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

(21) **PI 0713974-8 A2**

BRPI0713974A2

(22) Data de Depósito: 10/07/2007
(43) Data da Publicação: 18/12/2012
(RPI 2189)

(51) Int.Cl.:
G06K 19/07
G06F 9/06

(54) Título: ESTRUTURA DE DADOS E GERENCIAMENTO EM TERMINAIS DE CARTÃO INTELIGENTE

(30) Prioridade Unionista: 14/07/2006 US 11/486.578

(73) Titular(es): Microsoft Corporation

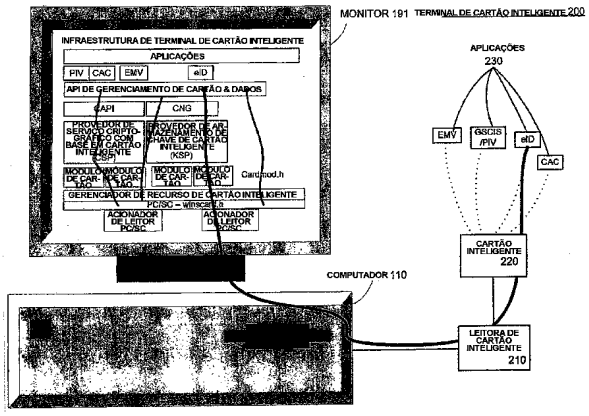
(72) Inventor(es): Shivaram H. Mysore

(74) Procurador(es): NELLIE ANNE DAIEL-SHORES

(86) Pedido Internacional: PCT US2007015706 de 10/07/2007

(87) Publicação Internacional: WO 2008/008321 de 17/01/2008

(57) Resumo: ESTRUTURA DE DADOS E GERENCIAMENTO EM TERMINAIS DE CARTÃO INTELIGENTE. Uma estrutura de dados e gerenciamento de um terminal de cartão inteligente funciona de modo a prover interoperabilidade entre o terminal de cartão inteligente e um cartão inteligente, e, em particular, entre as aplicações do terminal e o cartão. Uma interface de programa de aplicação (API) é gravada na estrutura de dados e gerenciamento, a qual faz parte de uma infra-estrutura de terminal de cartão inteligente que acessa e processa, por meio do terminal de cartão inteligente, uma aplicação de cartão inteligente contida no cartão inteligente. A interface API provê informações relativas à aplicação de cartão inteligente ao terminal a fim de permitir que uma aplicação de terminal correspondente incorpore as informações para comunicação entre as duas aplicações. Além disso, um modelo de segurança e diretivas relacionadas ao cartão inteligente podem ser cumpridos pelo terminal de cartão inteligente.



"ESTRUTURA DE DADOS E GERENCIAMENTO EM TERMINAIS DE CARTÃO INTELIGENTE"

FUNDAMENTOS

Um cartão inteligente é um cartão eletrônico que contém memória e um processador, similar a um computador, para o armazenamento, recepção, e transmissão de dados. Além de seu tamanho compacto, os cartões inteligentes são ainda desejáveis em função do fato de serem à prova de violação e de utilizarem um modelo de segurança que possibilita que dados pessoais e sensíveis sejam seguramente carregados e armazenados. Os mesmos são, com freqüência, utilizados para fins de identificação, transações financeiras, e aplicações de acesso de segurança. Outras aplicações que requerem aperfeiçoamento ou podem ser aperfeiçoadas por meio da manipulação e armazenamento seguros de dados podem da mesma forma empregar cartões inteligentes.

Um terminal de cartão inteligente vem a ser um dispositivo que aceita e lê os dados contidos em um cartão inteligente e, deste modo, acessa as aplicações armazenadas no cartão inteligente. Por exemplo, o uso de um cartão inteligente monetário em um terminal de cartão inteligente financeiro permite que dinheiro seja transferido para a conta de um usuário de cartão inteligente, e um cartão inteligente de identificação em um terminal de cartão inteligente localizado em uma instalação poderá oferecer ao usuário do cartão inteligente de identificação acesso à instalação.

Nos tempos atuais, para um cartão inteligente contendo uma ou mais de uma aplicação, existem dificuldades no sentido de se descobrir as aplicações do cartão inteligente no terminal. O terminal pode não ter ciência da interface provida e o protocolo utilizado pelas aplicações do cartão inteligente. Os itens de descoberta criam dificuldade na produção das aplicações por parte do terminal. Além disso, o modelo de segurança de um cartão inteligente não é executado no terminal. Sendo assim, torna-se altamente desejável um recurso que execute o modelo de segurança de um cartão inteligente no terminal, e que, ao mesmo tempo permita que o terminal obtenha as informações necessárias em questão para a execução das aplicações do cartão inteligente. Outros aperfeiçoamentos desejáveis relativos aos cartões inteligentes e aos terminais de cartão inteligente dizem respeito ao controle de gerenciamento de erro e uso.

SUMÁRIO

A interoperabilidade entre um cartão inteligente e um terminal de cartão inteligente que acessa uma aplicação de cartão inteligente é provida por meio de uma estrutura de dados e gerenciamento. Uma interface de programa de aplicação (API) pode ser gravada na estrutura de dados e gerenciamento, que faz parte de uma infra-estrutura de terminal de cartão inteligente. A infra-estrutura de terminal de cartão inteligente acessa, processa e implementa a aplicação de cartão inteligente contida no cartão inteligente. A interface API

provê ao terminal as informações necessárias relativas à aplicação do cartão inteligente a fim de permitir que uma correspondente aplicação de terminal se desenvolva. A correspondente aplicação de terminal pode em seguida incorporar as informações para a interoperabilidade, descoberta, e segurança entre as aplicações de terminal e de cartão inteligente. O modelo e as diretivas de segurança relacionadas ao cartão inteligente poderão ser cumpridas pelo terminal de cartão inteligente.

Esta seção de sumário é provida no sentido de apresentar, de uma maneira simplificada, uma seleção de conceitos a ser descrita em mais detalhes abaixo na seção Descrição Detalhada. O presente sumário não pretende identificar os aspectos chave ou os aspectos essenciais da matéria reivindicada nem tampouco ser usado no sentido de limitar o âmbito de aplicação da matéria reivindicada.

DESCRIÇÃO DOS DESENHOS

O sumário acima e a descrição detalhada a seguir serão mais bem entendidos quando lidos em conjunto com os desenhos em anexo. As modalidades exemplares são mostradas nos desenhos, no entanto, deve-se entender que as modalidades não se limitam aos métodos e instrumentalidades específicas aqui ilustradas. Nos desenhos:

A Figura 1 é um diagrama em blocos representando um dispositivo computacional exemplar;

A Figura 2 é um diagrama em blocos representando um terminal de cartão inteligente exemplar;

A Figura 3 é uma diagrama em blocos representando uma infra-estrutura de terminal de cartão inteligente exemplar;

A Figura 4 é um diagrama em blocos representando uma estrutura de dados e geram;

A Figura 5 é um fluxograma ilustrando uma modalidade de um método de interoperabilidade entre uma aplicação de terminal de cartão inteligente e uma aplicação de cartão inteligente em um cartão inteligente; e

A Figura 6 é um fluxograma ilustrando uma modalidade de um método de cumprimento de um modelo de segurança de um cartão inteligente em um terminal de cartão inteligente.

DESCRIÇÃO DETALHADA

Com referência à Figura 1, um sistema exemplar para a implementação da presente invenção inclui um dispositivo computacional de uso geral na forma de um computador 110. Os componentes do computador 110 podem incluir, sem, no entanto, se limitarem a, uma unidade de processamento 120, a uma memória de sistema 130, ou a um barramento de sistema 121 que acopla os vários componentes de sistema, incluindo a memória de sistema à unidade de processamento 120. O barramento de sistema 121 pode

ser qualquer um dentre diversos tipos de estruturas de barramento, incluindo um barramento de memória ou uma controladora de memória, um barramento periférico, ou um barramento local que usa qualquer uma dentre uma variedade de arquiteturas de barramento. À guisa de exemplo, e não de limitação, tais arquiteturas incluem o barramento de Arquitetura de Padrão Industrial (ISA), o barramento de Arquitetura de Micro Canal (MCA), o barramento de Arquitetura ISA Aperfeiçoada (EISA), o barramento local da Associação de Padrões Eletrônicos de Vídeo (VESA), ou o barramento de Interconexão de Componentes Periféricos (PCI), mas também conhecido como barramento Mezanino.

