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

(21) **PI0609123-7 A2**

* B R P I 0 6 0 9 1 2 3 A 2 *

(22) Data de Depósito: 05/04/2006
(43) Data da Publicação: 23/02/2010
(RPI 2042)

(51) Int.Cl.:
H04L 9/00 (2010.01)
H04K 1/00 (2010.01)

(54) Título: **AUTENTICAÇÃO DE UNIDADE DE DISCO RÍGIDO**

(30) Prioridade Unionista: 13/04/2005 US 11/106.393

(73) Titular(es): MICROSOFT CORPORATION

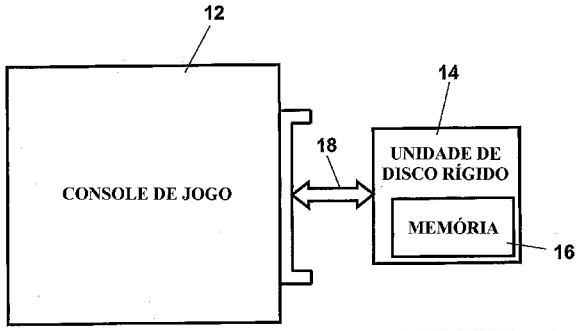
(72) Inventor(es): HEDLEY C. DAVIS, PRAKASH R. STIRRET

(74) Procurador(es): NELLIE ANNE DANIEL SHORES

(86) Pedido Internacional: PCT US2006012931 de 05/04/2006

(87) Publicação Internacional: WO 2006/113160de 26/10/2006

(57) Resumo: AUTENTICAÇÃO DE UNIDADE DE DISCO RÍGIDO. Trata-se de um console de jogo que determina, pela análise de um certificado criptografado, se uma unidade de disco rígido está autorizada para uso com o console de jogo. O certificado criptografado é armazenado na memória da unidade. Quando a unidade é detectada, o console de jogo recebe o certificado criptografado e o descriptografa. O certificado contém parâmetros com relação à unidade, tal como o número de série da unidade, o número de modelo da unidade, a capacidade de memória da unidade, e uma marca registrada que indica a autenticidade da unidade, por exemplo. O console de jogo também recebe esses parâmetros da unidade na forma não criptografada. Os parâmetros extraídos do certificado criptografado são comparados com os parâmetros lídos da memória da unidade de disco rígido. Se os parâmetros se corresponderem, a unidade é determinada como autêntica. O certificado é críptografado com uma chave privada de um par de chaves pública-privada e descríptografado com a chave pública correspondente de acordo com as técnicas criptográficas de chave pública bem conhecidas.



"AUTENTICAÇÃO DE UNIDADE DE DISCO RÍGIDO"

CAMPO DA INVENÇÃO

A presente invenção se refere em geral a sistemas de jogos e, mais especificamente, se refere à autenticação de periféricos de consoles de jogo, tais como unidades de disco rígido.

ANTECEDENTES DA INVENÇÃO

Os sistemas de jogos que incluem consoles capazes de serem acoplados a dispositivos periféricos externos, tais como unidades de disco rígido, por exemplo, estão suscetíveis a vários problemas. Diferentes fornecedores podem fornecer os dispositivos externos e os consoles de jogo. Portanto, é possível que os dispositivos externos não sejam compatíveis com os consoles. Um possível problema decorrente dessa situação é que a conexão entre um dispositivo externo e um console poderia danificar o console e/ou o dispositivo externo. Também é possível, independente da compatibilidade entre um determinado console e dispositivo externo, que o uso abundante desse par passe a impressão de um sistema de baixa qualidade. Além disso, o uso de dispositivos externos de um fabricante com consoles de jogo de outro fabricante poderia passar a impressão de que os produtos de um dos fabricantes são de baixa qualidade. Isso poderia resultar em perda de receita/lucro por parte de pelo menos um dos fabricantes.

