dados transmitidos sem fio a partir de um leitor de cartão que é destinado a um cartão sem contato. O dispositivo altera os dados e subseqüentemente transmite os dados alterados ao cartão. Ao invés de receber os dados transmitidos pelo leitor de cartão, o cartão recebe os dados alterados transmitidos pelo dispositivo. O cartão subseqüentemente processa os dados alterados e transmite uma mensagem relacionada aos dados alterados ao leitor de cartão. O leitor de cartão subseqüentemente concede aprovação da transação, com base na informação presente na mensagem transmitida pelo

cartão. Em um outro tipo de ataque *de capa*, um dispositivo intercepta dados transmitidos sem fio a partir do cartão que são destinados ao leitor de cartão. O dispositivo altera os dados e subseqüentemente transmite os dados alterados ao leitor de cartão. O dispositivo altera os dados e subseqüentemente transmite os dados alterados ao leitor de cartão. Ao invés de receber os dados transmitidos pelo cartão, o leitor de cartão processa os dados alterados e concede a aprovação da transação com base na informação presente nos dados alterados transmitidos pelo dispositivo. Em outros tipos de ataques *de capa* o dispositivo pode causar uma negativa de serviço, não enviando os dados interceptados ao cartão ou leitor de cartão.

Em um tipo de ataque de *cavalo de Tróia*, software malicioso embutido no cartão altera dados válidos antes da informação ser enviada ao leitor de cartão. O leitor de cartão definitivamente concede aprovação para a transação, com base nos dados alterados. Em um outro tipo de ataque de *cavalo de Tróia*, software malicioso embutido no leitor de cartão altera dados válidos antes do processo de autorização. O leitor de cartão definitivamente concede aprovação para a transação, com base nos dados alterados.

Para uma dada transação fora de linha, um ataque de intromissão ("*man in the middle*") pode ser utilizado para reduzir a quantia da transação como reconhecido definitivamente pelo cartão e pelo leitor de cartão. Por exemplo, para uma dada transação fora de linha envolvendo a aquisição de bens de um comerciante, o leitor de cartão pode transmitir dados sem fio destinados ao cartão, o que indica que o valor da transação é igual a $15. Entretanto, antes dos dados serem recebidos pelo cartão, o dispositivo intercepta os dados e altera os dados de tal modo que os dados alterados indicam que o valor da transação é somente igual a $1. Uma vez que o cartão subseqüentemente recebe os dados alterados e transmite a mensagem relacionada aos dados alterados ao leitor de cartão, o leitor de cartão subseqüentemente concede aprovação de uma transação igual a somente $1.

Ao receber a aprovação, o comerciante libera as mercadorias acreditando que a quantia da transação aprovada foi igual a $15. A diferença entre a quantia da transação real e a quantia da transação reduzida pode afetar a quantia definitivamente recebida pelo comerciante a partir de um emissor do cartão.

G. BREVE SUMÁRIO DA INVENÇÃO

Em um aspecto geral, esta aplicação descreve um leitor. De acordo com várias realizações, o leitor compreende uma interface sem contato e um módulo de transação. O módulo de transação é acoplado à interface sem contato, e é estruturado e arranjado para processar uma transação com menos de meio segundo de tempo de interação entre um cartão e o leitor.

Em um outro aspecto geral, este pedido descreve um cartão. De acordo com várias realizações, o cartão compreende um módulo de transação estruturado e arranjado para comunicação sem fio, e o cartão é estruturado e arranjado para operar em um modo de chip e um modo de dados de tira magnética.

Em um outro aspecto geral, este pedido descreve um sistema. De acordo com várias realizações, o sistema compreende um leitor e um cartão. O leitor compreende uma interface sem contato e um módulo de transação. O cartão é estruturado e arranjado para se comunicar com o leitor, via interface sem contato. O módulo de transação é acoplado à interface sem contato. O módulo de transação é acoplado à interface sem contato e é estruturado e arranjado para processar uma transação sem contato com menos de meio segundo de tempo de interação entre o cartão e o leitor.

Em um outro aspecto geral, este pedido descreve um método para reduzir um tempo de interação para uma transação sem contato. De acordo com várias realizações, o método compreende, em um leitor, executar pelo menos um processo de gerenciamento de risco baseado na transação, antes de energizar uma interface sem contato, iniciar comunicação com um cartão utilizado para a transação sem contato, receber informação associada

ao cartão e terminar a comunicação com o cartão antes de autorizar a transação sem contato.

Em um outro aspecto geral, o pedido descreve um método para evitar um ataque de intromissão em uma transação sem contato. De acordo com várias realizações, o método compreende receber uma assinatura dinâmica que compreende um contador de transação de aplicação, um número imprevisível de terminal, uma quantia de transação, um código de moeda corrente de transação e um número de cartão imprevisível. O método compreende também receber um número de cartão imprevisível, recalcular a assinatura dinâmica usando o número de cartão imprevisível e memorizar a transação sem contato fora de linha se a assinatura dinâmica é validada.

Aspectos da invenção podem ser implementados por um dispositivo de computação e/ou um programa de computador armazenado em um meio legível por computador. O meio legível por computador pode compreender um disco, um dispositivo e/ou um sinal propagado.

H. DESCRIÇÃO DOS DESENHOS

Várias realizações da invenção são descritas aqui por meio de exemplo, em conjunto com as figuras a seguir.

Figura 1 ilustra várias realizações de um leitor para reduzir um tempo de interação para uma transação sem contato;

Figura 2 ilustra várias realizações de um sistema para reduzir um tempo de interação para uma transação sem contato;

Figura 3 ilustra várias realizações de um método para reduzir um tempo de interação para uma transação sem contato;

Figura 4 é um fluxograma simplificado ilustrando várias realizações de uma etapa de processamento de transação preliminar do método da Figura 3;

Figura 5 é um fluxograma simplificado ilustrando várias realizações de uma etapa de seleção de aplicação do método da Figura 3;

Figura 6 é um fluxograma simplificado ilustrando várias realizações de uma etapa de autorização do método da Figura 3; e

Figura 7 ilustra várias realizações de um método para reduzir um tempo de interação para uma segunda transação sem contato.

I. DESCRIÇÃO DETALHADA DA INVENÇÃO

Deve ser entendido que pelo menos algumas das figuras e descrições da invenção foram simplificadas para focar em elementos que são relevantes para um entendimento claro da invenção, enquanto elimina, para fins de clareza, outros elementos que aqueles especialistas na técnica verificarão que podem também constituir uma porção da invenção. Portanto, como tais elementos são bem conhecidos na técnica, e como não facilitam necessariamente um melhor entendimento da invenção, uma descrição de tais elementos não é provida aqui.

Figura 1 ilustra várias realizações de um leitor 10 para reduzir um tempo de interação para uma transação sem contato. O leitor 10 pode ser qualquer tipo de dispositivo que está estruturado e arranjado para se comunicar com um outro dispositivo, via uma interface sem contato. De acordo com várias realizações, o leitor 10 pode ser um dispositivo do comerciante que está integrado a um dispositivo de ponto de venda, ou um dispositivo de comerciante que é separado, porém está em comunicação com um dispositivo de ponto de venda. Conforme usado aqui, a frase "tempo de interação" refere-se ao tempo de interação entre o leitor 10 e um outro dispositivo, e não inclui o tempo requerido para entrar em linha para autorização ou para o leitor validar uma assinatura estática ou dinâmica para autenticação de dados fora de linha. O leitor 10 pode ser utilizado com infraestrutura de sistema de pagamento existente para mercados que requerem tempos de transação mais rápidos que aqueles associados a protocolos de pagamentos tradicionais. De acordo com várias realizações, o leitor 10 pode ser utilizado para reduzir o tempo de interação a menos de aproximadamente

500 milissegundos.

O leitor 10 compreende uma interface sem contato 12 e um módulo de transação 14, acoplados à interface sem contato. O módulo de transação 14 é estruturado e arranjado para processar uma transação sem contato com menos da metade de um segundo de tempo de interação entre o leitor 10 e um outro dispositivo. O módulo de transação 14 pode também ser estruturado e arranjado para efetuar autenticação de dados estática e/ou autenticação de dados dinâmica conforme descrito em mais detalhe abaixo. De acordo com várias realizações, o leitor 10 compreende adicionalmente um módulo de segurança 16 acoplado ao módulo de transação 14. O módulo de segurança 16 é estruturado e arranjado para evitar um ataque de intromissão em uma transação sem contato.