O computador 110 inclui tipicamente uma variedade de meios legíveis em computador. Os meios legíveis em computador podem ser quaisquer meios disponíveis que podem ser acessados pelo computador 110 e incluem meios voláteis e não voláteis, e meios removíveis e não removíveis. À guisa de exemplo, e não de limitação, os meios legíveis em computador podem compreender meios de armazenamento em computador e meios de comunicação. Os meios de armazenamento em computador incluem meios voláteis e não voláteis, e meios removíveis e não removíveis implementados em qualquer método ou tecnologia para o armazenamento de informações, como, por exemplo, instruções legíveis em computador, estruturas de dados, módulos de programa ou outros dados. Os meios de armazenamento em computador incluem, porém, não se limitam à memória RAM, à Memória ROM, à memória EEPROM, à memória flash ou a qualquer outra tecnologia de memória, CD-ROM, discos versáteis digitais (DVD) ou outro armazenamento de disco ótico, cassetes magnéticos, fita magnética, armazenamento de disco magnético ou outros dispositivos de armazenamento magnéticos, ou qualquer outro meio que possa ser usado para armazenar as informações desejadas e que possam ser acessadas pelo computador 110. Os meios de comunicação tipicamente incorporam instruções legíveis em computador, estruturas de dados, módulos de programa, ou outros dados em um sinal de dados modulado, como, por exemplo, uma onda portadora ou outro mecanismo de transporte, e incluem quaisquer meios de liberação de informação. O termo "sinal de dados modulado" significa um sinal que tem uma ou mais de suas características definidas ou modificadas de tal maneira a codificar informações no sinal. À guisa de exemplo, e não de limitação, os meios de comunicação incluem meios de conexão física, como, por exemplo, uma rede com fio ou uma conexão direta, e meios sem fio, como, por exemplo, meios acústicos, de RF, infravermelhos ou outros meios sem fio. As combinações de quaisquer dentre os meios acima devem ser também incluídas dentro do âmbito de aplicação dos meios legíveis em computador.

A memória de sistema 130 inclui um meio de armazenamento em computador na forma de uma memória volátil e/ou não volátil, como, por exemplo, a memória ROM 131 e a memória RAM 132. Um sistema básico de entrada e saída 133 (BIOS), contendo as rotinas

básicas que ajudam a transferir informações entre os elementos dentro do computador 110, como, por exemplo, durante a inicialização, fica tipicamente armazenado na memória ROM 131. A memória RAM 132 tipicamente contém dados e/ou módulos de programa que são imediatamente acessíveis à e/ou que são correntemente operados pela unidade de processamento 120. À guisa de exemplo, e não de limitação, a Figura 1 ilustra o sistema operacional 134, os programas de aplicação 135, outros módulos de programa 136, e os dados de programa 137.

O computador 110 pode incluir ainda outros meios de armazenamento em computador removíveis / não removíveis, voláteis / não voláteis. À guisa de exemplo somente, a Figura 1 ilustra uma unidade de disco rígido 141 que lê a partir de ou grava em um meio magnético não removível e não volátil, uma unidade de disco magnético 151 que lê a partir de ou grava em um disco magnético removível, não volátil 152, e uma unidade de disco ótico 155 que lê a partir de ou grava em um disco ótico removível, não volátil 156, como, por exemplo, um CD ROM ou outro meio ótico. Outros meios de armazenamento em computador removíveis / não removíveis, voláteis / não voláteis que podem ser usados no ambiente operacional exemplar incluem, porém não se limitam a, cassetes de fita magnética, cartões de memória flash, discos versáteis digitais, fita de vídeo digital, memória RAM de estado sólido, memória ROM de estado sólido, ou coisa do gênero. A unidade de disco rígido 141 é tipicamente conectada ao barramento de sistema 121 através de uma interface de memória não removível, como, por exemplo, a interface 140, e a unidade de disco magnético 151 e a unidade de disco ótico 155 são tipicamente conectadas ao barramento de sistema 121 por meio de uma interface de memória removível, como, por exemplo, a interface 150.

As unidades e seus meios de armazenamento em computador associados apresentados acima e ilustrados na Figura 1 provêm o armazenamento de instruções legíveis em computador, estruturas de dados, módulos de programa e outros dados para o computador 110. Na Figura 1, por exemplo, a unidade de disco rígido 141 é ilustrada como o sistema operacional de armazenamento 144, os programas de aplicação 145, outros módulos de programa 146, e os dados de programa 147. Observa-se que estes componentes podem ser iguais aos ou diferentes do sistema operacional 134, dos programas de aplicação 135, de outros módulos de programa 136, ou dos dados de programa 137. O sistema operacional 144, os programas de aplicação 145, os outros módulos de programa 146, e os dados de programa 147 recebem números diferentes na presente invenção a fim de ilustrar que, no mínimo, os mesmos são cópias diferentes. Um usuário pode entrar comandos e informações para o computador 110 através de dispositivos de entrada, como, por exemplo, por meio de um teclado 162 ou de um dispositivo de indicação 161, comumente referidos como mouse, um trackball ou mesa sensível ao toque.

Outros dispositivos de entrada (não mostrados) podem incluir um microfone, um joystick, uma controladora de jogos, uma antena parabólica de satélite, um leitor ótico (scanner), ou coisa do gênero. Estes e outros dispositivos de entrada são com freqüência conectados à unidade de processamento 120 através de uma interface de entrada de usuário 160 que é acoplada ao barramento de sistema, mas podem ser conectados por meio de uma outra interface e estruturas de barramento, como, por exemplo, uma porta paralela, uma porta de jogos, ou um barramento serial universal (USB). Um monitor 191 ou outro tipo de dispositivo de imagem é também conectado ao barramento de sistema 121 via uma interface, como, por exemplo, uma interface de vídeo 190. Além do monitor, os computadores podem incluir ainda outros dispositivos de saída periféricos, como, por exemplo, alto-falantes 197 e uma impressora 196, os quais podem ser conectados por meio de uma interface periférica de saída 195.

O computador 110 pode operar em um ambiente de rede utilizando conexões lógicas a um ou mais computadores remotos, como, por exemplo, um computador remoto 180. O computador remoto 180 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo de rede não hierárquica ou outro nó de rede comum, e tipicamente inclui muitos dos ou todos os elementos descritos acima com relação ao computador 110, embora apenas um dispositivo de armazenamento de memória 181 seja ilustrado na Figura 1. As conexões lógicas ilustradas incluem uma rede de área local (LAN) 171 e uma rede de área remota (WAN) 173, mas podem incluir ainda outras redes. Estes ambientes de rede são comuns em escritórios, em redes de computador empresariais, em intranets e na Internet.

Quando utilizado em um ambiente de rede LAN, o computador 110 é conectado à rede LAN 171 através de uma interface de rede ou adaptador 170. Quando utilizado em um ambiente de rede WAN, o computador 110 tipicamente inclui um modem 172 ou outro meio para o estabelecimento de comunicações pela rede WAN 173, como, por exemplo, a Internet. O modem 172, que pode ser interno ou externo, pode ser conectado ao barramento de sistema 121 via a interface de entrada de usuário 160, ou por outro mecanismo apropriado. Em um ambiente de rede, os módulos de programa ilustrados com relação ao computador 110, ou porções dos mesmos, podem ser armazenados no dispositivo de armazenamento de memória remoto. À guisa de exemplo, e não de limitação, a Figura 1 ilustra programas de aplicação remota 185 residentes no dispositivo de memória 181. Será apreciado que as conexões de rede mostradas são exemplares e outros meios para se estabelecer um enlace de comunicação entre os computadores podem ser utilizados.

Todos os métodos ou porções dos métodos descritos no presente invenção podem ser incorporados em um hardware, em um software, ou em uma combinação dos mesmos. Quando incorporados em um software, os métodos, ou certos aspectos ou porções dos

mesmos, podem ser incorporados na forma de um código de programa que, quando executado por um sistema computacional, faz com que o sistema computacional execute os métodos. Este código de programa pode ser armazenado em qualquer meio legível em computador, de acordo com o termo acima definido.

Um terminal de cartão inteligente vem a ser um dispositivo que acessa e processa as aplicações armazenadas em um cartão inteligente, que é um pequeno cartão eletrônico contendo memória e um processador. Um cartão inteligente pode ser similar a um computador, e funciona de modo a armazenar, processar, receber, e transferir dados. Um cartão inteligente pode conter uma ou mais aplicações, as quais podem ser acessadas por meio do processamento do terminal de cartão inteligente.

Um terminal de cartão inteligente exemplar 200 é mostrado na Figura 2. O terminal de cartão inteligente 200 pode incluir um computador, como, por exemplo, o computador 110, um monitor 191 ou outro tipo de dispositivo de vídeo, e uma leitora de cartão inteligente 210. A leitora de cartão inteligente 210 opera como uma interface entre o computador 110 e o cartão inteligente, como, por exemplo, o cartão inteligente 220 mostrado na Figura 2, permitindo, assim, que o computador 110 acesse e processe as aplicações 230 do cartão inteligente 220.

A leitora de cartão inteligente 210 pode ser uma leitora de cartão inteligente de proximidade ou sem contato 210, na qual o cartão inteligente 220 é lido pela leitora de cartão inteligente 210 sem nenhum contato direto entre a leitora 210 e o cartão 220. Por exemplo, a leitora de cartão inteligente de proximidade 210 pode acessar o cartão inteligente 220 quando o cartão inteligente 220 é mantido ou posicionado próximo da leitora de cartão inteligente de proximidade 210. Em uma modalidade, o padrão ISO 14443 pode ser usado de modo a definir um cartão inteligente de proximidade 220 e a leitora de cartão inteligente de proximidade 210 para compatibilidade com outros cartões 220 e leitoras 210 que aderem ao padrão ISO 14443. A leitora de cartão inteligente de proximidade 210, de acordo com o padrão, é uma leitora de identificação de radiofreqüência padrão (RFID), incluindo uma micro controladora embutida e uma antena de laço magnético a fim de ler o cartão inteligente 220. A antena de laço magnético opera a uma radiofreqüência de 13,56 MHz. A leitora de cartão inteligente de proximidade 210 pode ler o cartão inteligente de proximidade 220 quando o cartão fica a 10,16 centímetros (4 polegadas) da leitora 210. Além disso, o padrão ISO 14443 inclui quatro partes: (i) características físicas, (ii) energia de radiofreqüência e interface de sinal/ (iii) inicialização e anti-colisão; e (iv) protocolos de transmissão.

