



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

(21) **PI 0620579-8 A2**



(22) Data de Depósito: 28/03/2006
(43) Data da Publicação: 02/05/2012
(RPI 2156)

(51) *Int.Cl.:*
G06K 19/06
G06K 5/00

(54) **Título:** APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE

(30) **Prioridade Unionista:** 08/12/2005 US 11/296,309

(73) **Titular(es):** Ho Chun-Hsin

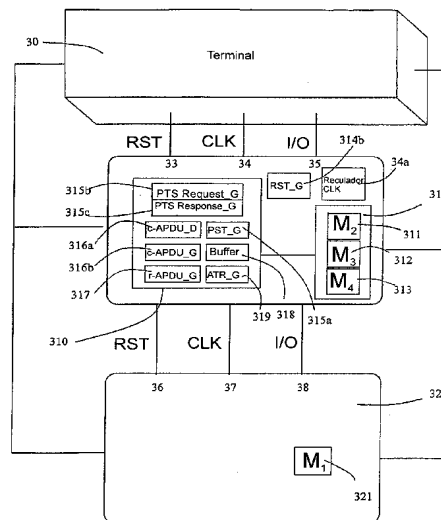
(72) **Inventor(es):** Ho Chun-Hsin

(74) **Procurador(es):** Edmundo Brunner Ass em Prop Indl Ltda

(86) **Pedido Internacional:** PCT US2006011329 de 28/03/2006

(87) **Publicação Internacional:** WO 2007/067202de 14/06/2007

(57) **Resumo:** APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE. Um cartão inteligente é revelado e inclui um processador; uma primeira interface para utilização em comunicação com um terminal; uma segunda interface para utilização em comunicação com outro cartão inteligente; e um aparelho de geração RST para a geração de um sinal para o outro cartão inteligente.





PI0620579-8

1/22

APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE.

Campo da invenção

A presente invenção está relacionada com um cartão
5 inteligente, e mais particularmente, com um cartão inteligente dentro
de um sistema de cartão duplo para utilização em conjunto com um
terminal tal qual um leitor de cartão de caixa automático ou um leitor
de cartão de um ponto de venda, ou em conjunto com um terminal de
comunicação, i.e., um telefone móvel.

10 Histórico da Invenção

No passado, um cartão magnético era utilizado como um
cartão de banco ou cartão de crédito.

Dentro de um sistema de cartão magnético, dados de
identificação pessoal para a identificação do possuidor do cartão
15 magnético, o qual é conhecido como uma senha é armazenada no
cartão magnético e a coincidência entre a senha
eletromagneticamente lida a partir do cartão carregada em uma leitora
de cartão e uma senha manualmente inserida pelo dono do cartão é
checada para determinar se o usuário do cartão é o dono válido do
20 cartão.

Todavia, os seguintes problemas residem no cartão
magnético.

Primeiramente, a senha gravada no cartão magnético pode
ser lida por um equipamento simples e assim a utilização por uma
25 pessoa não autorizada pode ser facilmente conseguida.

Em segundo lugar, a senha deve ser conhecida somente
pelo possuidor.

Entretanto, o equipamento para a escrituração da senha é

necessário e a pessoa que prepara o cartão acaba ciente da senha.

Em terceiro lugar, a proteção de segurança para um caixa automático ou de uma leitora de cartão de crédito não é perfeita e a prevenção de vazamento da senha não é perfeita.

5 De qualquer forma, a senha não pode ser alterada pelo titular e o cartão é utilizado mesmo quando outra pessoa torna-se conhecedora da senha.

Para superar os problemas acima, a patente dos Estados Unidos da América número 4,758,718, intitulada "Cartão IC de Alta
10 Segurança com uma Senha Atualizável" por Fujisaki e outros, revela um cartão IC possuindo um microprocessador e uma memória.

Na FIGURA 1, o número 10 denota um cartão IC utilizado como meio de identificação para a identificação de uma pessoa, o número 11 denota um microprocessador para controlar o registro e a
15 atualização de dados de senha, o número 12 denota uma interface de comunicação para a conexão com um aparelho de terminal, o número 13 denota um teclado para inserir os dados da senha, o número 14 denota um aparelho de monitor tal qual um LCD para exibir os dados da senha, o número 15 denota uma memória possuindo áreas para o
20 armazenamento de dados necessários para o registro e atualização da senha, o número 16 denota uma área de memória de senha na memória 15, a área de senha possuindo 16 bits, o número 17 denota uma área para o armazenamento do número de vezes de não coincidência da senha na memória 15, o número 18 denota uma área
25 para o armazenamento dos dados representando um tipo e atributos do cartão IC 10 e o número 19 denota uma bateria.

A memória 15 possui uma área de registro de senha na qual a senha deve ser registrada e uma área de atualização de senha na

qual os dados de atualização para a atualização da senha registrada na área de registro estão armazenados.

A senha é inserida por meio de uma operação de chaveamento e o microprocessador controla o registro da senha e
5 registra a senha inserida na área de registro de senha.

Quando a senha registrada é para ser alterada, o número de vezes de entrada de erro da senha registrada no microprocessador é checada baseada nos dados pré-estabelecidos na área de atualização da senha.

10 Se o número de vezes erradas é menor que um número predeterminado, a área de registro bem como a área de atualização da senha é liberada e a nova senha inserida é permitida para ser registrada na área de registro.

Nos dias de hoje, cartões IC ou “cartões inteligentes” são
15 utilizados em várias aplicações tais como pagamento em um ponto de venda (conhecido como “cartões de banco”), telefones públicos, pagamento de estacionamento, pagamento de pedágio, telefones móveis (e.g. cartões SIM), serviços de saúde, transporte público, ou bolsa eletrônica.

20 Cada uma dessas aplicações está associada com um cartão específico: cartão do banco, cartão de telefone, cartão de estacionamento, cartão SIM para telefones GSM, e assim por diante.

Um dos problemas encontrados na utilização diária de tal variedade de cartões resta no fato de que um dos cartões pode não
25 estar disponível quando for para ser utilizado, não importando se foi deixado em casa, acabou o crédito, ou expirou.

Em adição, a administração e transporte de vários cartões é inconveniente.

Desta forma existe uma forte necessidade para os então chamados “cartões multi-aplicação”.

Por exemplo, a patente dos Estados Unidos da América número 6,325,293, intitulada “Método e Sistema para a Utilização de um Cartão Micro-circuito em uma Pluralidade de Aplicações” por Moreno, revela um cartão micro-circuito incluindo aparelho ativando uma aplicação padrão a ser executada aparelho ativando uma aplicação alvo a ser executada e um aparelho de troca ativando o cartão a ser configurado sob comando tanto como um cartão de aplicação padrão ou como uma cartão de aplicação alvo.

A FIGURA 2 mostra a organização e a seqüência geral de operação do método então descrito.