Cada um dos módulos 14, 16 pode ser implementado em hardware ou em firmware. De acordo com várias realizações, os módulos 14, 16 podem ser implementados como aplicações de software, programas de computador, etc., utilizando qualquer linguagem de computador adequada (por exemplo, C, C++, Delphi, Java, JavaScript, Perl, Visual Basic, VBScript, etc.) e pode ser realizado permanentemente ou temporariamente em qualquer tipo de máquina, componente, equipamento físico ou virtual, meio de armazenagem ou sinal propagado capaz de fornecer instruções a um dispositivo. O código de software pode ser armazenado com uma série de instruções ou comandos em um meio legível por computador, de tal modo que quando um processador lê o meio, as funções aqui descritas são executadas. Conforme usado aqui, o termo "meio legível por computador" pode incluir, por exemplo, dispositivos de memória magnéticos e ópticos tais como disquetes, discos compactos de ambas variedades de somente leitura ou escrevíveis, controladores de disco óptico e controladores de disco rígido. Um meio legível por computador pode também incluir armazenagem de memória que pode ser física, virtual, permanente, temporária, semi permanente e/ou

semi temporária. Um meio legível por computador pode incluir adicionalmente um ou mais sinais propagados, e tais sinais propagados podem ou não ser transmitidos em uma ou mais ondas de portadora. Embora os módulos 14, 16 sejam mostrados na Figura 1 como dois módulos separados, um especialista na técnica verificará que a funcionalidade dos módulos 14, 16 pode ser combinada em um único modo.

Figura 2 ilustra várias realizações de um sistema 20 para reduzir um tempo de interação para uma transação sem contato. Conforme usado aqui, o termo "cartão" refere-se a qualquer tipo de dispositivo que pode se comunicar com o leitor 10 através da interface sem contato 12. De acordo com várias realizações, o cartão 22 pode ser um cartão inteligente, um telefone móvel, um assistente digital pessoal, etc. O cartão 22 é estruturado e arranjado para se comunicar com o leitor 10 via interface sem contato 12. De acordo com várias realizações, o cartão 22 compreende um módulo de transação 24 estruturado e arranjado para cooperar com o leitor 10 para executar a transação sem contato. O cartão 22 pode compreender adicionalmente um módulo de segurança 26 estruturado e arranjado para cooperar com o leitor 10 para evitar um "ataque de intromissão" na transação sem contato. Os módulos 24, 26 podem ser similares aos módulos 14, 16 do leitor 10. De acordo com várias realizações, o cartão 22 pode ser um cartão de modo dual que é estruturado e arranjado para operar em um modo de chip ou em um modo de dados de tira magnética (utilizando dados equivalentes a Trilha 2). O modo de operação utilizado pelo cartão 22 pode ser determinado pelo cartão 22 com base nas capacidades do leitor 10.

O sistema 20 pode compreender adicionalmente uma rede 28 acoplada ao leitor 10 e um emissor 30. A rede 28 pode ser qualquer tipo adequado de rede conhecido na técnica, pode ser acoplada ao leitor 28 de qualquer maneira adequada conhecida na técnica, e pode ser acoplada ao emissor 30 de qualquer maneira adequada conhecida na técnica. A rede 28

pode incluir qualquer tipo de sistema de fornecimento incluído, porém não limitada a uma rede de área local (por exemplo, Ethernet), uma rede de área extensa (por exemplo, a Internet e/ou *World Wide Web*), uma rede telefônica (por exemplo, analógica, digital, com fio, sem fio, PSTN, ISDN, GSM, GPRS e/ou xDSL), uma rede comutada por pacotes, uma rede rádio, uma rede de televisão, uma rede de cabo, uma rede de satélite, e/ou qualquer outra rede de comunicações com fio ou sem fio configurada para transportar dados. A rede 28 pode incluir elementos, tais como, por exemplo, nós intermediários, servidores proxy, roteadores, chaves e adaptadores configurados para direcionar e/ou fornecer dados.

Figura 3 ilustra várias realizações de um método 40 para reduzir um tempo de interação para uma transação sem contato. O método 40 pode ser implementado pelo sistema 20 da Figura 2. O método 40 compreende as etapas gerais de processamento de transação preliminar 42, processamento de descoberta 44, seleção de aplicação 46, processamento de aplicação 48 e autorização de transação 50.

Para minimizar o tempo de interação entre o cartão 22 e o leitor 10 para uma dada transação, a etapa de processamento de transação preliminar 42 é executada pelo leitor 10, antes de requerer que o cartão 22 seja apresentado. Durante a etapa de processamento de transação preliminar 42, o leitor 10 executa certos processos de gerenciamento de risco baseados em transação. Por exemplo, de acordo com várias realizações, o leitor 10 pode obter a quantia de transação e comparar a quantia de transação com um limite de transação, um limite de piso, um limite de método de verificação de detentor do cartão, etc. Uma vez que a etapa de processamento de transação preliminar 42 é completada, o leitor 10 pode orientar um detentor do cartão para apresentar o cartão 22. Com base no processamento de transação preliminar, o leitor 10 pode requerer que a transação seja terminada, processada em linha ou processada fora de linha. Um fluxograma

simplificado ilustrando várias realizações da etapa de processamento de transação preliminar 42 é mostrado na Figura 4.

A etapa de processamento de descoberta 44 segue a etapa de processamento de transação preliminar 42. Uma vez que o cartão 22 é apresentado e está dentro do alcance do leitor 10, o leitor 10 energiza a interface sem contato 12 e estabelece comunicação com o cartão 22 via interface sem contato 12, durante a etapa de processamento de descoberta 44. Se o leitor 10 detecta cartões sem contato múltiplos 22 dentro de seu alcance, o leitor 10 pode indicar a condição a um detentor do cartão e pode requisitar que somente um cartão 22 seja apresentado para a transação. Em adição, um leitor 10 pode abortar uma transação durante a etapa de processamento de descoberta 44 e desenergizar a interface sem contato 12 sob o comando de um comerciante ou após um período de interrupção predefinido.

A etapa de seleção de aplicação 46 segue a etapa de processamento de descoberta 44. Durante a etapa de seleção de aplicação 46, o leitor 10 transmite uma primeira mensagem de comando (por exemplo, SELECIONE PPSE) ao cartão 22. A primeira mensagem de comando pode servir como uma requisição para uma lista de identificadores de aplicação, rótulos de aplicação e indicadores de prioridade de aplicação para aplicações que são suportadas pelo cartão 22 e estão acessíveis via interface sem contato 12. Sensível à primeira mensagem de comando, o cartão 22 constrói tal lista e transmite a lista ao leitor 10. De acordo com várias realizações, a lista pode ser provida dentro da informação de controle de arquivo (FCI) transmitida ao leitor 10. O leitor 10 então utiliza a lista transmitida pelo cartão 22 para construir uma lista de aplicações comum ao leitor 10 e ao cartão 22. Após construir a lista de aplicações comuns, o leitor 10 transmite uma segunda mensagem de comando (por exemplo, SELECIONE AID) para o cartão 22. A segunda mensagem de comando pode servir como uma requisição para conduzir a transação utilizando uma aplicação específica a partir da lista de

aplicações comuns. De acordo com várias realizações, a aplicação específica pode ser a aplicação comum tendo a prioridade mais alta, conforme indicado pelos indicadores de prioridade de aplicação previamente transmitidos pelo cartão 22. Sensível à segunda mensagem de comando, o cartão 22 transmite uma requisição ao leitor 10 para prover vários detalhes concernentes às capacidades do leitor 10 e exigências específicas de transação do leitor 10. De acordo com várias realizações, os detalhes requeridos podem ser providos em uma lista de objetos de dados de terminal (por exemplo, PDOL) associada ao leitor 10. Se a lista de objetivos de dados de terminal inclui um elemento de dados particular (por exemplo, qualificadores de transação do terminal), o processo avança para a etapa de processamento de aplicação 48. De outro modo, o leitor 10 pode terminar a transação ou tentar processar a transação através de uma outra interface. Um diagrama de fluxo simplificado ilustrando várias realizações da etapa de seleção de aplicação 46 é mostrado na Figura 5.

Durante a etapa de processamento de aplicação 48, o leitor 10 transmite uma terceira mensagem de comando (por exemplo, GPO) ao cartão 22, sensível à requisição do cartão para detalhes concernentes a capacidades do leitor 10 e exigências de transação específicas do leitor 10. A terceira mensagem de comando é estruturada de tal modo que pode ser utilizada no lugar de três comandos separados requeridos por especificações prévias. Reduzindo o número de comandos e respostas requeridos para completar a transação sem contato, o tempo de interação requerido entre o cartão 22 e o leitor 10 é adicionalmente minimizado. A terceira mensagem de comando pode compreender valores para qualquer número de elementos de dados requeridos pelo cartão 22. Vários valores de elementos de dados indicam o tipo de transações suportadas pelo leitor 10, se o processamento fora de linha e/ou em linha é suportado ou requerido pelo leitor 10, cujos métodos de verificação de detentor do cartão são suportados ou requeridos pelo leitor 10, etc. Os elementos de dados podem compreender qualificadores de transação

de terminal, a quantia da transação, um número imprevisível de terminal, um código de moeda corrente de transação, e quaisquer outros dados requeridos pelo cartão 22 em sua resposta à segunda mensagem de comando.