De maneira alternativa, a leitora de cartão inteligente 210 pode ser uma leitora de cartão inteligente inserível 210. Quando a leitora do cartão inteligente 210 é do tipo inserível, o acesso às aplicações 230 do cartão inteligente 220 é concedido no momento em que o

cartão inteligente 220 ou uma porção do cartão inteligente 220 é inserida na leitora de cai inserível 210. O padrão ISO 7816 é um padrão estabelecido que descreve os cartões inteligentes de contato, como, por exemplo, um cartão inteligente inserível 220. O cartão inteligente inserível 220 pode ser concebido de acordo com as exigências do padrão ISO 7816, as quais incluem os critérios relacionados aos conteúdos das mensagens, comandos, e respostas transmitidas entre o cartão 220 e a leitora 210; aos métodos de acesso aos arquivos e dados do cartão 220; e aos métodos para a troca de mensagens segura. Outros tipos de leitoras de cartão inteligente 210 podem ser empregados, não se fazendo limitação a uma leitora de cartão inteligente de proximidade 210 ou a uma leitora de cartão inteligente inserível 210.

O cartão inteligente 220 pode conter uma ou mais aplicação 230. Por exemplo, conforme mostrado na Figura 2, o cartão inteligente 220 inclui quatro aplicações 230: a aplicação EMV (Europay, MasterCard, Visa), a aplicação GSCIS/PIV, a aplicação eID, e a aplicação CAC. Outras aplicações 230 e número de aplicações 230 são possíveis. Além disso, o cartão inteligente 220 pode conter aplicações não relacionadas 230 e/ou podem, em contrapartida, conter diversas variações de uma aplicação 230. Qualquer combinação de aplicações 230 pode ser contida no cartão inteligente 220.

Uma infra-estrutura de terminal de cartão inteligente 300 de acordo com uma modalidade é mostrada na Figura 3. A infra-estrutura de terminal de cartão inteligente 300 opera no sentido de acessar, processar, e implementar as aplicações 230 do cartão inteligente 220. Além disso, a infra-estrutura 300 permite o gerenciamento de condições de erro e um modelo de uso.

A infra-estrutura de terminal de cartão inteligente 300 pode incluir vários meios, dispositivos, software, e/ou hardware para a execução de funções, inclusive as aplicações de terminal 305; uma estrutura de dados e gerenciamento 310; um componente de segurança criptográfica 320; um componente de segurança criptográfica adicional 325; um servidor provedor criptográfico base de cartão inteligente 330; um provedor de armazenamento de chave de cartão inteligente 335; um ou mais módulos de cartão 340 (como, por exemplo, os módulos de cartão 340a-d, conforme mostrado); um gerenciador de recursos de cartão inteligente 345; um PC/SC - winscard.h 350; e uma ou mais unidades de leitora 355 (como, por exemplo, a unidade de leitora 355a e 355b).

O componente de segurança criptográfica 320 permite que os programadores adicionem segurança criptográfica às aplicações, como, por exemplo, as aplicações de terminal 305. O componente de segurança criptográfica 320 permite a criação e a troca de documentos e outros dados em um ambiente seguro em um meio não seguro, por exemplo, a Internet. O componente de segurança criptográfica adicional 325 pode prover uma funcionalidade similar, porém maior, uma vez que o componente de segurança criptográfica

320. Em uma modalidade exemplar e não limitante, o componente de segurança cripta320 pode ser uma CryptoAPI. Em uma modalidade exemplar e não limitante adicional, o componente de segurança criptográfica 325 pode ser o CNG, ou uma CryptoAPI.

O servidor provedor criptográfico base de cartão inteligente 330 pode operar de modo a se comunicar com cartões inteligentes individuais, como, por exemplo, o cartão inteligente 220, através dos módulos de cartão inteligente 340. O servidor provedor criptográfico base de cartão inteligente 330 pode conter implementações de padrões e algoritmos criptográficos de modo a garantir uma segurança criptográfica. O servidor provedor criptográfico base de cartão inteligente 330 pode incluir uma biblioteca de enlace dinâmico (DLL), que pode implementar funções e servir como um facilitador de comunicação entre um sistema operacional e o servidor provedor criptográfico base de cartão inteligente 330.

Os módulos de cartão inteligente 340 podem funcionar de modo a traduzir as características de cartões inteligentes particulares ao se comunicarem com os cartões inteligentes através do gerenciador de recursos de cartão inteligente 345, em uma interface uniforme para a infra-estrutura de interface de terminal de cartão inteligente 300. O módulo de cartão inteligente 340 pode ser implementado como uma biblioteca DLL. O provedor de armazenamento chave de cartão inteligente 335 funciona de modo a executar as operações de armazenamento chave conforme requerido pela infra-estrutura de dados de terminal de cartão inteligente 300.

O gerenciador de recursos de cartão inteligente 345 pode ser responsável pela tarefa de gerenciar o acesso às leitoras de cartão inteligente 210 e aos cartões inteligentes 220. Algumas funções realizadas podem incluir a identificação e o monitoramento de recursos; a alocação de leitoras e recursos através de múltiplas aplicações; e o suporte de primitivas de transação a fim de acessar os serviços disponíveis em um dado cartão inteligente 220. O gerenciador de recursos de cartão inteligente 345 pode ser acessado diretamente através de um gerenciador de recursos de interface API ou indiretamente através de um provedor de serviço de cartão inteligente. O gerenciador de recursos de interface API é um conjunto de funções que provêm acesso direto aos serviços do gerenciador de recursos de cartão inteligente 345.

A estrutura de dados e gerenciamento 310 da infra-estrutura de terminal de cartão inteligente 300 funciona de modo a auxiliar no desenvolvimento e criação das aplicações de terminal 305. As aplicações de terminal 305 correspondem às aplicações de cartão inteligente 230. A estrutura de dados de gerenciamento 310 pode também gerenciar condições de erro, assim como um modelo de uso para a comunicação entre o terminal de cartão inteligente 200 e o cartão inteligente 220. Adicionalmente, a estrutura de dados e gerenciamento 310 pode ser uma interface de programa de aplicação (API) e, em uma

modalidade, pode ser responsável pela propagação de mensagens de erro para as aplicações de terminal 305. Uma estrutura de dados e gerenciamento 310 de acordo com uma modalidade é mostrada na Figura 4.

A estrutura de dados e gerenciamento exemplar 310 inclui vários meios, dispositivos, software e/ou hardware para a execução de funções, inclusive um componente de interface 410, um componente de gerenciamento de condição de erro 420, um componente de gerenciamento de uso 430, um componente de comunicação 440, um componente de conexão 450, e um componente de diretivas de terminal 460.

O componente de interface 410 funciona como um enlace a partir do terminal de cartão inteligente 200 para uma aplicação de cartão inteligente 230 ao obter as informações relativas à aplicação de cartão inteligente 230. As informações relacionadas à aplicação 230 podem incluir uma interface e/ou um protocolo da aplicação 230, o que poderá auxiliar o terminal 200 na identificação a acesso apropriados da aplicação 230 do cartão inteligente 220. Adicionalmente, as informações podem também ser usados no sentido de cumprir uma diretiva do cartão inteligente 220 ao tornar o terminal 200 ciente da existência e exigências da diretiva.

Uma interface API correspondente, que corresponde à aplicação de cartão inteligente 230, pode ser criada, por exemplo, por um fabricante ou programador da aplicação de cartão inteligente 230, e a interface API correspondente pode ser gravada, pelo fabricante ou programador, à estrutura de dados e gerenciamento 310. O componente de interface 410 pode usar esta interface API correspondente no sentido de criar uma aplicação de terminal 305 correspondente à aplicação de cartão inteligente 230.

O componente de gerenciamento de condição de erro 420 funciona de modo a detectar um erro relacionado ao uso do cartão inteligente 220 e, após a detecção do erro, retransmitir uma mensagem de erro correspondente. A mensagem de erro pode ser retransmitida para o componente de comunicação 440. Vários erros poderão resultar da tentativa de o terminal de cartão inteligente 200 acessar a aplicação de cartão inteligente 230 do cartão inteligente 220. Por exemplo, o cartão 220 pode ser inserido de maneira imprópria na leitora de terminal de cartão inteligente 210. quando este erro é detectado pelo componente de gerenciamento de condição de erro 420, o erro é, por conseguinte, retransmitido para o componente de comunicação 440. Um outro erro poderá resultar quando o terminal de cartão inteligente 200 tenta ler uma aplicação 230 que não se encontra no cartão inteligente 220. Mais uma vez, o componente de gerenciamento de condição de erro 420 poderá detectar este erro e em seguida operar no sentido de retransmitir uma mensagem de erro apropriada para o componente de comunicação 440 após a detecção do erro.