Como mostrado na FIGURA 2, a subscrição tomada por um cliente 20 a partir do operador de rádio telefone 21 operando o rádio telefone do usuário 22 inclui não só serviço de rádio telefone em geral, e.g., pagamento de estacionamento, onde a quantia será incluída como um item específico no consumo de telefonia listado mensalmente recebido do operador 21 (cobrança representada como 23).

Após estacionar o carro próximo a uma máquina de métrica de estacionamento “pague-e-mostre” 24 programada para aceitar pagamento de cartões pré-pagos emitidos pela cidade 25, o motorista pode descobrir que nenhum cartão de estacionamento utilizável está disponível, ou que o cartão está sem crédito ou inválido.

Para realizar o pagamento requerido pela máquina, o usuário então seleciona o comando “estacionamento” no seu radio-telefone, e.g., por meio do pressionamento de um botão 26 ou por meio da seleção de uma opção dentro de um menu apontando os serviços

oferecidos pela operadora de telefonia.

Este comando faz com que o cartão SIM 27 do rádio-telefone, seja reconfigurado como cartão de estacionamento.

5 O usuário então extrai o cartão 27 do rádio-telefone e o insere (seta 28) na máquina 24, a qual percebe o cartão como sendo um cartão de estacionamento e o cartão é então operado e debitado como tal.

10 O usuário reinsere o cartão 27 (seta 29) no rádio-telefone 22 onde é lido pelo rádio-telefone o qual automaticamente o reconfigura para sua função GSM.

Embora tais cartões multi-aplicação sejam tecnicamente factíveis, na prática eles são muito difíceis de implementar, como demonstrado por várias tentativas pioneiras desde a invenção do cartão IC propriamente dito.

15 Com a utilização espalhada em larga escala de cartões inteligentes na indústria móvel tais como o cartão SIM para o GSM, USIM para o WCDMA, RUIM para o CDMA2000 e o PIM para a rede PHS, uma grande variedade de aplicações tem sido desenvolvidas através da utilização de cartões inteligentes residentes em telefones
20 móveis (SIM/USIM/RUIM/PIM, doravante denominados como UICC, Universal Integrated Circuit Card – cartão de circuito integrado universal) para fornecer serviços de segurança.

Operadores móveis asseguram a segurança do uso de serviços móveis pela autenticação das chaves armazenadas nos
25 cartões inteligentes que as operadoras móveis emitiram para os subscritores.

Em adição, operadoras móveis também fornecem serviços Premium tais como banco móvel, serviços de negociação no mercado

acionário móvel por meio do armazenamento de chaves fornecidas pelos bancos ou outros provedores de serviço nos cartões SIM.

As chaves são manipuladas através de uma interface de aplicação desenvolvida por um Kit de ferramentas SIM (STK) o qual está também residido no cartão SIM propriamente dito.

Quando telefones WAP (Wireless Application Protocol – protocolo de aplicação sem fio) estão disponíveis, WIM (Wireless Identity Module – módulo de identidade sem fio) são também desenvolvidos pelos vendedores de cartões SIM para assegurar a segurança do WAP por meio do armazenamento de certificado e de algoritmo PKI dentro do SIM propriamente dito (cartão SWIM) ou outro cartão WIM sozinho o qual pode ser inserido dentro de outra baia de cartão dentro do telefone móvel.

O teclado e a tela de exibição do telefone móvel facilitam o cartão inteligente inserido com uma grande interface de usuário e a natureza móvel do acesso remoto aos provedores de serviço ainda alcançam o objetivo da mobilidade de serviço.

Visando alcançar a mobilidade de serviço, os provedores de serviço tais como bancos, administradoras de cartões de crédito, emissores de cartões de transporte, emissores de certificado e corretores da bolsa estão ansiosos para cooperar com o operador móvel para emitir cartões SIM aprimorados de forma que forneçam serviços que caiam dentro de suas profissões.

Entretanto, o provisionamento e gerenciamento das capacidades e funcionalidades estão sob o controle dos operadores móveis, desta forma formando um sistema fechado onde apenas as partes acordadas estão autorizadas a participar.

Além disso, o relacionamento entre os provedores de

serviços e os operadores móveis é um de falta de confiança mútua e ambos possuem questões similares sobre o controle da segurança e métodos de pagamento.

5 Isto se torna o principal obstáculo para o desenvolvimento de serviços de segurança móveis.

Dentro do mundo da telecomunicação móvel, outra demanda emergente baseada nos cartões inteligentes é a então chamada “titularidade SIM múltipla” a qual indica a tendência de um usuário de telefone móvel único possuindo mais de um cartão SIM que pode ser
10 emitido por operadores móveis diversos.

A tendência surge devido às seguintes razões:

- possuir contas separadas para utilização pessoal e profissional
- ter SIM's de operadores móveis de diferentes países enquanto viaja para economizar a cobrança da taxa de roaming
15
- manter SIM's separados para diferentes planos de serviços tais como ligações durante o dia e fora do pico
- manter SIM's separados para pacotes de tarifas promocionais diferentes para economizar custos
20

Um telefone móvel especial com capacidade para dois chips ou duas baias costumava ser introduzido para resolver as questões acima, por meio do fornecimento de uma baia de chip adicional no telefone móvel para que outro provedor de serviço ou outro operador
25 móvel possa emitir seu próprio cartão inteligente ou SIM armazenando suas próprias chaves secretas.

Entretanto, os telefones especiais são normalmente caros e não muito bem aceitos pelo usuário, assim formando um local de

mercado fragmentado onde os provedores de serviço podem jogar.

Desta forma, é necessário que seja fornecido um cartão inteligente que possa retificar essas desvantagens da arte anterior e resolver os problemas acima.

5 **Resumo da invenção**

Este parágrafo extrai e compila algumas características da presente invenção; outras características serão reveladas nos parágrafos que acompanham.

10 É pretendida a cobertura de várias modificações e arranjos similares incluídos dentro do espírito e escopo das reivindicações apensadas.

Em concordância com um aspecto da presente invenção, um cartão inteligente inclui um processador; uma primeira interface para utilizar em comunicação com um terminal; uma segunda interface
15 para utilização em comunicação com outro cartão inteligente; e meios de geração RST para gerar um sinal RST para outro cartão inteligente.

Preferencialmente, o processador ainda inclui uma setor de armazenamento para receber e salvar um sinal ATR (Answer To
20 Reset – resposta para reiniciar) a partir de outro cartão inteligente.

Preferencialmente, o processador ainda inclui meios de geração de ATR para a geração de um sinal ATR.

Preferencialmente, o processador ainda inclui meios de geração de solicitação PTS (Protocol Type Selection – seleção de tipo
25 de protocolo) para a geração de um sinal de solicitação PTS para outro cartão inteligente.

Preferencialmente o processador ainda inclui meios de geração de resposta PTS para a geração de um sinal de resposta

PTS para o terminal.

Preferencialmente o processador ainda inclui meios de determinação PTS para determinar se o sinal de solicitação PTS é aceitável por ambos o terminal e outro cartão inteligente.

5 Preferencialmente, o processador ainda inclui um regulador de relógio para o fornecimento de uma frequência de relógio para outro cartão inteligente.