Com base no tipo de transações suportadas pelo leitor 10, o cartão 22 então executa um número de processo de gerenciamento de risco associados a um tipo de transação particular. De acordo com várias realizações, os processos de gerenciamento de risco podem incluir verificar um indicador de cartão interno para proteger contra rompimento da transação, comparar um valor de um código de moeda corrente da aplicação com um valor de um código de moeda corrente de transação, comparar o número de entradas de número de identificação pessoal com um limite predeterminado, determinar se um método de verificação de detentor de cartão é requerido, comparar a quantia de transação com um limite de valor inferior associado a um cartão 22, comparar a quantia de transação com uma quantia de transação total cumulativa associada ao cartão 22, comparar um valor de um contador de transação consecutiva com um valor de limite de transação consecutiva, etc. Efetuando os processos de gerenciamento de risco citados neste ponto da transação, em oposição a ser efetuado em um ponto mais tarde de acordo com especificações tradicionais, o tempo de interação entre o cartão 22 e o leitor 10 é adicionalmente minimizado. Com base no processamento de gerenciamento de risco, o cartão 22 pode requerer que a transação seja atenuada, processada em linha ou processada fora de linha. Em seguida à conclusão dos processos de gerenciamento de risco, o cartão 22 constrói a resposta apropriada para a terceira mensagem de comando e transmite a resposta ao leitor 10. A informação incluída na resposta pode variar, dependendo de se o cartão 22 deseja que a transação seja autorizada em linha, autorizada fora de linha ou terminada. Por exemplo, quando o cartão 22 deseja que a transação seja autorizada em linha, a resposta pode incluir um contador de transação de aplicação (ATC) que indica o número de transações

processadas pelo cartão, um criptograma de aplicação gerado pelo cartão 22 utilizando o contador de aplicação de transação e dados de terminal (por exemplo, o número imprevisível de terminal e a quantia de transação) incluídos na terceira mensagem de comando, um perfil de intercâmbio de aplicação (AIP) que indica suporte a características de gerenciamento de risco, dados de aplicação de emissor e dados equivalentes a Trilha 2, e vários outros elementos de dados.

Quando o cartão 22 deseja que a transação seja autorizada fora de linha, a resposta à terceira mensagem de comando pode incluir um contador de transação de aplicação (ATC) que indica o número de transações processadas pelo cartão. A resposta pode também incluir uma assinatura dinâmica gerada pelo cartão 22, utilizando o contador de transação de aplicação, os dados de terminal (por exemplo, o número imprevisível de terminal, a quantia de transação e a moeda corrente de transação) incluídos na terceira mensagem de comando, e um número imprevisível de cartão. A resposta pode incluir adicionalmente um criptograma de aplicação gerado pelo cartão 22, utilizando o contador de transação de aplicação e dados de terminal (por exemplo, o número imprevisível de terminal e a quantia de transação) incluídos na terceira mensagem de comando. Em adição, a resposta pode incluir um localizador de arquivo de aplicação (AFL) que indica a localização de arquivos e gravações relacionados à aplicação, um perfil de intercâmbio de aplicação (AIP) que indica suporte para características de gerenciamento de risco, dados de aplicação de emissor e vários outros elementos de dados. De acordo com várias realizações, o cartão 22 pode incrementar o contador de transação de aplicação antes de seu cálculo do criptograma de aplicação e assinatura dinâmica. Se o tamanho da assinatura dinâmica excede um limiar predeterminado, a assinatura dinâmica pode ser retornada na etapa de autorização 50, em resposta a uma quarta mensagem de comando descrita abaixo. De acordo com várias realizações, o criptograma de

aplicação gerado pelo cartão 22 compreende menos elementos de dados do que os criptogramas de aplicação utilizados pelas especificações prévias. Utilizando menos elementos de dados para gerar o criptograma da aplicação, o tempo de processamento global é reduzido e o tempo de interação entre o cartão 22 e o leitor 10 é adicionalmente minimizado.

A etapa de autorização 50 segue a etapa de processamento de aplicação 48. Após o leitor 10 receber a resposta para a terceira mensagem de comando do cartão 22, o cartão 22 pode ser removido do alcance do leitor 10, quando a transação deve ser autorizada em linha. Portanto, o cartão 22 não é requerido para permanecer dentro do alcance do leitor 10 enquanto a autorização em linha é requisitada e executada. Por ser capaz de remover o cartão 22 neste ponto do processo de transação, o tempo de interação entre o cartão 22 e o leitor 10 é adicionalmente minimizado. O leitor 10 pode então enviar o criptograma da aplicação, provido pelo cartão 22 em resposta à terceira mensagem de comando, em linha ao emissor 30. Com base em uma resposta subseqüentemente recebida pelo emissor 30, o leitor 10 aprova ou declina da transação.

Quando a transação deve ser autorizada fora de linha, o leitor 10 transmite uma quarta mensagem de comando (por exemplo, LER GRAVAÇÃO) ao cartão 22, após receber a resposta à terceira mensagem de comando a partir do cartão 22. A quarta mensagem de comando pode servir como uma requisição para as gravações indicadas no localizador de arquivo de aplicação (AFL) providas pelo cartão 22 em resposta à terceira mensagem de comando. Sensível à quarta mensagem de comando, o cartão 22 transmite as gravações apropriadas ao leitor 10. Portanto, o cartão 22 não é requerido a permanecer dentro do alcance do leitor 10, enquanto a autorização fora de linha é executada. Por ser capaz de remover o cartão 22 neste ponto no processo de transação, o tempo de interação entre o cartão 22 e o leitor 10 é adicionalmente minimizado. O leitor 10 pode então verificar se o cartão 22

expirou. Se o leitor 10 determina que o cartão 22 não expirou, o leitor 10 pode então efetuar autenticação de dados fora de linha. O tipo de autenticação de dados fora de linha efetuado, dados de autenticação estáticos (SDA) ou dados de autenticação dinâmicos (DDA) são determinados com base no perfil de intercâmbio de aplicação (AIP) provido pelo cartão 22 em resposta à terceira mensagem de comando.

Para autenticação de dados estática, o leitor 10 tenta validar a assinatura estática provida pelo cartão 22 em resposta à terceira mensagem de comando. A autenticação de dados estáticos envolve validar dados de aplicação importantes para assegurar que os dados não tenham sido alterados fraudulentamente. Se a assinatura estática é validada, a transação é aprovada fora de linha. De outro modo, a transação pode ser enviada em linha ou terminada. Para autenticação de dados dinâmicos, o leitor 10 tenta validar a assinatura dinâmica provida pelo cartão 22, em resposta à terceira mensagem de comando. A autenticação de dados dinâmicos envolve validar dados de aplicação importantes para assegurar que os dados não tenham sido alterados fraudulentamente e que o cartão 22 é genuíno. De acordo com várias realizações, a validação da assinatura dinâmica pode compreender utilizar o contador de transação de aplicação (ATC) e o número imprevisível de terminal providos pelo cartão 22 em resposta à terceira mensagem de comando, para recalcular a assinatura dinâmica. Se a assinatura dinâmica é validada, o leitor 10 gera uma mensagem de liberação que inclui o criptograma provido pelo cartão 22 em resposta à terceira mensagem de comando e outros dados relacionados. De outro modo, a transação pode ser enviada em linha ou terminada. De acordo com várias realizações, se a assinatura dinâmica não é validada, o leitor 10 pode enviar a transação em linha utilizando o criptograma previamente recebido do cartão 22. Então, o leitor 10 pode gerar uma requisição em linha com um criptograma fora de linha. Um fluxograma simplificado ilustrando várias realizações da etapa de

autorização 50 é mostrado na Figura 6.

Conforme descrito abaixo, o método 40 pode ser utilizado para minimizar o tempo de interação entre o cartão 22 e o leitor 10 para uma transação sem contato por menos de aproximadamente 500 milissegundos. Para evitar um ataque *de capa* fora de linha na transação sem contato, várias realizações do método 40 podem utilizar um novo tipo de autenticação de dados dinâmicos. Para transações fora de linha, o cartão 22 pode utilizar o contador de transação de aplicação (ATC) e o número imprevisível de cartão, juntamente com o número imprevisível de terminal, a quantia da transação e o código de moeda corrente da transação incluídos na terceira mensagem de comando (por exemplo, GPO) para criar a assinatura dinâmica. O localizador de arquivo de aplicação (AFL) que é subseqüentemente enviado com a assinatura dinâmica ao leitor 10 na resposta à terceira mensagem de comando, indica gravações contendo os certificados RSA e dados relacionados a autenticação de dados dinâmicos. Portanto, durante a etapa de autenticação 50, o leitor 10 pode ler um certificado do emissor, um certificado de cartão sem contato, e dados relacionados a autenticação de dados dinâmicos. De acordo com várias realizações, o leitor 10 pode utilizar o contador de transação de aplicação (ATC), o número imprevisível de cartão, o número imprevisível de terminal, a quantia de transação e o código de moeda corrente da transação recebidos do cartão 22, em resposta à quarta mensagem de comando para recalcular a assinatura dinâmica para fins de validação. Em instâncias em que a transação sem contato tenha sido submetida a um ataque *de capa*, o recálculo não coincidirá com a assinatura dinâmica previamente recebida do cartão 22. Para tais instâncias, o leitor 10 pode declinar ou terminar a transação sem contato.