O componente de gerenciamento de uso 430 pode cumprir uma diretiva de uso

relativa ao cartão inteligente 220. Em uma modalidade, a diretiva de uso é o modelo de segurança para o cartão inteligente 220. A diretiva de uso pode ser incluída nas informações relacionadas à aplicação de cartão inteligente e, neste caso, poderá ser incorporada à interface API gravada na estrutura de dados e gerenciamento 310. A diretiva de uso pode ser dependente das definições de diretiva de grupo, das definições de diretiva de máquina local, ou das definições de diretiva de aplicação, por exemplo. A diretiva de uso pode ser cumprida pelo componente de gerenciamento de uso 430, o qual poderá obter a diretiva de uso e monitorar o uso do cartão inteligente 220 e suas aplicações 230. Quando a diretiva de uso definida é violada, o componente de gerenciamento de uso 430 poderá cumprir a diretiva e não permitir que a ação tentada seja processada. Além disso, o componente de gerenciamento de uso 430 pode operar no sentido de retransmitir as informações de uso, as quais poderão ser uma mensagem de violação, para o componente de comunicação 440 após a detecção de uma violação da diretiva de uso relativa ao cartão inteligente 220.

O componente de comunicação 440, para comunicação entre o cartão inteligente 220 e o terminal de cartão inteligente 200, pode ser um recurso extra da estrutura de dados e gerenciamento exemplar 310. Conforme acima mencionado, tanto o componente de gerenciamento de condição de erro 420 como o componente de gerenciamento de uso 430 podem retransmitir informações para o componente de comunicação 440. As informações recebidas podem incluir uma detecção de erro, uma violação de diretiva de uso, ou outro tipo de comunicação. Quando o componente de gerenciamento de condição de erro 420 detecta um erro relacionado ao uso do cartão inteligente 220 e envia uma indicação deste erro para o componente de comunicação 440, o componente de comunicação 440 poderá exibir no monitor 191 do terminal de cartão inteligente 200 a mensagem de erro. A mensagem de erro pode incluir instruções para um usuário do cartão inteligente 220 e para o terminal 200. O componente de comunicação 440 poderá ainda exibir uma indicação da violação da diretiva de uso relacionada ao cartão inteligente, conforme reportado pelo componente de gerenciamento de uso 430. Esta indicação poderá ainda ser exibida no monitor 191.

O componente de comunicação 440, após recebimento de uma indicação de uma condição de erro ou uma violação de uso, pode criar uma entrada de registro do erro ou violação. O componente de comunicação 440 pode enviar uma mensagem para uma aplicação, por exemplo, a fim de prover uma indicação para a aplicação da condição de erro ou violação de uso. A mensagem enviada para a aplicação pode, por exemplo, produzir um som ou tom que serve como um alerta de que a mensagem foi enviada.

Em uma modalidade, a estrutura de dados e gerenciamento 310 pode incluir ainda o componente de conexão 450, o qual pode operar no sentido de criar um canal entre a aplicação de cartão inteligente 230 e a correspondente aplicação de terminal 305 quando

nenhum erro é detectado e/ou a diretiva de uso é cumprida. O canal criado pode ser um canal seguro entre o terminal 200 e o cartão 220.

O componente de diretiva de terminal 460 pode ser incluído na estrutura de dados e gerenciamento 310 a fim de incorporar diretivas adicionais e/ou restrições no processamento da aplicação de cartão inteligente 230. Por exemplo, um programador da aplicação de terminal 305 pode desejar estabelecer um limite de tempo sobre o uso do terminal 200 para uma aplicação em particular 230. As diretivas adicionais e/ou restrições podem ser incorporadas.

A Figura 5 ilustra um método de interoperabilidade exemplar entre a aplicação de terminal de cartão inteligente 305 e a aplicação de cartão inteligente 230 em um cartão inteligente 220. O método de interoperabilidade pode ser implementado por um programador de aplicação de terminal de cartão inteligente para que a aplicação de terminal 305 opere sem restrições em uma aplicação de cartão inteligente 230 residente em um cartão inteligente 220 inserido na leitora de terminal de cartão inteligente 210.

Na referência numérica 505, é obtida uma interface API gravada em uma estrutura de dados e gerenciamento 310 do terminal de cartão inteligente 200. A interface API corresponde à aplicação de cartão inteligente 230. A fim de criar a aplicação de terminal correspondente 305, são usadas as informações relativas à aplicação de cartão inteligente 230. Na referência numérica 510, estas informações são obtidas a partir da interface API. As informações relativas à aplicação de cartão inteligente 230 podem incluir, porém, sem se limitar a, uma interface da aplicação de cartão inteligente 230, um protocolo usado pela aplicação de cartão inteligente 230, e um modelo de segurança do cartão inteligente 220. Na referência numérica 515, as informações obtidas relativas à aplicação de cartão inteligente 230 são incorporadas, por exemplo, pelo componente de interface 410 da estrutura de dados e gerenciamento 310,na aplicação de terminal 305 que corresponde à aplicação de cartão inteligente 230, várias operações de dados e gerenciamento opcionais podem ser implementadas pela estrutura de dados e gerenciamento 310.

Na referência numérica 520, o modelo de segurança do cartão inteligente 220, que pode ser obtido como parte das informações relativas à aplicação de cartão inteligente 230, poderá ser cumprido. Na referência numérica 525, a operação de cumprimento pode incluir ainda o monitoramento de um uso do cartão inteligente 220 no terminal 200. A operação de monitoramento pode ser concorrente a uma análise de um modelo de segurança, ou diretiva de uso, do cartão inteligente 220. Na referência numérica 530, é realizada uma determinação, por exemplo, pelo componente de gerenciamento de uso 430, a fim de assegurar quando o uso monitorado viola o modelo de segurança. Na referência numérica 535, quando o modelo de segurança é violado, uma mensagem de violação, neste caso, poderá ser retransmitida. A mensagem de violação pode ser retransmitida por meio da

exibição de uma mensagem no dispositivo de vídeo, como, por exemplo, no monitor 191, por meio da criação de uma entrada de registro da violação, ou por meio da transmissão de uma mensagem para uma aplicação, por exemplo. A mensagem enviada para a aplicação pode, por exemplo, produzir um som ou tom que serve como uma notificação de que a mensagem foi enviada. Qualquer combinação de retransmissão da mensagem de erro pode ser realizada.

Após a retransmissão da mensagem de violação, o método poderá voltar para a referência numérica 525 a fim de monitorar mais uma vez o uso do cartão inteligente 220. Quando, conforme determinado na referência numérica 530, o modelo não é violado, outras determinações poderão ser feitas, neste caso, a fim de determinar se o modelo de segurança foi violado posteriormente.

Na referência numérica 540, após as etapas 520 e/ou 530, quando o modelo de segurança não é violado pelo cartão inteligente 220, um canal de comunicação seguro entre o cartão inteligente 220 e o terminal de cartão inteligente 200 pode ser criado. O canal pode ser feito depois de o modelo de segurança do cartão 220 ser cumprido e/ou depois de uma determinação de que o modelo não foi violado para que o cartão inteligente 220 e o terminal 200 se comuniquem de maneira segura e realizem as funções pretendidas do cartão inteligente 220. Por exemplo, depois de a estrutura de dados e gerenciamento 310 determinar que um modelo de segurança predefinido não está sendo violado, um canal de comunicação segura pode ser criado, por exemplo, pelo componente de conexão 450.

Na referência numérica 545, a aplicação de terminal de cartão inteligente pode ser configurada de modo a definir com mais detalhes uma diretiva de terminal e/ou uma restrição de terminal. O componente de diretiva de terminal 460 pode realizar a configuração a fim de estabelecer e incorporar diretivas adicionais e/ou restrições adicionais sobre o uso do cartão inteligente 220 e/ou o processamento da aplicação de cartão inteligente 230. A configuração pode ser feita após as etapas 520, 530, quando é determinado que um modelo de segurança do cartão inteligente 220 não foi violado, e/ou 540.

A Figura 6 ilustra um método exemplar de cumprimento de um modelo de segurança de um cartão inteligente 220 sobre um terminal de cartão inteligente 200. Na referência numérica 610, o modelo de segurança do cartão inteligente 220 é obtido a partir de uma estrutura de dados e gerenciamento 310 da infra-estrutura de terminal 300. A obtenção do modelo de segurança do cartão inteligente a partir da estrutura 310 pode incluir a leitura de uma interface API aplicada ou gravada na estrutura de dados e gerenciamento 310. A estrutura de dados e gerenciamento 310 da infra-estrutura de terminal de cartão inteligente 300 pode funcionar de modo a ajudar no desenvolvimento e criação de uma aplicação de terminal 305. A aplicação de terminal 305 corresponde a uma aplicação de cartão inteligente e230.