Mais vantajosamente, o processador ainda inclui meios de determinação de comando APDU (Application Protocol Data Unit –
10 unidade de dados de protocolo de aplicação) para determinar se um sinal APDU de comando emitido a partir do terminal está associado com o cartão inteligente ou com outro cartão inteligente.

Mais vantajosamente, o processador ainda inclui meios de geração APDU de comando para a geração de um sinal APDU de
15 comando para outro cartão inteligente.

Mais vantajosamente, o processador ainda inclui um setor de armazenamento para receber e salvar um sinal APDU de resposta a partir de outro cartão inteligente.

Mais vantajosamente, o processador ainda inclui meios de
20 geração APDU de resposta para a geração de um sinal APDU de resposta para o terminal.

Mais vantajosamente, o cartão inteligente é provido com uma antena para comunicação com um terminal sem contato.

Mais vantajosamente, o cartão inteligente compreende um
25 cartão SIM (Subscriber Identity Module – módulo de identidade do subscritor), um cartão USIM (Universal Subscriber Identity Module – módulo de identidade do subscritor universal), um cartão UIM (User Identity Module – módulo de identidade do usuário) e um cartão RUIM

(Removable User Identity Module – módulo de identidade do usuário removível).

Mais vantajosamente, o cartão inteligente compreende um cartão de crédito, um cartão de débito e um cartão de saque
5 automático.

Breve descrição dos desenhos

Os objetos e vantagens acima da presente invenção irão tornar-ser mais prontamente aparentes para àqueles ordinariamente versados na arte após a revisão da seguinte descrição detalhada e
10 dos desenhos que a acompanham, nos quais:

FIGURA 1 – é um diagrama de blocos mostrando um cartão IC convencional;

FIGURA 2 – é um diagrama mostrando vários aparelhos e jogadores em conformidade com um outro método convencional;

15 **FIGURA 3** – é um diagrama de blocos de uma primeira incorporação de um cartão inteligente em um sistema de dois cartões para utilização com um terminal de transação em conformidade com a presente invenção;

FIGURA 4 – é um diagrama de blocos de uma segunda
20 incorporação de um cartão inteligente em um sistema de dois cartões para utilização com um terminal de comunicação em conformidade com a presente invenção; e

FIGURA 5A e 5B – são fluxogramas mostrando um método de transação opor meio da utilização de um sistema de dois cartões
25 em conformidade com a presente invenção.

Descrição detalhada da invenção

A presente invenção revela um cartão inteligente em um sistema de cartão duplo e um método para a utilização do mesmo, e

os objetos e vantagens da presente invenção irão tornar-se mais prontamente aparentes para aqueles ordinariamente versados na arte após a revisão da seguinte descrição detalhada.

5 A invenção não tem necessidade de estar limitada às seguintes incorporações.

Primeira incorporação

Favor referir-se à FIGURA 3.

10 Ela ilustra um diagrama de blocos de uma primeira incorporação de um cartão inteligente em um sistema de cartão duplo para a utilização com um terminal de transação em conformidade com a presente invenção.

Como mostrado na FIGURA 3, o sistema de dois cartões para utilização com o terminal de transação 30 consiste de um primeiro cartão 32 e um segundo cartão 31.

15 O primeiro cartão 32 possui uma primeira memória 321 para o armazenamento da primeira informação de identificação para utilização em uma transação alvo com um terminal de transação 30.

20 O segundo cartão 31 inclui um processador 310 um aparelho de geração RST 314b, uma segunda memória 311, uma terceira memória 312, uma quarta memória 313, e um regulador de relógio 34a.

A segunda memória 311 armazena segundas informações de identificação para utilização em uma transação alvo com o terminal de transação 30.

25 A terceira memória 312 armazena informações relacionadas às transações.

A quarta memória 313 armazena primeiras informações pessoais que não estão asseguradas pelo primeiro cartão 32.

O regulador de relógio 34a recebe um sinal de relógio a partir do terminal de transação 30 via linha CKL 34 e fornece outro sinal de relógio para o primeiro cartão 32 via linha CKL 37.

5 O sinal do relógio fornecido por meio do regulador de relógio 34a pode ser o mesmo ou diferente do fornecido pelo terminal de transação 30.

Neste meio tempo, o primeiro cartão 32 é instalado com um primeiro sistema operacional e o segundo cartão 31 é instalado com um segundo sistema operacional.

10 O segundo cartão 31 pode fazer o papel de um cartão inteligente e de um leitor de cartão simultaneamente visando controlar o primeiro cartão 32.

15 O segundo cartão 31 está acoplado ao terminal de transação 30 por meio de três linhas: linha RST 33, linha CLK 34, e porta I/O 35, cujas linhas estão naturalmente em adição a uma linha de fornecimento de energia VCC e uma linha terra GND.

Mais ainda, o terminal de transação 30 é um leitor de cartão inteligente de um aparelho portátil ou um terminal fixo como um caixa de banco ou um ponto de venda.

20 Além disso, o primeiro cartão 32 é acoplado ao segundo cartão 31 por meio de três linhas: linha RST 36, linha CLK 37, e porta I/O 38, como mostrado.

25 Na realidade, o segundo cartão 31 é provido com duas portas I/O, porta I/O 35 e porta I/O 38 para comunicar com o terminal de transação 30 e o primeiro cartão 32, respectivamente.

Certamente, o segundo cartão 31 está apto a realizar diferentes protocolos de comunicação da porta I/O 35 e da porta I/O 38.

Em conformidade com a primeira incorporação da presente invenção, o segundo cartão 31 está também apto a emitir comandos da unidade de dados de protocolo de aplicação (APDU) através da porta I/O 38 para o primeiro cartão 32, e o segundo cartão 31 fornece 5 sinais de relógio para o primeiro cartão 32 através da linha CLK 27.

Em outras palavras, o segundo cartão 31 age tanto como um cartão inteligente e um leitor de cartão inteligente no controle do primeiro cartão 32.

Em geral, um cartão inteligente envia uma resposta para 10 recomeçar (ATR) por meio da porta I/O para uma leitora de cartão após uma voltagem de fornecimento VCC, um relógio CLK e um sinal de recomeço RST ter sido aplicado.

A corrente de dados e os elementos de dados do ATR estão definidos e descritos em detalhes na norma ISO/IEC 7816-3.

15 O formato ATR básico é mostrado na tabela 1.

Tabela 1 – Os elementos de dados do ATR e seus significados em conformidade com a norma ISO/IEC 7816-3.

Elemento de dados	Descrição
TS	Caractere inicial
T0	Caractere de formato
TA1, TB1, TC1, TD1...	Caractere de interface
T1, T2,..., TK	Caractere histórico
TCK	Caractere de checagem

Os primeiros dois bytes, designados TS e T0, definem vários 20 parâmetros de transferência fundamentais e a presença de bytes subseqüentes.

Os caracteres de interface especificam parâmetros de transferência especiais para o protocolo, os quais são importantes para a transferência de dados seguinte.