Sendo assim, é necessário um sistema de jogo capaz de determinar se um dispositivo periférico externo está autorizado para utilização com um console de jogo.

SUMÁRIO DA INVENÇÃO

Em uma concretização exemplificativa da presente invenção, os dispositivos periféricos externos para uso em consoles de jogo são autorizados por meio do uso de certificados criptografados. Um certificado criptografado é armazenado na memória de um dispositivo periférico externo de console de jogo. Quando o console de jogo detecta o dispositivo externo, o certificado criptografado é recebido pelo console de jogo e descriptografado. O conteúdo do certificado descriptografado é analisado para determinar a autenticidade do dispositivo externo. Se o dispositivo externo for determinado como autêntico, serão permitidas operações normais. Se o dispositivo externo não for determinado como autêntico, as interações subseqüentes entre o dispositivo externo e o console de jogo serão proibidas.

O certificado compreende parâmetros com relação ao dispositivo externo. Os parâmetros de dispositivo podem incluir a ID do dispositivo, o número de série do dispositivo, o número de modelo do dispositivo, e/ou a capacidade de memória do dispositivo, por exemplo. Em uma concretização, o certificado compreende uma marca, tal como uma marca registrada com uma imagem, por exemplo, que indica a autenticidade do dispositivo externo. O certificado é criptografado com uma chave privada de um par de chaves pública-privada de acordo com as técnicas criptográficas de chave pública bem conhecidas. Os parâmetros não criptografados do dispositivo e o certificado criptografado são armazenados na memória do dispositivo externo. A marca não criptografada é armazenada

no console de jogo.

Quando o console de jogo, estando ligado ou em outro momento apropriado, detecta o dispositivo externo, o console de jogo lê, do dispositivo externo, os parâmetros não criptografados deste. O console de jogo também lê o certificado criptografado do dispositivo externo. Em seguida, o certificado criptografado é descriptografado com a chave pública correspondente do par de chaves pública-privada. Em uma concretização exemplificativa da presente invenção, a chave pública é armazenada no console de jogo. Os componentes do certificado descriptografado, como por exemplo, os parâmetros do dispositivo externo e a marca, são comparados com os parâmetros não criptografados de dispositivo lidos do dispositivo externo e com a marca lida do console de jogo. Se as comparações indicarem que os parâmetros do dispositivo e as marcas são os mesmos, o dispositivo externo é determinado como autêntico. Se as comparações indicarem que os parâmetros de dispositivo e as marcas não são os mesmos, o dispositivo externo não é determinado como autêntico.

BREVE DESCRIÇÃO DOS DESENHOS

O precedente e outros objetivos, aspectos e vantagens serão melhor compreendidos com base na descrição detalhada a seguir com referência aos desenhos, em que:

A Figura 1 é uma representação de um sistema de jogo compreendendo um console de jogo e um dispositivo periférico externo de acordo com uma concretização exemplificativa da presente invenção;

A Figura 2 é um diagrama da unidade de disco rígi-

do compreendendo parâmetros de dispositivo e um certificado criptografado armazenado na memória, de acordo com uma concretização exemplificativa da presente invenção;

A Figura 3 é uma representação de um certificado de acordo com uma concretização exemplificativa da presente invenção;

A Figura 4 é um diagrama de fluxo de dados de um processo de autenticação de acordo com uma concretização exemplificativa da presente invenção;

A Figura 5 é uma continuação da Figura 4; e

A Figura 6 ilustra um exemplo de um ambiente de sistema de computação adequado, no qual uma concretização exemplificativa da presente invenção pode ser implementada.