Na referência numérica 615, o modelo de segurança é incorporado na aplicação de terminal de cartão inteligente 305, a qual é desenvolvida de modo a corresponder à aplicação de cartão inteligente 230. Na referência numérica 620, é feita uma determinação no sentido de garantir se uma condição de erro, a qual pode ser definida pelo modelo de segurança, é detectada. Esta detecção pode ser periódica ou continuamente realizada no sentido de detectar condições de erro. Na referência numérica 625, após a detecção da condição de erro na referência numérica 620, uma mensagem de erro correspondente à condição de erro detectado é transmitida. O componente de gerenciamento de condição de erro 420 pode realizar a detecção de condição de erro e pode, após a detecção de um erro, transmitir a notificação do erro para o componente de comunicação 440. O componente de comunicação 440 pode retransmitir a mensagem de erro por meio da exibição de uma mensagem correspondente em um dispositivo de vídeo, como, por exemplo, no monitor 191, por meio da criação de uma entrada de registro da violação, ou por meio da transmissão de uma mensagem para uma aplicação, por exemplo. A mensagem enviada para a aplicação pode, por exemplo, produzir um som ou tom que serve como uma notificação de que a mensagem foi enviada. Qualquer combinação de retransmissão da mensagem de erro pode ser realizada.

Como se pode apreciar, as modalidades apresentadas podem ser implementadas como um todo ou em parte em um ou mais sistemas ou dispositivos computacionais. A Figura 1 ilustra os componentes funcionais de um exemplo de um sistema computacional 100 no qual aspectos podem ser incorporados ou praticados. Conforme usado no presente documento, os termos "sistema computacional", "sistema de computador", e "computador" se referem a qualquer máquina, sistema ou dispositivo que compreenda um processador capaz de executar ou de outra forma processar códigos e/ou dados de programa. Exemplos de sistemas computacionais incluem, sem nenhuma limitação pretendida, computadores pessoais (PC), minicomputadores, computadores de grande porte, clientes magros, PC de rede, servidores, estações de trabalho, computadores do tipo laptop, computadores portáteis, equipamentos eletrônicos programáveis pelo consumidor, consoles de multimídia, consoles de jogo, receptores de satélite, conversores do tipo set-top box (aparelhos decodificadores), máquinas contadoras automáticas (caixas bancárias eletrônicas), jogos de videogame do tipo arcade, telefones móveis, assistentes digitais pessoais (PDA) ou qualquer outro sistema ou máquina baseada em processador. Os termos "código de programa" e "código" referem-se a qualquer conjunto de instruções executadas ou de outra forma processadas por um processador. O código de programa e/ou dados de programa podem ser implementados na forma de rotinas, programas, objetos, estruturas de dados ou coisa do gênero que realizam funções particulares.

Nota-se que os exemplos acima foram providos tão-somente para os fins de

explanação e de forma alguma devem ser construídos como limitantes. Embora as invenções tenham sido descritas com referência a várias modalidades, deve-se entender que as palavras utilizadas no presente documento são palavras de descrição e ilustração, ao invés de palavras de limitação. Além disso, embora as modalidades tenham sido descritas no presente documento com referência a meios, materiais, e exemplos particulares, as modalidades não pretendem ficar limitadas às particularidades aqui apresentadas; ao contrário, as modalidades se estendem a todas as estruturas, métodos e usos funcionalmente equivalentes, tais como as que se encontram dentro do âmbito de aplicação das reivindicações em apenso.

REIVINDICAÇÕES

1. Infra-estrutura de terminal de cartão inteligente (300) para um terminal de cartão inteligente (200), a infra-estrutura de terminal (300) sendo **CARACTERIZADA** pelo fato de que compreende:

- uma estrutura de dados e gerenciamento (310), em que a estrutura (310) compreende:

- um componente de interface (410) para a obtenção de informações relativas a uma aplicação de cartão inteligente (230) em um cartão inteligente (220);

- um componente de gerenciamento de condição de erro (420) de modo a detectar um erro do cartão inteligente (220);

- um componente de gerenciamento de uso (430) para o cumprimento de uma diretiva de uso relacionada ao cartão inteligente (220); e

- um componente de comunicação (440) para a comunicação entre o cartão inteligente (220) e o terminal de cartão inteligente (220).

2. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que a estrutura de dados e gerenciamento (310) é uma interface de programa de aplicação (API).

3. Infra-estrutura de terminal de cartão inteligente, de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que as informações relativas à aplicação de cartão inteligente (230) no cartão inteligente (220) é pelo menos de (i) uma interface da aplicação de cartão inteligente (230); (ii) um protocolo usado pela aplicação de cartão inteligente (230); e (iii) um modelo de segurança do cartão inteligente (220).

4. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que compreende ainda:

- um módulo de cartão (340) para a provisão das informações relativas à aplicação de cartão inteligente (230) no cartão inteligente (220) para a estrutura de dados e gerenciamento (310).

5. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 4, **CARACTERIZADA** pelo fato de que compreende ainda:

- uma aplicação de terminal (305) correspondente à aplicação de cartão inteligente (230) e criada a partir das informações relativas à aplicação de cartão inteligente (230) no cartão inteligente (220).

6. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que o componente de gerenciamento de condição de erro (420) opera ainda no sentido de retransmitir uma mensagem de erro para o componente de comunicação (440) após a detecção do erro.

7. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a

reivindicação 6, **CARACTERIZADA** pelo fato de que o componente de comunicação (440) retransmite a mensagem de erro do terminal de cartão inteligente (200) por meio de pelo menos um dentre (i) a exibição da mensagem de erro em um dispositivo de vídeo (191); (ii) a criação de uma entrada de registro correspondente à mensagem de erro; e (iii) o envio da mensagem de erro para uma aplicação.

8. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que o componente de gerenciamento de uso (43) opera ainda no sentido de retransmitir as informações de uso para o componente de comunicação (440) após a detecção de uma violação da diretiva de uso relacionada ao cartão inteligente (220).

9. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 8, **CARACTERIZADA** pelo fato de que o componente de comunicação (440) retransmite uma indicação da violação da diretiva de uso relativa ao cartão inteligente (220) por meio de pelo menos um dentre (i) a exibição da indicação da violação em um dispositivo de vídeo (191); (ii) a criação de uma entrada de registro correspondente à violação; e (iii) o envio da indicação da violação para uma aplicação.

10. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que compreende ainda:

- um componente de conexão (450) para a criação de um canal entre a aplicação de cartão inteligente (230) e uma aplicação de terminal correspondente (305) quando nenhum erro é detectado ou a diretiva de uso é cumprida.

11. Infra-estrutura de terminal de cartão inteligente (300), de acordo com a reivindicação 1, **CARACTERIZADA** pelo fato de que compreende ainda:

- um componente de diretiva de terminal (460) para a incorporação de diretivas de terminal ou de restrições relativas ao processamento da aplicação de cartão inteligente (230).

12. Método de interoperabilidade entre uma aplicação de terminal de cartão inteligente (305) e uma aplicação de cartão inteligente (230) em um cartão inteligente (220), o método sendo **CARACTERIZADO** pelo fato de que compreende as etapas de:

- obter uma interface de programa de aplicação (API) gravada na estrutura de um terminal de cartão inteligente (505);

- obter as informações relativas à aplicação de cartão inteligente da interface API (510); e

- incorporar as informações relativas à aplicação de cartão inteligente na aplicação de terminal de cartão inteligente (515).

13. Método de interoperabilidade, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que a etapa de obter as informações relativas à aplicação

de cartão inteligente da interface API (510) compreende a obtenção de pelo menos um dentre (i) uma interface da aplicação de cartão inteligente; (ii) um protocolo usado pela aplicação de cartão inteligente; e (iii) um modelo de segurança do cartão inteligente.

14. Método de interoperabilidade, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende ainda a etapa de:

- cumprir o modelo de segurança do cartão inteligente no terminal de cartão inteligente (520).

15. Método de interoperabilidade, de acordo com a reivindicação 14, **CARACTERIZADO** pelo fato de que o cumprimento do modelo de segurança do cartão inteligente (520) compreende:

- o monitoramento do uso do cartão inteligente (525); e

- após a determinação de que o uso monitorado viola o modelo de segurança (530), a indicação de uma mensagem de violação (535).

16. Método de interoperabilidade, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende ainda a etapa de:

- criar um canal de comunicação segura entre o cartão inteligente e o terminal de cartão inteligente (540).

17. Método de interoperabilidade, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que compreende ainda a etapa de:

- configurar a aplicação de terminal de cartão inteligente de modo a definir ainda uma diretiva de terminal ou uma restrição (545).

18. Método de cumprimento de um modelo de segurança de cartão inteligente, o método sendo **CARACTERIZADO** pelo fato de que compreende as etapas de:

- obter o modelo de segurança do cartão inteligente a partir de uma estrutura de dados e gerenciamento do terminal de cartão inteligente (610); e

- incorporar o modelo de segurança em uma aplicação de terminal de cartão inteligente correspondente ao cartão inteligente (615).

19. Método, de acordo com a reivindicação 18, **CARACTERIZADO** pelo fato de que a obtenção do modelo de segurança do cartão inteligente a partir de uma estrutura de dados e gerenciamento do terminal de cartão inteligente compreende a leitura da interface de programa de aplicação (API) aplicada à estrutura de dados e gerenciamento.