Os caracteres históricos descrevem a extensão das funções

básicas do cartão inteligente.

O caractere de checagem, o qual é uma soma de checagem dos bytes anteriores podem ser opcionalmente enviados como o último byte do ATR, dependendo do protocolo de transmissão.

5 Mais ainda, esta corrente de dados do ATR é sempre enviada com um valor divisor e contém vários dados relevantes para o protocolo de transmissão e para o cartão.

Como sabido, o cartão inteligente mostra vários parâmetros nos caracteres de interface do ATR, tais como o protocolo de
10 transmissão e o tempo de espera do caractere.

Além disso, se um terminal quer modificar um ou mais destes parâmetros, uma seleção de tipo de protocolo (PTS) deve ser realizada antes da execução real do protocolo.

O terminal pode utilizar isto para modificar certos parâmetros
15 de protocolo, na medida em que é permitido pelo cartão.

Na presente invenção, com referência à FIGURA 3 e 4, o processador 310 do segundo cartão 31 inclui um armazenador 318, um aparelho de geração de ATR 319, um aparelho de determinação PTS 315a, um aparelho de geração de pedido PTS 315b, um aparelho
20 de geração de resposta PTS 315c, um aparelho de determinação APDU de comando 316a, um aparelho de geração APDU de comando 316b, e um aparelho de geração APDU de resposta 317.

Em uma transação, um terminal de transação 30 determina se um primeiro cartão 32 existe após ser ligado (estágio S500 e
25 S501).

Se um primeiro cartão 32 não existe dentro de um sistema de transação, então o terminal de transação 30 irá realizar uma falta de transação com o segundo cartão 31 (estágio S502).

Mais ainda, a falta de transação pode também ser uma comunicação sem contato com outro terminal por meio de uma antena prevista no segundo cartão 31.

5 Neste caso, a comunicação é através de uma comunicação de rádio.

Por outro lado, se um primeiro cartão 32 existe, então o terminal de transação 30 irá realizar em um sistema de dois cartões.

10 Dentro de um sistema de dois cartões, sinais que são para serem enviados para o primeiro cartão 32, todos vão através do segundo cartão 31.

Em outras palavras, o terminal de transação 30 não se comunica diretamente com o primeiro cartão 32.

Isto é, o segundo cartão 31 é um escravo do terminal de transação 30, mas também um mestre para o primeiro cartão 32.

15 Desta forma, sinais de recomeço (RST2) emitidos a partir do terminal de transação 30 são enviados diretamente para o segundo cartão 31 apenas, não importando se a transação está relacionada ao primeiro cartão 32 ou ao segundo cartão 31.

20 Uma vez que o segundo cartão recebe o RST2, então o aparelho de geração de RST 314b irá gerar um sinal de recomeço (RST1) para o primeiro cartão 32 (estágio S503).

25 Após o recebimento do RST1, o primeiro cartão 32 responde com um sinal de resposta-para-recomeço (ATR1) para o armazenador 318 (e.g., armazenador primeiro-dentro primeiro-fora (FIFO)) do segundo cartão 31 (estágio S504).

Após o recebimento do ATR1 a partir do primeiro cartão 32, o aparelho de geração ATR 319 do segundo cartão 31 gera outro sinal de resposta-para-recomeço (ATR2') para o terminal de transação 30

(estágio S505).

No geral, o sinal de resposta-para-recomeço deve ocorrer entre 400 e 40.000 ciclos de relógio após o terminal de transação 30 enviar um sinal de recomeço.

5 Com uma taxa de relógio de 3,5712 MHz, isso corresponde a um intervalo de 112 μ s a 11,20ms, enquanto a 4,9152 MHz, o intervalo é de 81,38 μ s a 8,14ms.

Se o terminal de transação 30 não receber o ATR dentro deste intervalo, ele repete a seqüência de ativação várias vezes
10 (usualmente até três vezes) para tentar detectar um ATR.

Se todas estas tentativas falharem, o terminal assume que o cartão está faltando e responde de acordo.

Entretanto, se o ATR1 é enviado para o segundo cartão 31 após o segundo cartão 31 receber o RST2 a partir do terminal de
15 transação 30, como mencionado acima, então será difícil para o ATR1 responder dentro do tempo.

Desta forma, para superar este problema, o aparelho de geração de RST 314b do segundo cartão 31, está programado para gerar espontaneamente um sinal de recomeço (RST1) para o primeiro
20 cartão 32, uma vez que o segundo cartão 31 está ligado independentemente do recebimento do RST2 a partir do terminal de transação 30.

Isto quer dizer que o aparelho de geração de RST 314b não necessariamente espera até que o RST2 seja enviado a partir do
25 terminal de transação 30 antes de enviar o RST1 para o primeiro cartão 32 para evitar resposta atrasada para o terminal de transação 30.

Assim, o segundo cartão 31 preserva o ATR1 enviado a

partir do primeiro cartão 32 dentro do armazenador 318 até o RST2 ser recebido.

Desta forma, o ATR1 pode ser imediatamente enviado após o RST2 ser emitido.

5 Após o terminal de transação receber um sinal ATR a partir de um aparelho de geração de ATR 319, o terminal então continuamente envia um sinal de solicitação PTS (Seleção de Tipo de Protocolo) (PTS1) para o segundo cartão 31 para realizar a negociação PTS (estágio S506).

10 Então o aparelho de geração de solicitação PTS 315b do segundo cartão 31 irá gerar um sinal de solicitação PTS (PTS2) para o primeiro cartão 32.

Em resposta ao PTS2, o primeiro cartão 32 envia um sinal de resposta PTS (PTS3) de volta para o segundo cartão 31.

15 Da mesma forma, o aparelho de determinação PTS 315a do segundo cartão 31 determina se o protocolo indicado pelo primeiro sinal de solicitação PTS emitido a partir do terminal de transação 30 está apto para ser realizado por ambos o primeiro cartão 32 e o segundo cartão 31 em conformidade com o PTS3 enviado a partir do
20 primeiro cartão 31.

A seguir, o aparelho de geração de resposta PTS 315c do segundo cartão 31 irá enviar outro sinal de resposta PTS (PTS4) para o terminal de transmissão 30.

25 Esta seqüência irá continuar até o protocolo indicado do terminal de transação 30 ser aceito entre o terminal de transação 30 e o segundo cartão 31 e entre o segundo cartão 31 e o primeiro cartão 32.

Uma vez que um protocolo indicado é encontrado, o terminal

de transação 30 irá enviar um sinal APDU de comando (c-APDU1) para o aparelho de determinação APDU de comando 316a do segundo cartão 31 (estágio S507) solicitando uma transação.

5 Após o recebimento do c-APDU1, o aparelho de determinação APDU de comando 316a determina se o c-APDU1 solicita uma falta de transação ou uma transação alvo (estágio S508).