Figura 7 ilustra várias realizações de um método 60 para reduzir um tempo de interação para uma segunda transação sem contato que ocorre em seguida à requisição para autorização em linha na etapa 50 do

método 40. De acordo com várias realizações, o método 60 pode compreender uma porção do método 40. O método 60 pode ser implementado pelo sistema 20 da Figura 2. O método 60 pode ser utilizado para minimizar o tempo de interação entre o cartão 22 e o leitor 10 para a segunda transação sem contato, para menos de aproximadamente 500 milissegundos. De acordo com várias realizações, o método 60 compreende as etapas gerais da segunda requisição de transação 62, seleção de aplicação 64, processamento de aplicação 66 e aprovação de transação 68.

A segunda transação sem contato não é uma transação financeira. Como a segunda transação sem contato compreende o cartão 22 ser apresentado dentro do alcance do leitor 10 por uma segunda vez, o processo pode ser referido como um processamento de retorno do cartão. Antes do início do processo, durante a primeira transação descrita acima, ambos leitor 10 e cartão 22 podem indicar um ao outro que suportam processamento de retorno de cartão. Por exemplo, o leitor 10 e o cartão 22 podem indicar seu suporte de processamento de retorno de cartão durante a etapa de seleção de aplicação 46 da primeira transação.

Após a requisição para a autorização em linha na etapa 50 do método 40, o leitor 10 ou o cartão 22 (via detentor do cartão) pode requisitar a segunda transação sem contato durante a segunda etapa de requisição de transação 62. De acordo com várias realizações, o leitor 10 pode requisitar a segunda transação sem contato durante a segunda etapa de requisição de transação 62, quando uma resposta do emissor à requisição de autorização em linha compreende uma mensagem a ser fornecida ao cartão 22. Tal mensagem pode ser utilizada para prover atualizações ou reinícios de contagem para o cartão 22, ou para bloquear a conta. Por exemplo, em uma resposta de autorização em linha, o emissor 30 pode incluir uma mensagem de escrita na resposta que requisita que o cartão 22 seja apresentado por uma segunda vez. Desta maneira, o emissor 30 pode ser capaz de bloquear subseqüentemente a

conta, repor a capacidade de gasto fora de linha, aumentar o limite de gasto fora de linha, etc., mesmo se o cartão 22 não tiver requisitado que estas atitudes sejam tomadas. Para orientar o detentor do cartão a apresentar o cartão 22 por uma segunda vez, o leitor 10 pode exibir uma mensagem indicando que tempo de processamento de cartão adicional é requerido, uma mensagem requisitando apresentar, por favor, o cartão novamente, etc.

De acordo com outras realizações, o cartão 22 pode requerer a segunda transação no sentido de receber uma recarga quando a capacidade de gasto fora de linha do cartão se torna baixa. Por exemplo, quando a capacidade de gasto fora de linha do cartão torna-se baixa, o cartão 22, via detentor do cartão, pode requisitar uma recarga, requisitando uma autorização em linha e provendo a quantia de gasto disponível corrente. Para assegurar que o cartão 22 sendo apresentado é o mesmo cartão 22 que foi apresentado para a primeira transação, o cartão 22 pode ser autenticado durante a segunda etapa de requisição de transação 62.

A etapa de seleção de aplicação 64 segue a segunda etapa de requisição de transação 62. A etapa de seleção de aplicação 64 do método 60 pode ser similar à etapa de seleção de aplicação 46 do método 40 descrito acima. Durante a etapa de seleção de aplicação 64, o leitor 10 transmite uma mensagem de comando (por exemplo, SELECIONE VSDC AID) ao cartão 22. A mensagem de comando pode servir como uma requisição para conduzir a segunda transação, utilizando uma aplicação específica a partir da lista de aplicações comuns previamente construídas pelo leitor 10. Sensível à mensagem de comando, o cartão 22 transmite uma PDOL ao leitor 10. A PDOL pode ser similar à PDOL transmitida ao leitor 10 durante a etapa de seleção de aplicação 46 do método 40 descrito acima. Se a PDOL inclui um elemento de dados particular (por exemplo, qualificadores de transação de terminal), o processo avança para a etapa de processamento de aplicação 66.

A etapa de processamento de aplicação 66 segue a etapa de

seleção de aplicação 64. A etapa de processamento de aplicação 66 pode ser similar à etapa de processamento de aplicação 48 do método 40 descrito acima, porém é diferente em que nenhum processamento de transação financeira é envolvido. Durante a etapa de processamento de aplicação 66, o leitor 10 transmite uma outra mensagem de comando (por exemplo, GPO) ao cartão 22. Ao receber a mensagem de comando, o cartão 22 constrói uma resposta enviada e transmite a resposta ao leitor 10.

A etapa de aprovação de transação 68 segue a etapa de processamento de aplicação 66. De acordo com várias realizações, se o emissor 30 decide recarregar a capacidade de gasto fora de linha associada ao cartão 22, o emissor 30 pode transmitir um criptograma de resposta e aprovar a transação ou incluir uma mensagem escrita com um código de autenticação de mensagem (MAC). O criptograma ou MAC podem servir para assegurar que as atualizações, reinícios de contagem, etc., sejam apenas feitas ao cartão 22 associados ao emissor 30.

Conforme descrito acima, o método 60 pode ser utilizado para mudar parâmetros de risco de cartão, contadores de cartão, estado de cartão, etc. Por exemplo, com respeito a mudar parâmetros de risco de cartão, o método 60 pode ser utilizado para aumentar o limite de gasto fora de linha, aumentar o limite de transação único, permitir que o cartão execute transações em duas ou mais moedas correntes diferentes, mude a taxa de conversão de moeda corrente utilizada, etc. Com respeito a mudar contadores de cartão, o método 60 pode ser utilizado, por exemplo, para reiniciar a quantidade de gasto disponível fora de linha, etc. Com respeito a mudar o estado do cartão, o método 60 pode ser utilizado para bloquear ou desbloquear uma aplicação particular. Um especialista na técnica verificará que o método 60 pode ser utilizado para trocar outros parâmetros, contadores, etc.

Embora várias realizações da invenção tenham sido descritas aqui por meio de exemplo, aqueles especialistas na técnica verificarão que

várias modificações, alterações e adaptações às realizações descritas podem ser realizadas, sem se afastar do espírito e escopo da invenção definida pelas reivindicações anexas. Por exemplo, de acordo com várias realizações, o leitor 10, sistema 20 e/ou método 40 descritos acima podem ser modificados para evitar tipos análogos de "ataques *de capa*" em conjuntos portáteis sem fio, *pen drives*, e outros dispositivos que utilizam a transmissão de informação sem fio. Adicionalmente, várias realizações do om60 podem ser utilizadas para processar transações relacionadas a conversões de moeda corrente, programas de fidelidade, etc.

REIVINDICAÇÕES

1. Leitor, caracterizado pelo fato de compreender:

uma interface sem contato;

um módulo de transação acoplado à interface sem contato, em que:

o módulo de transação é estruturado e arranjado para:

descobrir a presença de um dispositivo de pagamento sem contato dentro de uma distância predeterminada a partir do leitor;

energizar a interface sem contato quando da descoberta da presença do dispositivo de pagamento sem contato dentro de uma distância predeterminada a partir do leitor, em que a interface sem contato energizada permite a comunicação entre o dispositivo de pagamento sem contato e o leitor;

enviar para o dispositivo de pagamento sem contato, através da interface sem contato, uma requisição para dados; e

receber, a partir do dispositivo de pagamento sem contato, através da interface sem contato, os dados requisitados;

processar:

a transação sem contato com menos de meio segundo de tempo de interação entre o dispositivo de pagamento sem contato e o leitor; e

a autenticação de dados dinâmica e estática utilizando os dados requisitados; e

um módulo de segurança acoplado ao módulo de transação, em que o módulo de segurança é arranjado e estruturado para evitar um ataque de intermediários na transação sem contato.