20. Método, de acordo com a reivindicação 18, **CARACTERIZADO** pelo fato de que compreende ainda as etapas de:

- detectar uma condição de erro definida pelo modelo de segurança (620); e

- transmitir uma mensagem de erro correspondente à condição de erro (625).

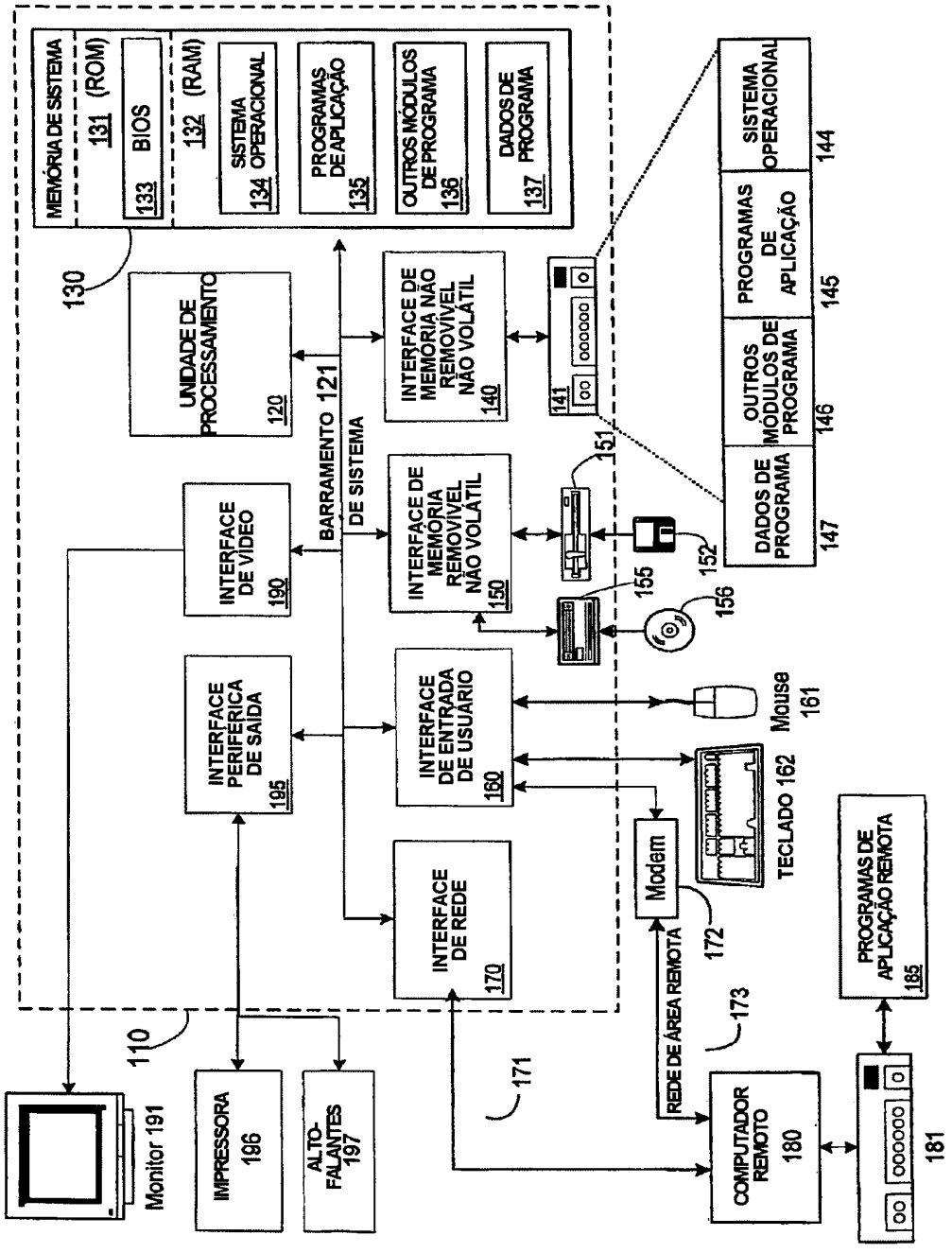

AMBIENTE COMPUTACIONAL
100
MEMÓRIA DE SISTEMA
131 (ROM)
BIOS
133
132 (RAM)
SISTEMA OPERACIONAL
134
PROGRAMAS DE APLICAÇÃO
135
OUTROS MÓDULOS DE PROGRAMA
136
DADOS DE PROGRAMA
137
130
UNIDADE DE PROCESSAMENTO
120
BARRAMENTO DE SISTEMA
121
INTERFACE DE MEMÓRIA NÃO REMOVÍVEL NÃO VOLÁTIL
140
141
151
INTERFACE DE VÍDEO
190
INTERFACE DE MEMÓRIA REMOVÍVEL NÃO VOLÁTIL
150
155
152
156
INTERFACE PERIFÉRICA DE SAÍDA
195
INTERFACE DE ENTRADA DE USUÁRIO
160
Mouse
161
TECLADO 162
INTERFACE DE REDE
170
Modem
172
171
173
REDE DE ÁREA REMOTA
110
Monitor 191
IMPRESSORA
196
ALTO-FALANTES
197
COMPUTADOR REMOTO
180
181
PROGRAMAS DE APLICAÇÃO REMOTA
185
SISTEMA OPERACIONAL
144
PROGRAMAS DE APLICAÇÃO
145
OUTROS MÓDULOS DE PROGRAMA
146
DADOS DE PROGRAMA
147