10 Se o c-APDU1 emitido a partir do terminal de transação 30 solicita uma transação alvo, o aparelho de geração APDU de comando 316b do segundo cartão 31 irá gerar um sinal APDU de comando (c-APDU2) para o primeiro cartão 32 (estágio S509) e então realizar uma transação alvo (estágio S510).

O primeiro cartão 32 irá enviar uma resposta APDU (r-APDU1) para o armazenador 318 do segundo cartão 31 após a transação alvo ser realizada (estágio S511).

15 Após o recebimento da r-APDU1 a partir do primeiro cartão 32, o aparelho de geração APDU de resposta 317 do segundo cartão 31 então gera outro sinal de resposta APDU (r-APDU2) para o terminal de transação 30 indicando que a transação alvo está finalizada (estágio S512).

20 Nesta incorporação da presente invenção a informação relacionada com a transação é re-escrita pelo processador 310 quando uma solicitação de transação emitida a partir do primeiro cartão é aprovada pelo terminal de transação baseada na primeira ou segunda informação de identificação.

25 Por exemplo, a informação relacionada à transação pode ser um saldo para um saldo de cartão de débito e o processador 310 pode aumentar/diminuir o saldo quando a transação é realizada.

Além disso, o segundo cartão 31 pode detectar a existência

de um primeiro cartão 32 pelo cálculo do tempo de resposta do ATR1 a partir do primeiro cartão 32 quando o sistema de dois cartões estiver inserido dentro de um terminal de transação; alternativamente, o segundo cartão 31 pode fornecer uma interface de usuário tal qual um menu do kit de ferramenta de aplicação SIM do cartão sim para o usuário configurar a presença do primeiro cartão se um sistema de dois cartões for inserido dentro de um telefone móvel.

Por exemplo, um cartão de ponto de venda (POS), o qual armazena valores é considerado como o segundo cartão 31 da presente invenção e um cartão de caixa automático, o qual armazena uma conta bancária, é considerado como o primeiro cartão 32.

Ambos possuem funções originais.

Na presente o cartão do ponto de venda (POS) pode ser considerado como um cartão máster, o qual é também um leitor de cartão e apto a ler o cartão do caixa automático em um terminal de transação.

Assim, um usuário pode remeter dinheiro da conta bancária armazenada no cartão do banco para a bolsa eletrônica do cartão do ponto de venda (POS) por meio de um terminal de transação em conformidade com a presente invenção.

No caso de um sistema de dois cartões dentro de um telefone móvel, o cartão SIM é considerado como o segundo cartão e o cartão do ponto de venda POS é considerado como o primeiro cartão da presente invenção, um usuário pode recarregar dinheiro na bolsa eletrônica do cartão do ponto de venda (POS) por meio de uma mensagem curta terminada móvel a partir do banco em resposta à mensagem curta originada a partir do usuário, visando preencher cartão de ponto de venda (POS).

Neste caso, o telefone celular é considerado um terminal.

Da mesma forma, a presente invenção fornece um sistema de dois cartões para a utilização com dois diferentes terminais de transação para facilitar a transação de informações na prática.

5 Segunda incorporação

Por favor refira-se à FIGURA 4.

Ela ilustra um diagrama de blocos de uma segunda incorporação de um cartão inteligente dentro de um sistema de dois cartões para a utilização com um terminal de comunicação em
10 concordância com a presente invenção.

Como mostrado na FIGURA 4 o sistema de dois cartões para utilização com o terminal de comunicação 40 consiste de um primeiro cartão 42 e um segundo cartão 41.

O primeiro cartão 42 possui uma primeira memória 421 para
15 o armazenamento de primeiras informações de identificação as quais incluem primeiras informações pessoais, primeiras chaves secretas e primeiras funções de segurança para utilização em comunicação com um terminal remoto 49 por meio do terminal de comunicação 40.

O segundo cartão 41 inclui um processador 410, uma
20 segunda memória 411, uma terceira memória 412 e um aparelho de seleção 413.

A segunda memória 411 armazena segundas informações de identificação as quais incluem segundas informações pessoais, segundas chaves secretas, e segundas funções de segurança para a
25 utilização em comunicação com um terminal remoto 49 por meio do terminal de comunicação 40.

A terceira memória 412 pode armazenar a primeira informação pessoal a qual não está assegurada pelo primeiro cartão

32.

O aparelho de seleção 413 é para determinar uma função de segurança do primeiro cartão e do segundo cartão a qual é para ser realizada.

5 O processador 410 efetua ou não o primeiro cartão 42 baseado em se o primeiro cartão ou o segundo cartão é selecionado por meio do aparelho de seleção 413.

Nesta incorporação, tanto o primeiro cartão 42 e o segundo cartão 41 poderiam ser um cartão SIM (Subscriber Identity Module –
10 módulo de identidade do subscritor), um cartão USIM (Universal Subscriber Identity Module – módulo de identidade do subscritor universal), um cartão UIM (User Identity Module – módulo de identidade do usuário) e um cartão RUIM (Removable User Identity Module – módulo de identidade do usuário removível), os quais são
15 utilizados para sistemas de comunicação móveis diferentes.

Quando dois cartões SIM são considerados como primeiro cartão 42 e segundo cartão 41, respectivamente, o segundo cartão SIM poderia integrar ambas as informações dos dois cartões SIM, tais como dois catálogos de telefone.

20 O aparelho de seleção está normalmente apresentado pelo menu do Kit de ferramentas SIM o qual fornece interface ao usuário para selecionar o SIM que deve ser utilizado para registrar-se à rede móvel.

Na prática, o sistema de dois cartões está apto a integrar
25 dois cartões SIM em um terminal de comunicação, i.e., telefone móvel.

Conforme a presente invenção, uma empresa de telecomunicações móvel poderia fornecer o serviço para o seu usuário

para integrar um cartão SIM velho de uma outra companhia com um cartão SIM novo.

5 O usuário poderia fazer uma ligação telefônica com duas identificações diferentes por meio da seleção de um dos dois cartões SIM à sua escolha.

Enquanto a invenção foi descrita em termos do que está presentemente considerado como sendo as incorporações mais práticas e preferidas, deve ser entendido que a invenção não precisa estar limitada às incorporações reveladas.

10 Ao contrário, ela é pretendida para cobrir várias modificações e arranjos similares incluídos dentro do espírito e do escopo das reivindicações apensadas, as quais devem ser acordadas com a mais ampla interpretação de forma a englobar todas as tais modificações e estruturas similares.

REIVINDICAÇÕES

1. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, caracterizado por um cartão inteligente, compreendendo:
 - 5 (a) um processador;
 - (b) uma primeira interface para utilização na comunicação com um terminal;
 - (c) uma segunda interface para utilização em comunicação com um outro cartão inteligente; e
 - 10 (d) meios de geração RST para a geração de um sinal RST para dito outro cartão inteligente.
2. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, caracterizado por um cartão inteligente, onde o dito processador ainda inclui um
15 armazenador para o recebimento e salvamento de um sinal ATR (Answer To Reset – resposta para recomeçar) a partir do dito outro cartão inteligente.
3. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, caracterizado por um
20 cartão inteligente, onde o dito processador ainda inclui meios de geração ATR para a geração de um sinal ATR.
4. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, caracterizado por um
25 cartão inteligente, onde o dito processador ainda inclui meios de geração de solicitação PTS (Protocol Type Selection – seleção de tipo de protocolo) para a geração de um sinal de solicitação PTS para o dito outro cartão inteligente.
5. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO**

INTELIGENTE, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito processador ainda inclui meios de geração de resposta PTS para a geração de um sinal de resposta PTS para o dito terminal.