2. Cartão, emitido por um emissor, caracterizado pelo fato de compreender:

um módulo de transação estruturado e arranjado:

para comunicação sem fio, em que o cartão é estruturado e arranjado para operar em ambos um modo de chip e um modo de dados de tira magnética;

para cooperar com um leitor para:

ser descoberto por estar dentro de uma distância predeterminada do leitor;

receber do leitor uma primeira mensagem de comando que contém uma requisição para uma lista de aplicativos que são suportados pelo cartão para conduzir uma transação sem contato;

enviar ao leitor, em resposta à primeira mensagem de comando, a lista requisitada de aplicativos;

receber do leitor uma segunda mensagem de comando requisitando a condução da transação sem contato utilizando um dos referidos aplicativos da lista de aplicativos;

enviar, em resposta à segunda mensagem de comando, uma requisição para prover um dos tipos de transação sem contato suportado pelo leitor;

receber uma terceira mensagem de comando contendo o requisitado um tipo da referida transação sem contato suportado pelo leitor;

enviar, em resposta à terceira mensagem de comando:

uma requisição para autorização fora de linha da transação sem contato; e

um endereço na memória do cartão dos dados relativos à um daqueles do referido aplicativo da lista de aplicativos;

receber, em resposta à requisição para a autorização fora de linha da transação sem contato, uma quarta mensagem de comando contendo uma requisição para os dados relativos à um daqueles do referido aplicativo da lista de aplicativos no endereço na memória do cartão;

enviar, em resposta à quarta mensagem de comando, os dados requisitados relativos à um daqueles do referido aplicativo da lista de aplicativos; e

executar a transação sem contato que inclui comunicações interativas com o emissor do cartão com menos de meio segundo de tempo de interação entre o cartão e o leitor; e

um módulo de segurança estruturado e arranjado para cooperar com o leitor para evitar um ataque de intermediários em uma transação sem contato.

3. Aparelho, caracterizado pelo fato de compreender:

um cartão emitido por um emissor; e

um leitor, compreendendo:

uma interface sem contato;

um módulo de transação, acoplado à interface sem contato; e estruturado e arranjado para:

descobrir a presença do cartão dentro de uma distância predeterminada a partir do leitor;

energizar a interface sem contato quando da descoberta da presença do cartão dentro da distância predeterminada a partir do leitor, em que a interface sem contato energizada permite a comunicação entre o cartão e o leitor;

enviar para o cartão, através da interface sem contato, uma requisição para dados; e

receber, a partir do cartão, através da interface sem contato, os dados requisitados;

processar uma transação sem contato com menos de meio segundo de tempo de interação entre o cartão e o leitor; e

um módulo de segurança, acoplado ao módulo de transação e estruturado para cooperar com o cartão para evitar, utilizando-se os dados requisitados, um ataque de intermediários na transação sem contato; e

em que o cartão está estruturado e arranjado para comunicar com o leitor através da interface sem contato, e inclui:

um módulo de transação estruturado e arranjado para:

enviar ao leitor:

uma requisição para informação; e

os dados requisitados;

receber, a partir do leitor:

as informações requisitadas; e

a requisição para dados, e

um módulo de segurança estruturado e arranjado para cooperar com o leitor para evitar utilizando-se as informações requisitadas, um ataque de intermediários na transação sem contato.

4. Aparelho leitor, caracterizado pelo fato de compreender:

um meio para iniciar a comunicação com um dispositivo de pagamento sem contato utilizado para uma transação sem contato através de:

energizar uma interface sem contato com o dispositivo de pagamento sem contato quando detecta-se o dispositivo de pagamento sem contato dentro de uma faixa predeterminada a partir do

aparelho leitor, em que a interface sem contato energizada permite a comunicação entre o cartão e o leitor; e

enviar para o dispositivo de pagamento sem contato, através da interface sem contato, uma primeira mensagem de comando que contém uma requisição para uma lista de aplicativos que são suportados pelo dispositivo de pagamento sem contato para conduzir a transação sem contato;

um meio para receber, através da interface sem contato, em resposta à primeira mensagem de comando, a lista requisitada de aplicativos;

um meio para enviar para o dispositivo de pagamento sem contato, através da interface sem contato, uma segunda mensagem de comando que requisita a condução da transação sem contato utilizando um dos referidos aplicativos da lista de aplicativos;

um meio para receber, através da interface sem contato, em resposta à segunda mensagem de comando, uma requisição a partir do dispositivo de pagamento sem contato para prover um tipo de transação sem contato suportado pelo leitor;

um meio para enviar, através da interface sem contato, uma terceira mensagem de comando para o dispositivo de pagamento sem contato que contém o um tipo requisitado da referida transação sem contato suportada pelo leitor;

um meio para receber a partir do dispositivo de pagamento sem contato, através da interface sem contato, em resposta à terceira mensagem de comando:

uma requisição para autorização fora de linha da transação sem contato; e

um endereço relacionado aos dados para dito aplicativo da lista de aplicativos;

um meio para enviar, através da interface sem contato, em resposta à requisição para a autorização fora de linha, uma quarta mensagem de comando para o dispositivo de pagamento sem contato que contém uma requisição para os dados no endereço para o referido aplicativo da lista de aplicativos;

um meio para receber, a partir do dispositivo de pagamento sem contato, através da interface sem contato, em resposta à quarta mensagem de comando, os dados requisitados no endereço para o referido aplicativo da lista de aplicativos;

um meio para terminar, em resposta ao recebimento dos dados requisitados no endereço para o referido aplicativo da lista de aplicativos, a comunicação com o dispositivo de pagamento sem contato através da interface sem contato; e

um meio que, após a referida terminação da comunicação com o dispositivo de pagamento sem contato, utiliza os dados requisitados no endereço para o referido aplicativo da lista de aplicativos, executa a autorização fora de linha da transação sem contato, em que o tempo entre o envio da primeira mensagem de comando e a terminação da comunicação através da interface sem contato com o dispositivo de pagamento sem contato é de menos do que meio segundo.

5. Aparelho leitor, de acordo com a reivindicação 4, caracterizado pelo fato de adicionalmente compreender:

um meio para ler a partir do dispositivo de pagamento sem contato:

uma assinatura dinâmica que inclui:

um contador de transação de aplicativo;

um código da moeda da transação; e

um número imprevisível do dispositivo de pagamento sem contato;

um meio para recalcular a assinatura dinâmica que utiliza o número imprevisível do dispositivo de pagamento sem contato; e

um meio para validar, utilizando a assinatura dinâmica, em que a autorização fora de linha da transação sem contato não é executada a não ser que a assinatura dinâmica seja validada pelo meio para validação.

6. Aparelho leitor, de acordo com a reivindicação 4, caracterizado pelo fato de adicionalmente compreender:

um meio para restabelecer a comunicação com o dispositivo de pagamento sem contato através da interface sem contato; e

um meio para completar uma segunda dita transação sem contato com menos de meio segundo de interação entre o dispositivo de pagamento sem contato e a leitora.

7. Aparelho leitor, de acordo com a reivindicação 6, caracterizado pelo fato de que a segunda dita transação sem contato é uma transação sem contato não financeira.

8. Aparelho leitor, de acordo com a reivindicação 6, caracterizado pelo fato de que o meio para completar a segunda dita transação sem contato adicionalmente compreende um meio para transmitir, através da interface sem contato, uma mensagem que contém uma mudança na memória no dispositivo de pagamento sem contato.

9. Aparelho leitor, caracterizado pelo fato de compreender:

um meio para descobrir a presença de um dispositivo de pagamento sem contato dentro de uma distância predeterminada a partir do aparelho leitor;

um meio para energizar uma interface sem contato quando da descoberta da presença do dispositivo de pagamento sem contato dentro da distância predeterminada a partir do aparelho leitor, em que a interface sem contato energizada permite a comunicação entre o dispositivo de pagamento sem contato e o aparelho leitor;

um meio para ler a partir do dispositivo de pagamento sem contato, através da interface sem contato, uma assinatura dinâmica a partir do dispositivo de pagamento sem contato, a assinatura dinâmica que inclui:

um código de moeda de transação; e

um número imprevisível do dispositivo de pagamento sem contato;

um meio para recalcular a assinatura dinâmica que utiliza o número imprevisível do dispositivo de pagamento sem contato;

um meio para validar, utilizando a assinatura dinâmica;

um meio para autorizar fora de linha a transação sem contato, se a assinatura dinâmica é validada; e

um meio para completar uma transação sem contato com menos de meio segundo de interação entre o dispositivo de pagamento sem contato e o aparelho leitor.

10. Aparelho leitor, de acordo com a reivindicação 9, caracterizado pelo fato de que o meio para ler adicionalmente lê um criptograma a partir do dispositivo de pagamento sem contato que compreende um contador de transação de aplicativo; e o aparelho leitor adicionalmente compreende um meio para requisitar que a transação sem contato seja processada em linha com o criptograma se a assinatura dinâmica não for validada pelo meio de validação.