FIG. 1

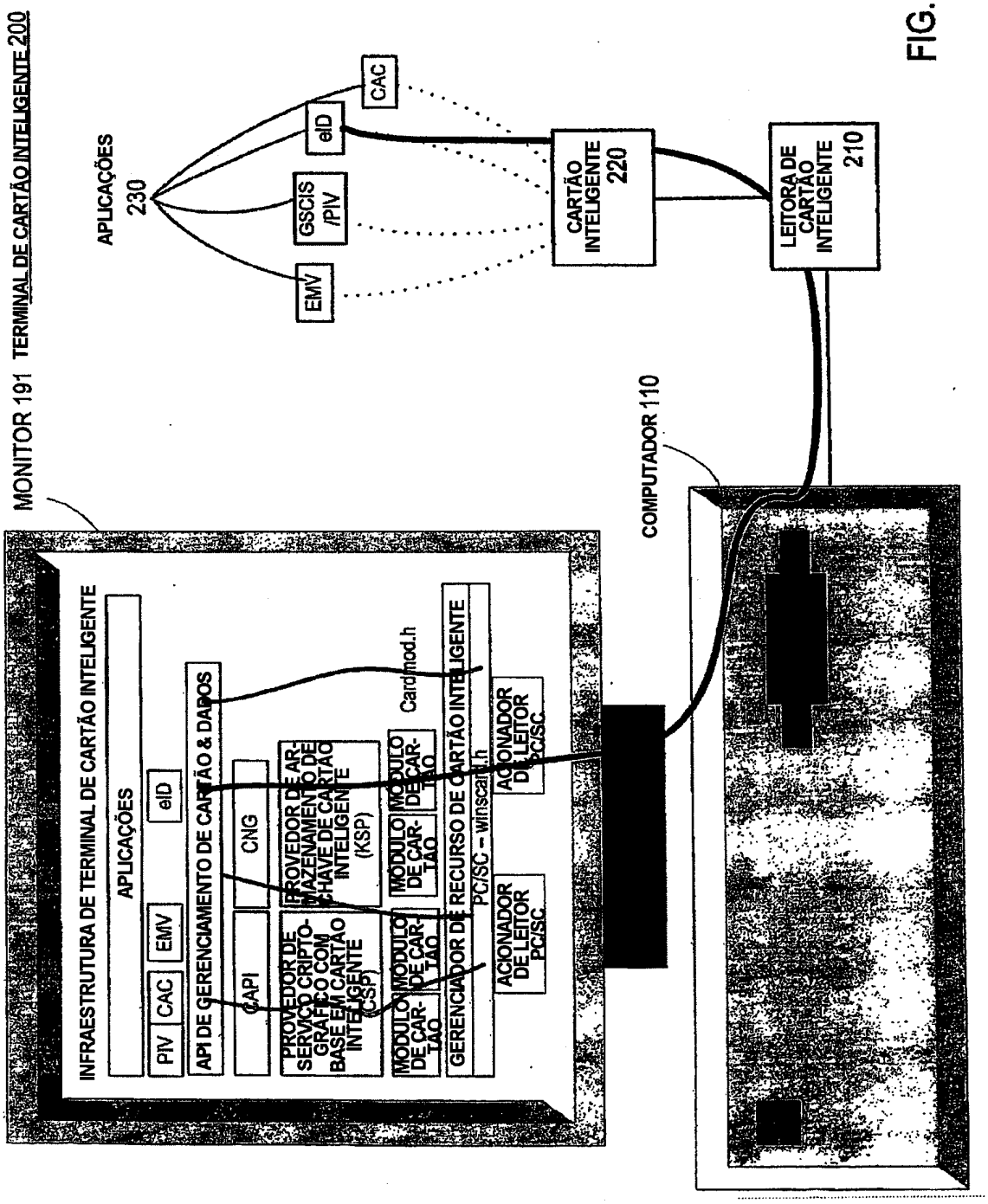

MONITOR 191 TERMINAL DE CARTÃO INTELIGENTE 200
INFRAESTRUTURA DE TERMINAL DE CARTÃO INTELIGENTE
APLICAÇÕES
PIV
CAC
EMV
eID
API DE GERENCIAMENTO DE CARTÃO & DADOS
CAPI
CNG
PROVEDOR DE SERVIÇO CRIPTOGRÁFICO COM BASE EM CARTÃO INTELIGENTE (CSP)
PROVEDOR DE ARMAZENAMENTO DE CHAVE DE CARTÃO INTELIGENTE (KSP)
MÓDULO DE CARTÃO
MÓDULO DE CARTÃO
MÓDULO DE CARTÃO
Cardmod.h
GERENCIADOR DE RECURSO DE CARTÃO INTELIGENTE
PC/SC – winscard.h
ACIONADOR DE LEITOR PC/SC
ACIONADOR DE LEITOR PC/SC
APLICAÇÕES
230
EMV
GSCIS /PIV
eID
CAC
CARTÃO INTELIGENTE 220
LEITORA DE CARTÃO INTELIGENTE 210
COMPUTADOR 110

FIG. 2

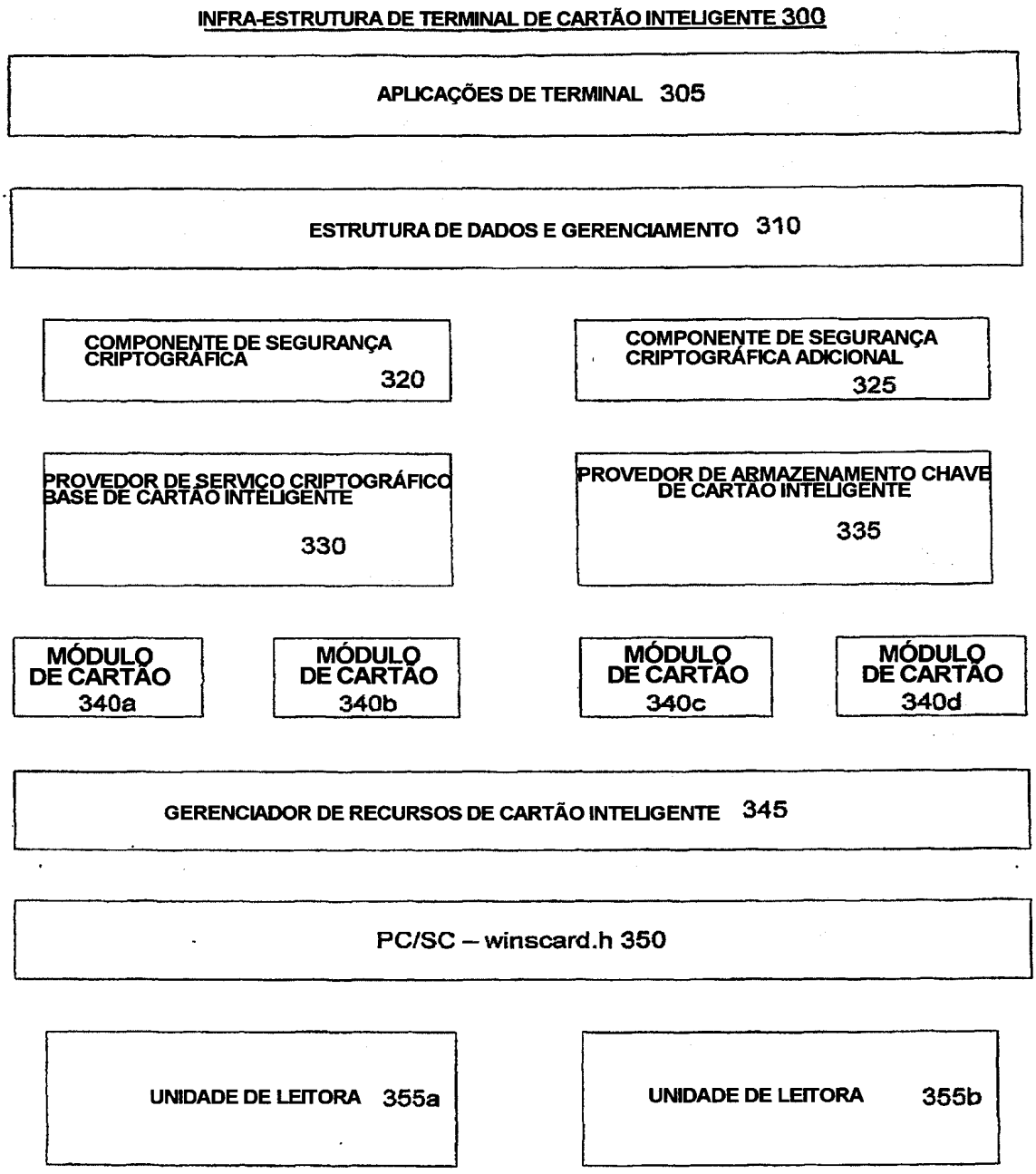

INFRA-ESTRUTURA DE TERMINAL DE CARTÃO INTELIGENTE 300
APLICAÇÕES DE TERMINAL 305
ESTRUTURA DE DADOS E GERENCIAMENTO 310
COMPONENTE DE SEGURANÇA CRIPTOGRÁFICA 320
COMPONENTE DE SEGURANÇA CRIPTOGRÁFICA ADICIONAL 325
PROVEDOR DE SERVIÇO CRIPTOGRÁFICO BASE DE CARTÃO INTELIGENTE 330
PROVEDOR DE ARMAZENAMENTO CHAVE DE CARTÃO INTELIGENTE 335
MÓDULO DE CARTÃO 340a
MÓDULO DE CARTÃO 340b
MÓDULO DE CARTÃO 340c
MÓDULO DE CARTÃO 340d
GERENCIADOR DE RECURSOS DE CARTÃO INTELIGENTE 345
PC/SC – winscard.h 350
UNIDADE DE LEITORA 355a
UNIDADE DE LEITORA 355b