5 6. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 4, **caracterizado** por um cartão inteligente, onde o dito processador ainda inclui meios de determinação PTS para determinar se o dito sinal de solicitação PTS é aceitável por ambos, dito terminal e dito outro cartão inteligente.

10 7. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito processador ainda inclui um regulador de relógio para o fornecimento de uma frequência de relógio para o dito outro cartão inteligente.

15 8. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito processador ainda inclui meios de determinação APDU (Application Protocol Data Unit – unidade de dados de protocolo de aplicativo) de comando para determinar se um sinal de comando APDU emitido a partir do dito terminal está associado com o dito cartão inteligente ou dito outro cartão inteligente.

20 9. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito processador ainda inclui meios de geração APDU de comando para a geração de um sinal APDU de comando para o dito outro cartão inteligente.

- 5
- 10
- 15
- 20
- 25
10. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde dito processador ainda inclui um armazenador para o recebimento e gravação de um sinal APDU de resposta a partir do dito outro cartão inteligente.
 11. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito processador ainda inclui meios de geração APDU de resposta para a geração de um sinal APDU de resposta para o dito terminal.
 12. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito cartão inteligente é fornecido com uma antena para comunicação com outro terminal.
 13. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito cartão inteligente compreende um cartão SIM (Subscriber Identity Module – módulo de identidade do subscritor), um cartão USIM (Universal Subscriber Identity Module – módulo de identidade do subscritor universal) e um cartão RUIM (Removable User Identity Module – módulo de identidade do usuário removível).
 14. **APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE**, conforme reivindicação 1, **caracterizado** por um cartão inteligente, onde o dito cartão inteligente compreende uma cartão de crédito, cartão de débito e cartão de saque.