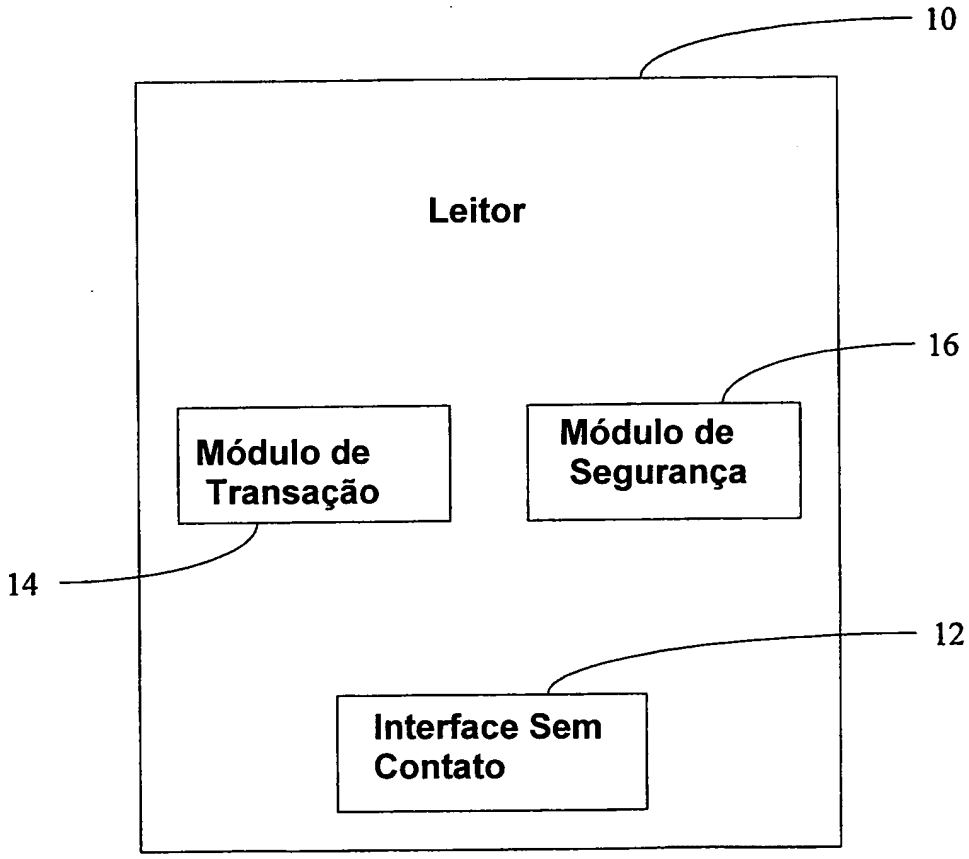

10
Leitor
16
Módulo de Transação
Módulo de Segurança
14
12
Interface Sem Contato

FIG. 1

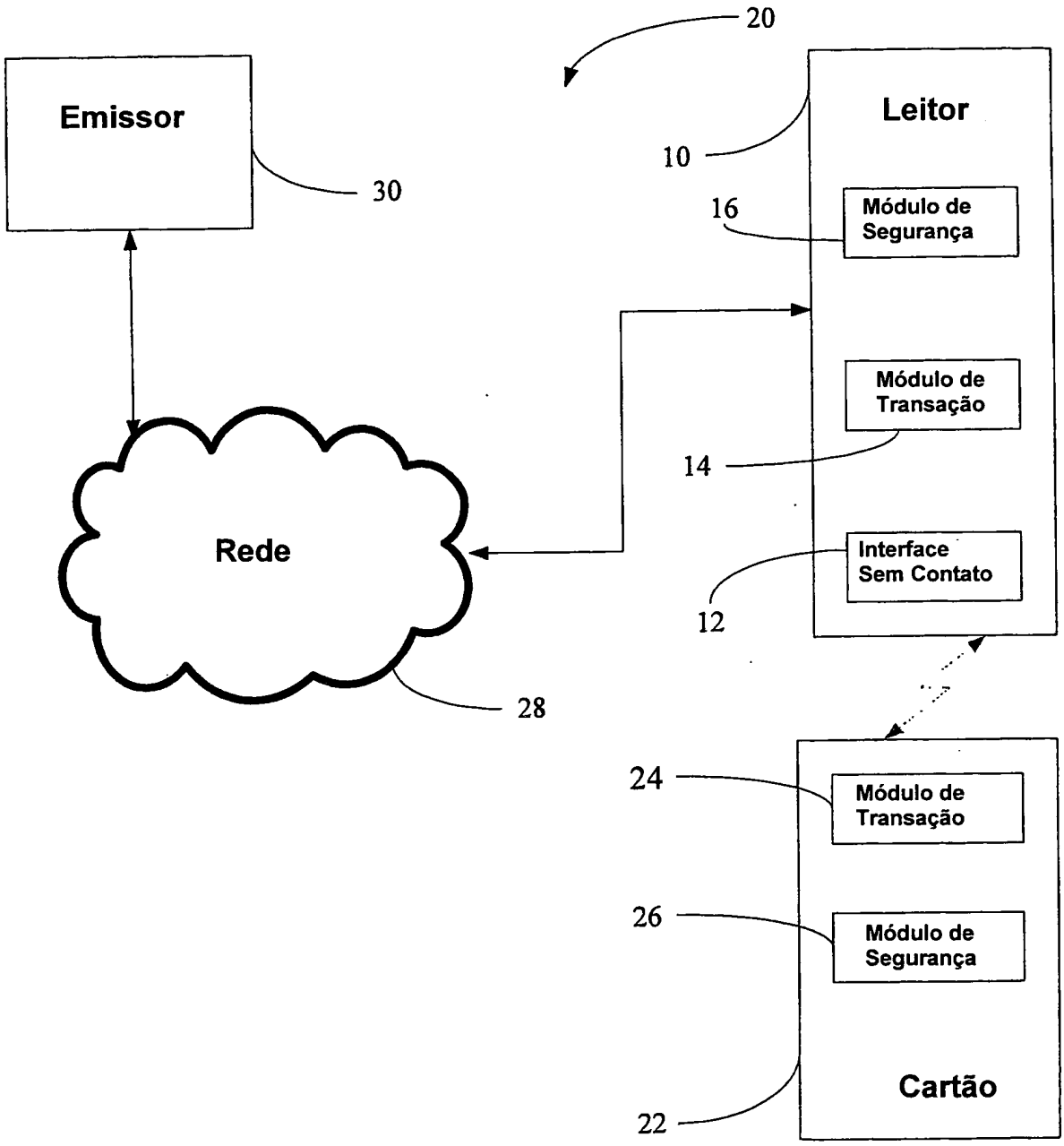

20
Emissor
30
Leitor
10
16
Módulo de Segurança
Módulo de Transação
14
Rede
Interface Sem Contato
12
28
24
Módulo de Transação
26
Módulo de Segurança
Cartão
22