FIG. 3

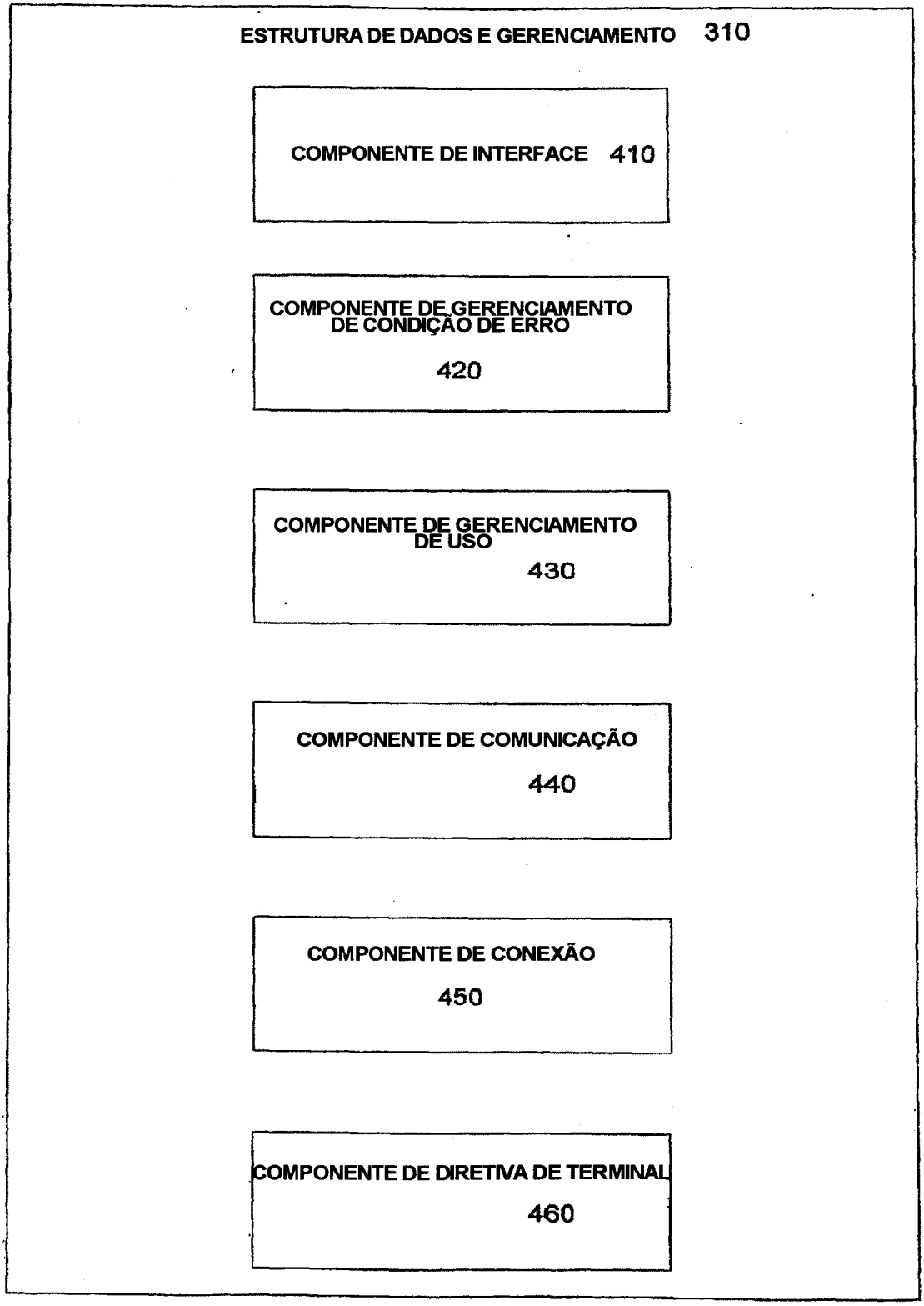

ESTRUTURA DE DADOS E GERENCIAMENTO 310
COMPONENTE DE INTERFACE 410
COMPONENTE DE GERENCIAMENTO DE CONDIÇÃO DE ERRO 420
COMPONENTE DE GERENCIAMENTO DE USO 430
COMPONENTE DE COMUNICAÇÃO 440
COMPONENTE DE CONEXÃO 450
COMPONENTE DE DIRETIVA DE TERMINAL 460

FIG. 4

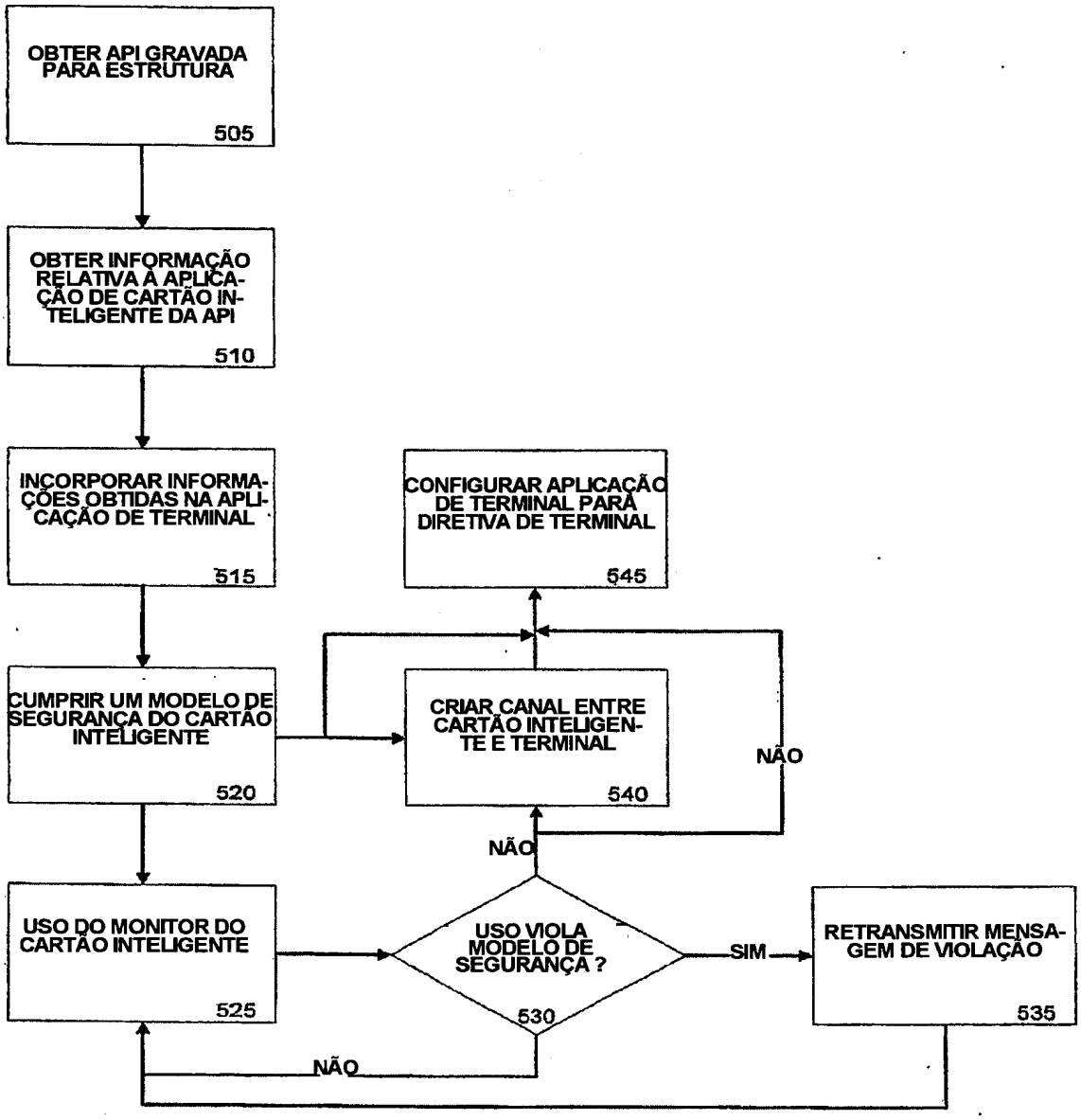

OBTER API GRAVADA PARA ESTRUTURA
505
OBTER INFORMAÇÃO RELATIVA À APLICAÇÃO DE CARTÃO INTELIGENTE DA API
510
INCORPORAR INFORMAÇÕES OBTIDAS NA APLICAÇÃO DE TERMINAL
515
CONFIGURAR APLICAÇÃO DE TERMINAL PARA DIRETIVA DE TERMINAL
545
CUMPRIR UM MODELO DE SEGURANÇA DO CARTÃO INTELIGENTE
520
CRIAR CANAL ENTRE CARTÃO INTELIGENTE E TERMINAL
540
NÃO
NÃO
USO DO MONITOR DO CARTÃO INTELIGENTE
525
USO VIOLA MODELO DE SEGURANÇA ?
530
SIM
RETRANSMITIR MENSAGEM DE VIOLAÇÃO
535
NÃO

FIG. 5

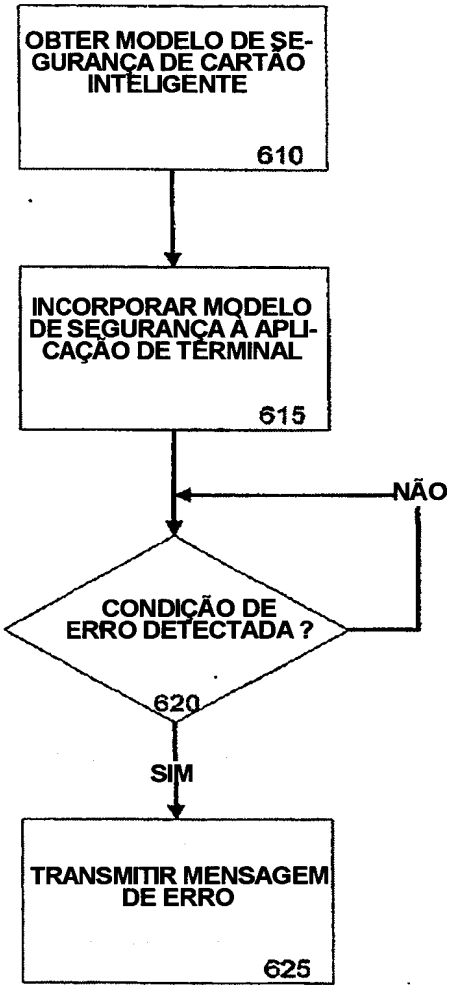

OBTER MODELO DE SEGURANÇA DE CARTÃO INTELIGENTE
610
INCORPORAR MODELO DE SEGURANÇA À APLICAÇÃO DE TERMINAL
615
NÃO
CONDIÇÃO DE ERRO DETECTADA ?
620
SIM
TRANSMITIR MENSAGEM DE ERRO
625

FIG. 6

RESUMO

"ESTRUTURA DE DADOS E GERENCIAMENTO EM TERMINAIS DE CARTÃO INTELIGENTE"

Uma estrutura de dados e gerenciamento de um terminal de cartão inteligente funciona de modo a prover interoperabilidade entre o terminal de cartão inteligente e um cartão inteligente, e, em particular, entre as aplicações do terminal e o cartão. Uma interface de programa de aplicação (API) é gravada na estrutura de dados e gerenciamento, a qual faz parte de uma infra-estrutura de terminal de cartão inteligente que acessa e processa, por meio do terminal de cartão inteligente, uma aplicação de cartão inteligente contida no cartão inteligente. A interface API provê informações relativas à aplicação de cartão inteligente ao terminal a fim de permitir que uma aplicação de terminal correspondente incorpore as informações para comunicação entre as duas aplicações. Além disso, um modelo de segurança e diretivas relacionadas ao cartão inteligente podem ser cumpridos pelo terminal de cartão inteligente.