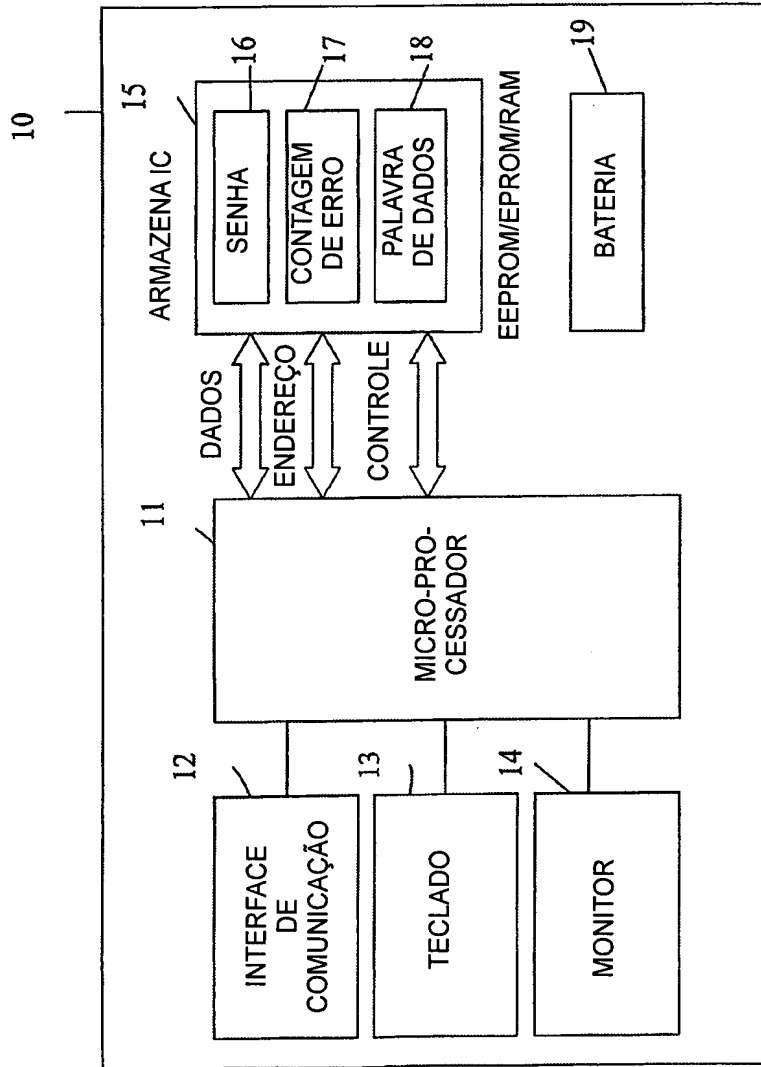


Fig. 01

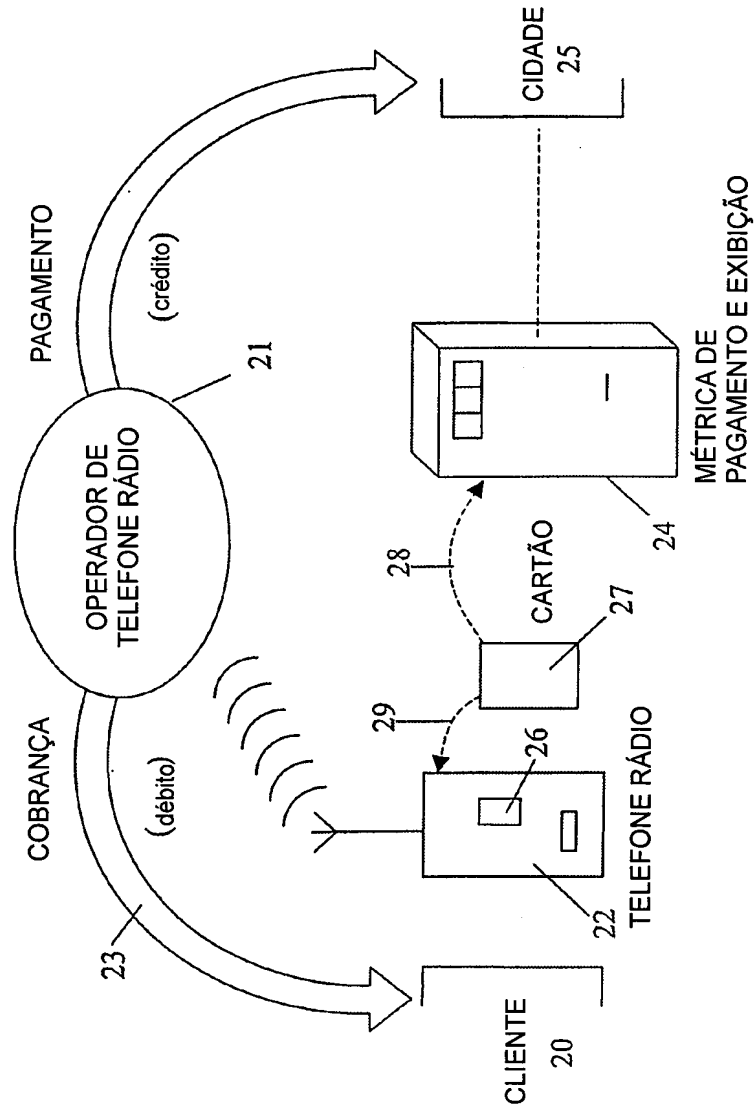


Fig. 02

e

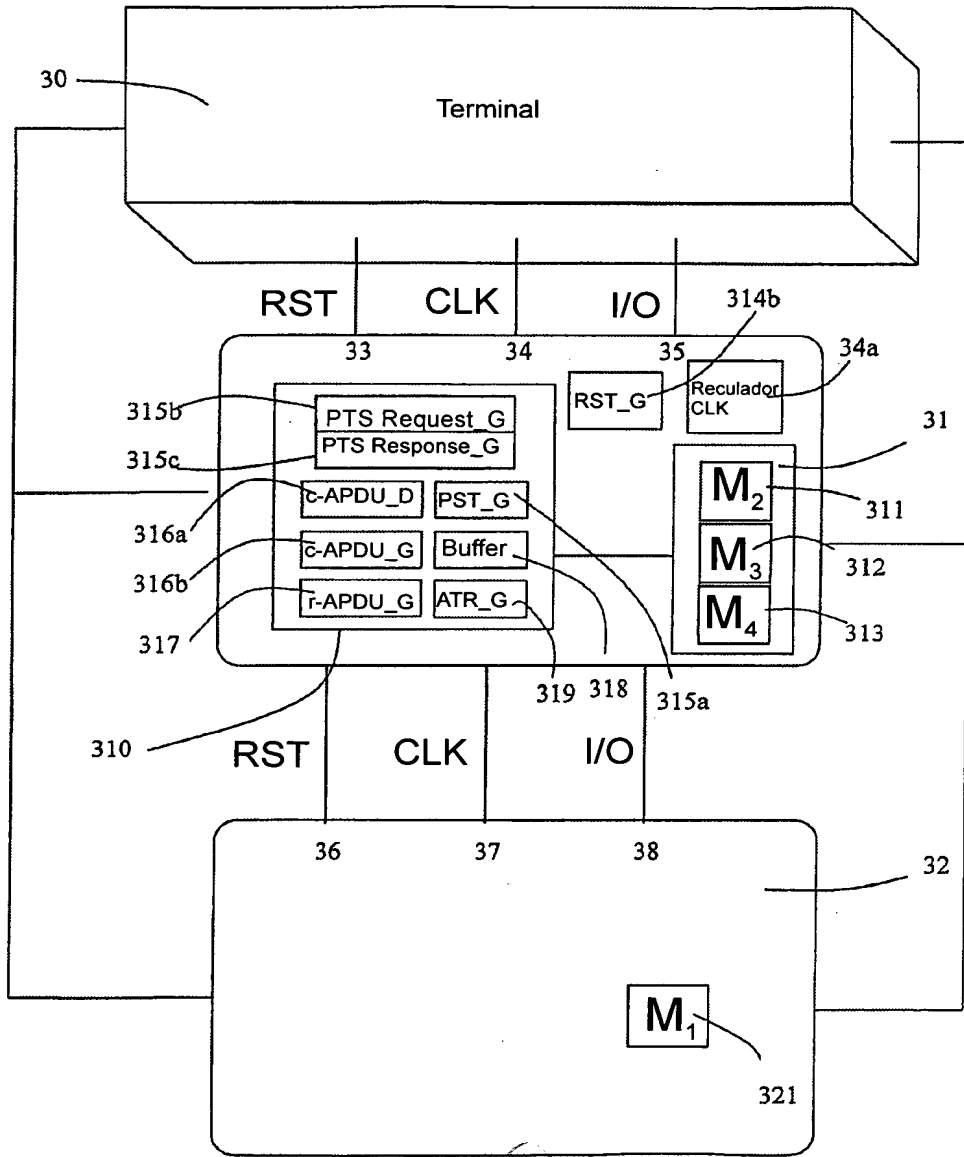


Fig. 03

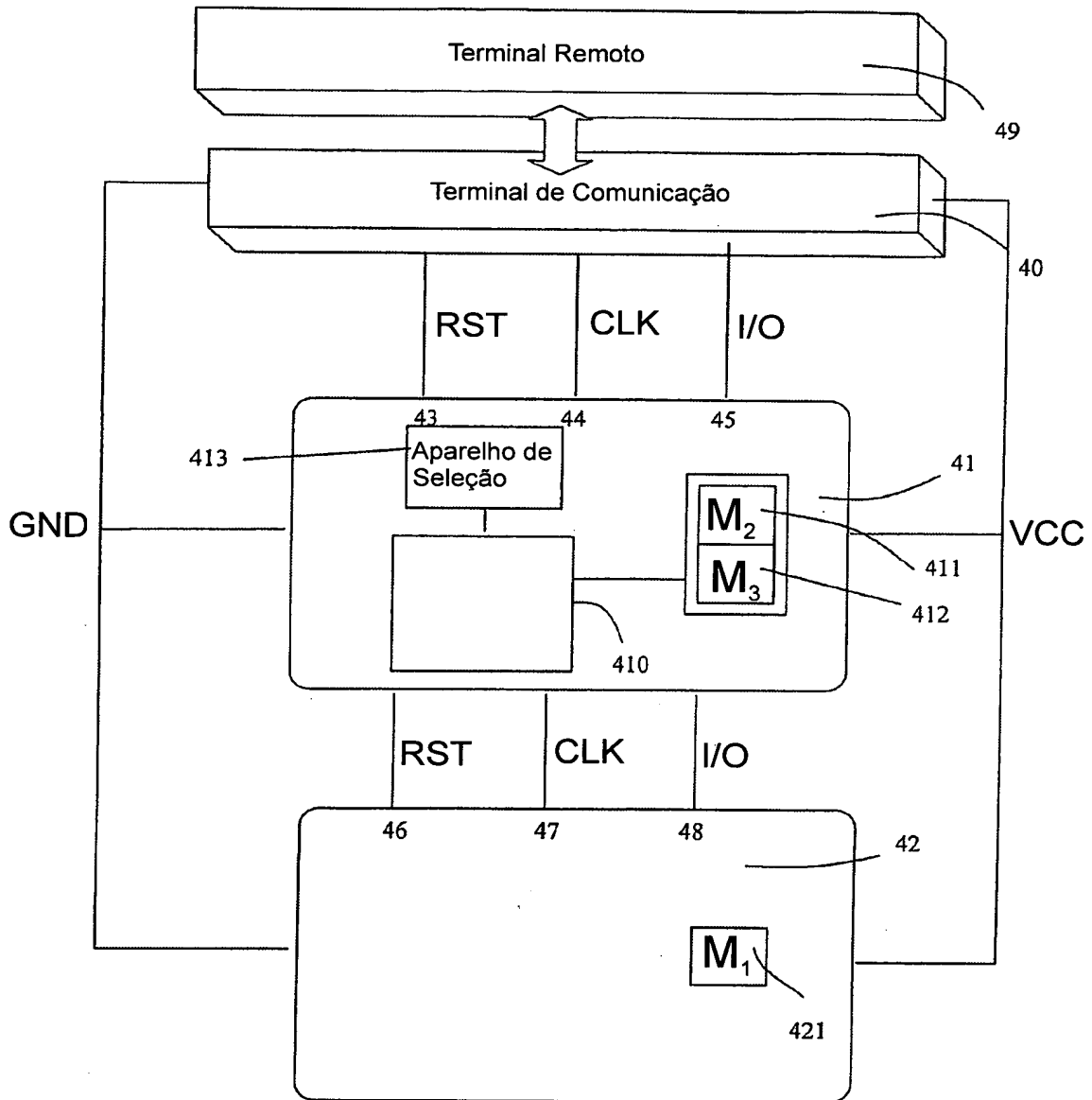


Fig. 04

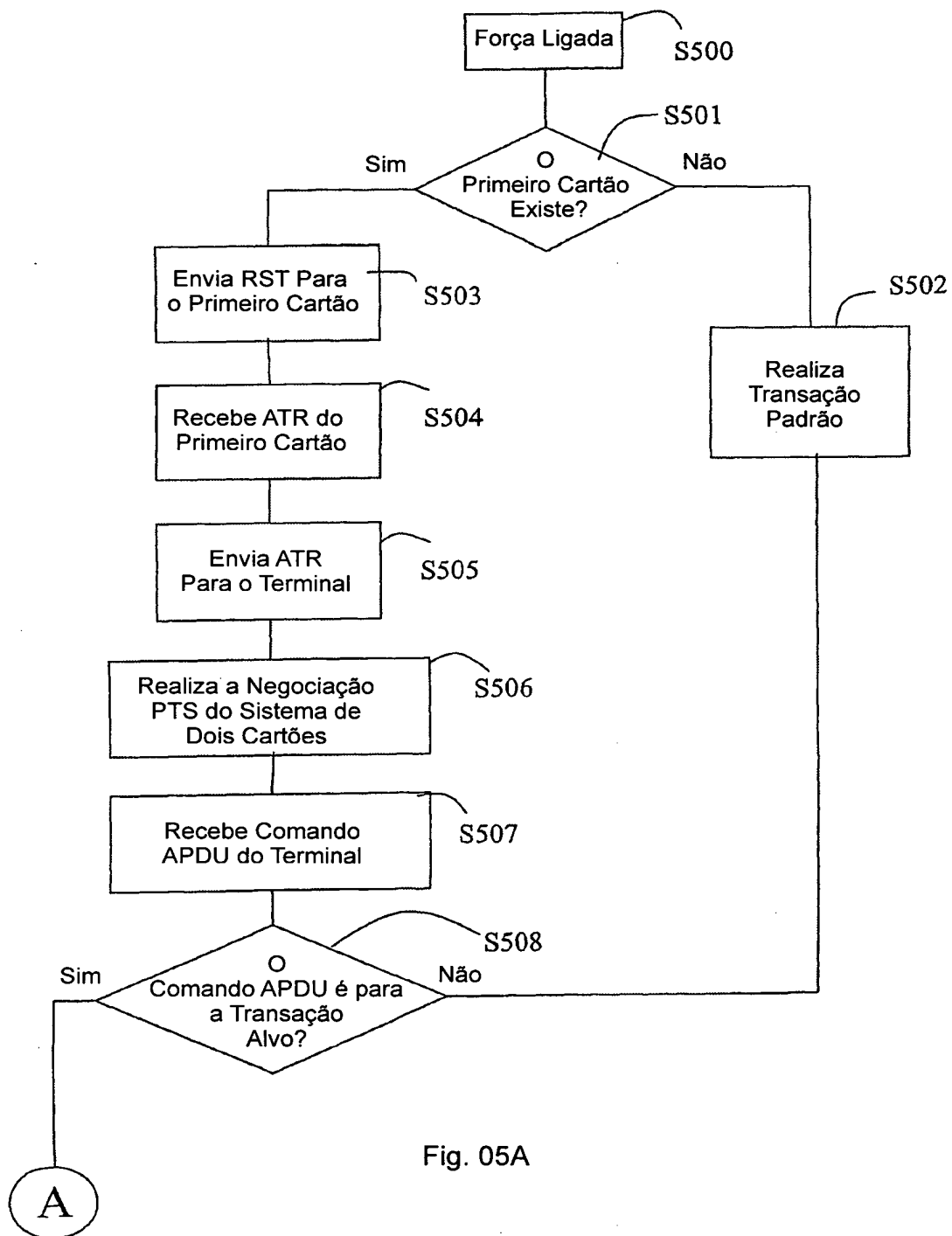


Fig. 05A

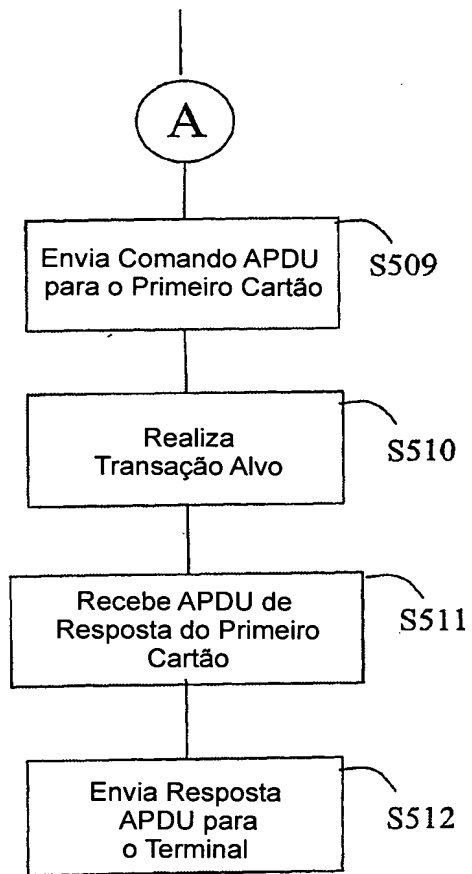


Fig. 05B

RESUMO

APERFEIÇOAMENTO INTRODUZIDO EM CARTÃO INTELIGENTE. Um cartão inteligente é revelado e inclui um processador; uma primeira interface para utilização em comunicação com um terminal; uma segunda interface para utilização em comunicação com outro cartão inteligente; e um aparelho de geração RST para a geração de um sinal para o outro cartão inteligente.