FIG. 2

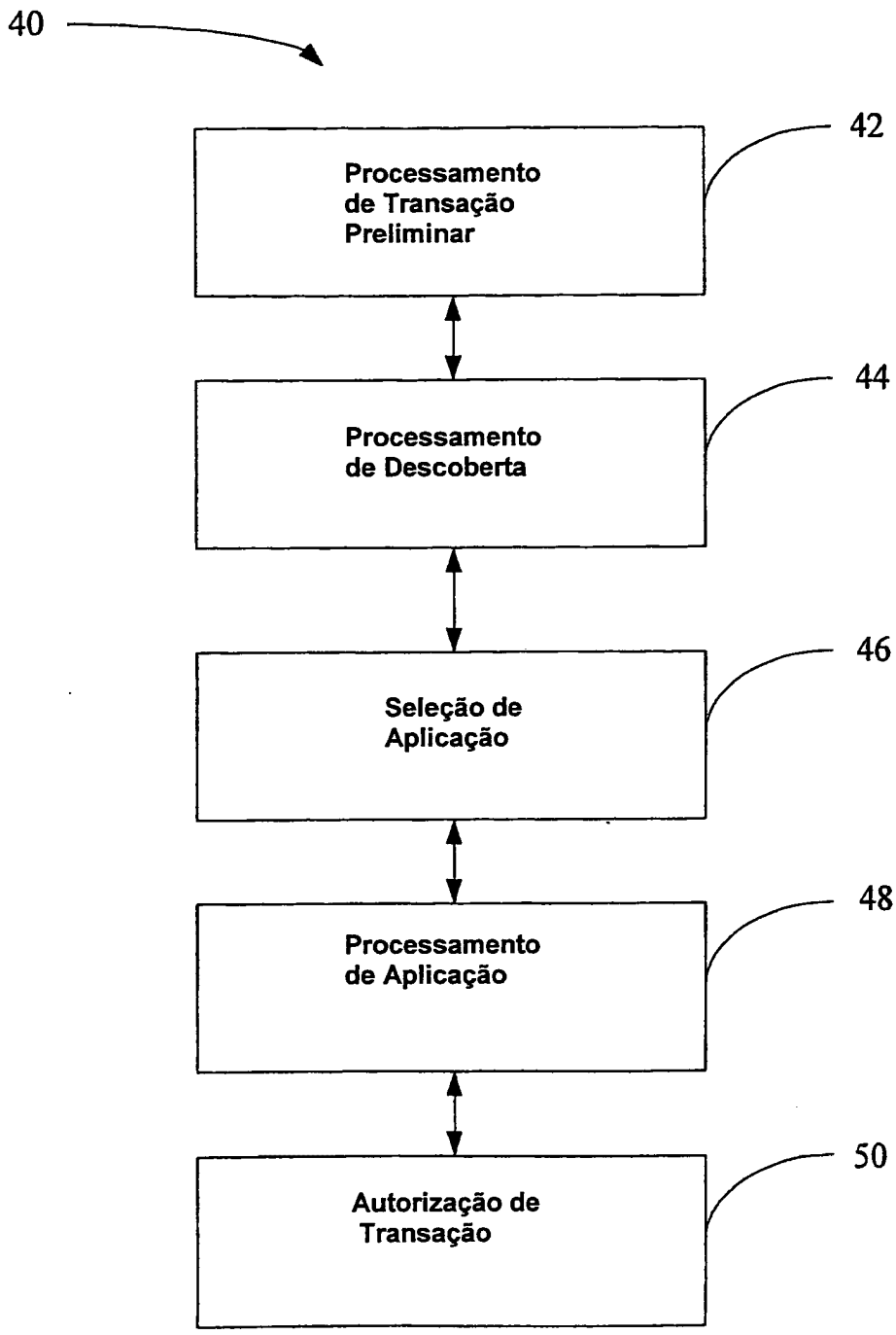

40
42
Processamento de Transação Preliminar
44
Processamento de Descoberta
46
Seleção de Aplicação
48
Processamento de Aplicação
50
Autorização de Transação

FIG. 3

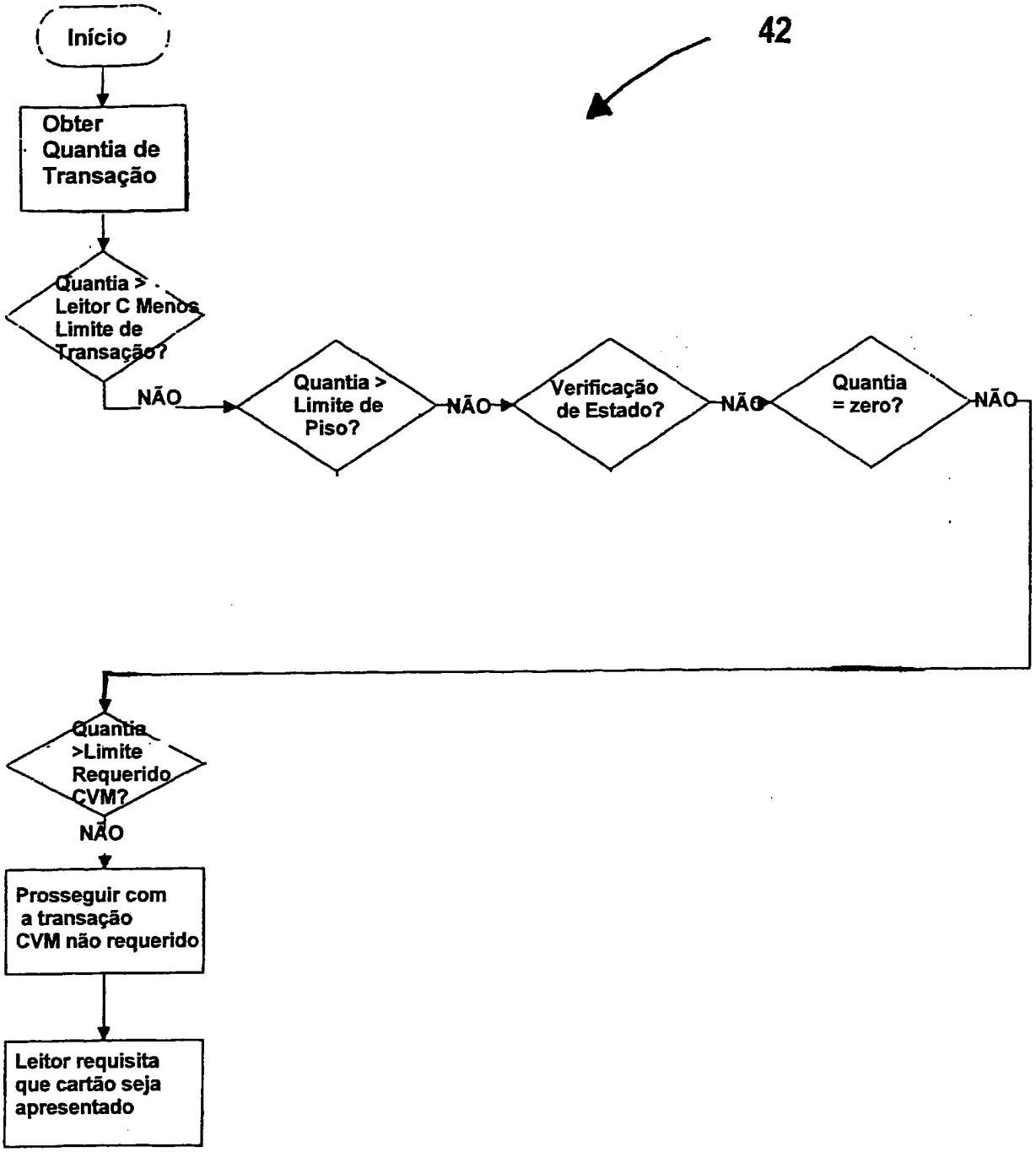

42
Início
Obter Quantia de Transação
Quantia > Leitor C Menos Limite de Transação?
NÃO
Quantia > Limite de Piso?
NÃO
Verificação de Estado?
NÃO
Quantia = zero?
NÃO
Quantia >Limite Requerido CVM?
NÃO
Prosseguir com a transação CVM não requerido
Leitor requisita que cartão seja apresentado

Fig. 4

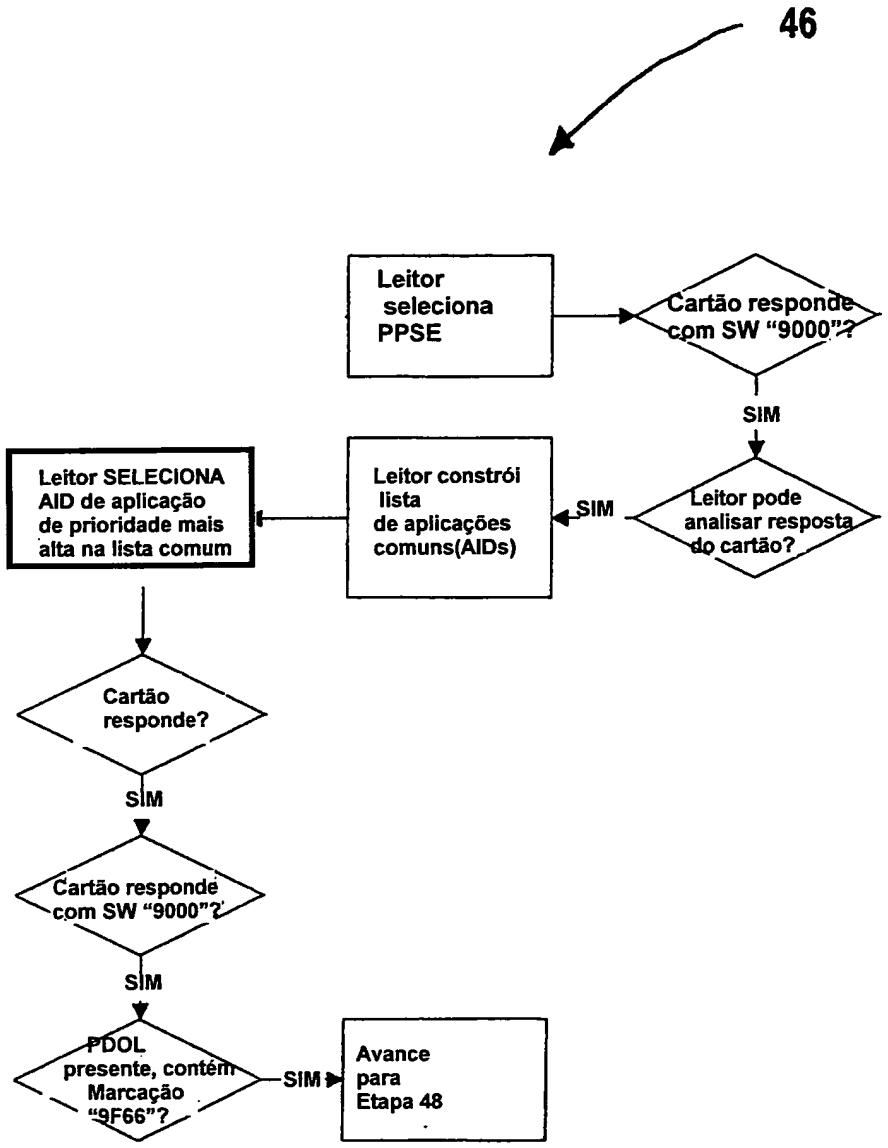

46
Leitor seleciona PPSE
Cartão responde com SW "9000"?
SIM
Leitor pode analisar resposta do cartão?
SIM
Leitor constrói lista de aplicações comuns(AIDs)
Leitor SELECIONA AID de aplicação de prioridade mais alta na lista comum
Cartão responde?
SIM
Cartão responde com SW "9000"?
SIM
PDOL presente, contém Marcação "9F66"?
SIM
Avance para Etapa 48

Fig. 5

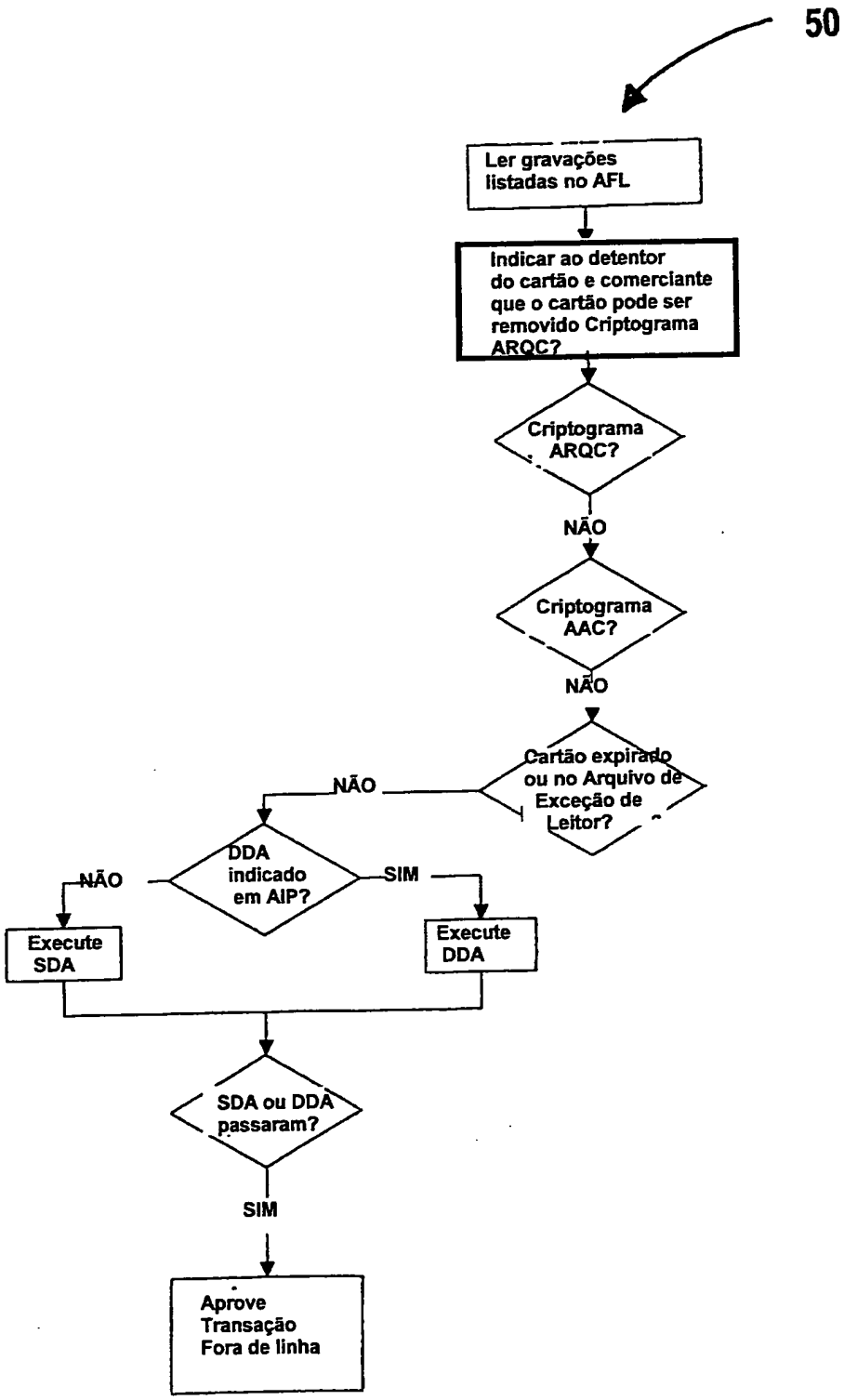

50
Ler gravações listadas no AFL
Indicar ao detentor do cartão e comerciante que o cartão pode ser removido Criptograma ARQC?
Criptograma ARQC?
NÃO
Criptograma AAC?
NÃO
Cartão expirado ou no Arquivo de Exceção de Leitor?
NÃO
DDA indicado em AIP?
NÃO
SIM
Execute SDA
Execute DDA
SDA ou DDA passaram?
SIM
Aprove Transação Fora de linha

Fig. 6

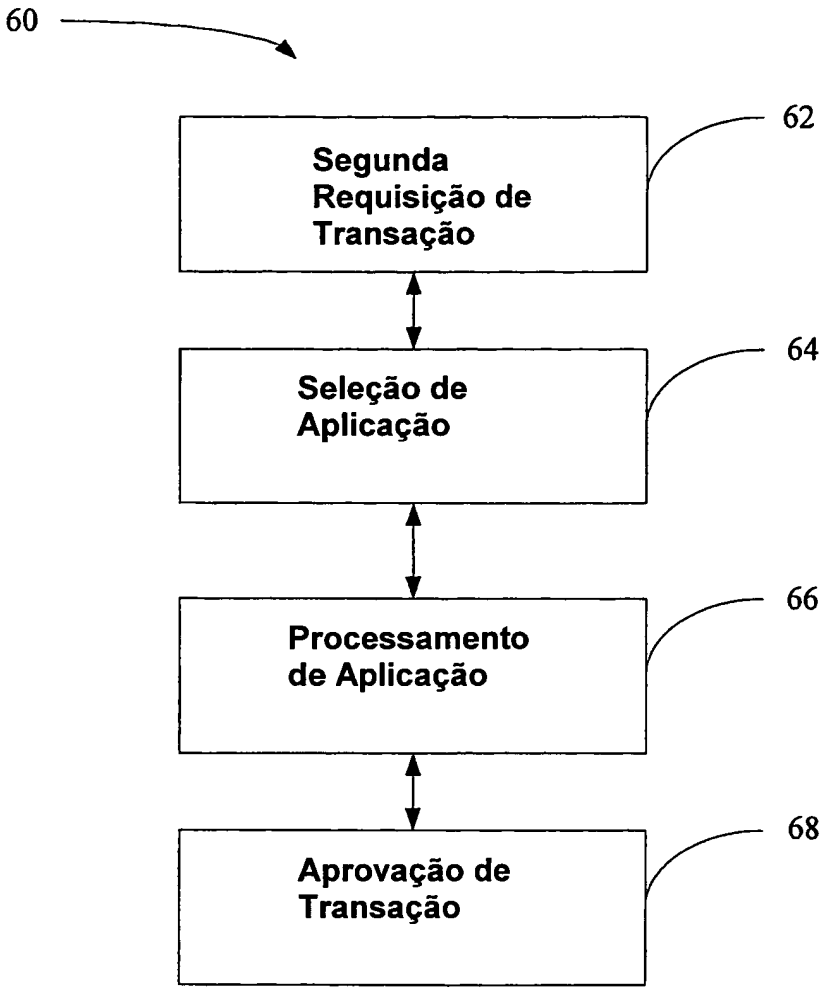

60
62
Segunda Requisição de Transação
64
Seleção de Aplicação
66
Processamento de Aplicação
68
Aprovação de Transação

FIG. 7

PI 0616470-6

RESUMO

"LEITOR, CARTÃO, APARELHO, E, APARELHO LEITOR PARA REDUZIR UM TEMPO DE INTERAÇÃO PARA UMA TRANSAÇÃO SEM CONTATO, E PARA EVITAR UM ATAQUE DE INTERMEDIÁRIOS NA TRANSAÇÃO SEM CONTATO"

O método compreende, em um leitor, efetuar pelo menos um processo de gerenciamento de risco baseado em transação, antes de energizar uma interface sem contato, iniciar comunicação com um cartão utilizado para a transação sem contato, receber informação associada ao cartão e terminar a comunicação com o cartão, antes de autorizar a transação sem contato.