DESCRIÇÃO DETALHADA DAS CONCRETIZAÇÕES ILUSTRATIVAS

A Figura 1 é uma representação de um sistema de jogo compreendendo um console de jogo 12 e um dispositivo periférico externo 14 de acordo com uma concretização exemplificativa da presente invenção. Os sistemas de jogos são conhecidos na técnica. Um exemplo de sistema de jogo conhecido é o sistema de jogo Xbox® da Microsoft Corporation. Conforme descrito neste documento, o dispositivo periférico externo 14 é caracterizado como uma unidade de disco rígido, mas não deve ser limitado a isto. O dispositivo periférico externo pode incluir qualquer dispositivo externo apropriado que possua memória, tal como outros tipos de dispositivos externos de memória (por exemplo, unidades de disco óptico, cartões *memory stick*), controladores de jogo, meios de exi-

bição, ou uma combinação desses, por exemplo. A unidade externa de disco rígido 14 pode ser acoplada ao console de jogo 12, de tal maneira que a unidade externa de disco rígido 14 fique em comunicação com o console de jogo 12. A seta 18 indica os meios de comunicação entre o console de jogo 12 e a unidade de disco rígido 14. Os meios de comunicação 18 podem compreender quaisquer meios de comunicação apropriados, tais como meios de comunicação fisicamente conectados, um meio de comunicação sem fio (por exemplo, infravermelho, eletromagnético), um meio de comunicação mecânico/elétrico (por exemplo, uma conexão de pino e encaixe, uma conexão USB), um meio de comunicação óptico, ou uma combinação desses, por exemplo. Em uma concretização exemplificativa da invenção, os meios de comunicação 18 estão de acordo com a bem conhecida especificação de interface Serial ATA (SATA). A unidade de disco rígido 14 compreende meios de armazenamento, tais como a memória 16.

A Figura 2 é um diagrama da unidade de disco rígido 14 compreendendo parâmetros de dispositivo 20 e um certificado criptografado 24 armazenado na memória 16, de acordo com uma concretização exemplificativa da presente invenção. A memória 16 armazena parâmetros de dispositivo 20 relativos à unidade de disco rígido particular 14. Os parâmetros de dispositivo 20 podem incluir qualquer parâmetro apropriado relativos à unidade de disco rígido 14. Os parâmetros apropriados 20 incluem um número de identificação da unidade de disco rígido 14, um número de série da unidade de disco rígido 1, um número de modelo da unidade de disco rígido 14, a

capacidade de memória da memória 16 na unidade de disco rígido 14, ou uma combinação desses, por exemplo. Os parâmetros de dispositivo 20 são armazenados na memória 16 na forma não criptografada. Imagina-se que os parâmetros de dispositivo 20 sejam armazenados na memória 16 pelo fornecedor da unidade de disco rígido 14. Em uma concretização exemplificativa da presente invenção, os parâmetros de dispositivo 20 são armazenados na memória somente para leitura (ROM), ou semelhante, impedindo assim acesso e/ou modificação desses parâmetros. Imagina-se que a capacidade de memória seja a quantidade de memória disponível a um usuário. Sendo assim, deve-se compreender que a capacidade da memória 16 pode depender de onde os parâmetros de dispositivo 20 estão armazenados. Por exemplo, se os parâmetros de dispositivo 20 estiverem armazenados na ROM, a capacidade de memória da memória 16 não será afetada. Entretanto, se os parâmetros de dispositivo 20 não estiverem armazenados na ROM, então a capacidade de memória poderá ser reduzida pelo tamanho dos parâmetros de dispositivo 20 armazenados na memória 16.

A memória 16 compreende o certificado criptografado 24. O certificado é criptografado com uma chave privada de um par de chaves do sistema de criptografia de chaves públicas. A criptografia de chaves públicas é conhecida na técnica. Qualquer sistema criptográfico de chaves públicas apropriado pode ser usado, tal como a conhecida cifra criptográfica RSA, por exemplo. Existe uma descrição da cifra criptográfica RSA na Patente US de Número 4.405.829, intitulada "Cryptographic Communications System and Method", expe-

dida em 20 de setembro de 1983, no nome de Rivest, Shamir, e Adleman. A Patente de Número 4.405.829 é incorporada a título de referência como informação de pano de fundo. A criptografia de chaves públicas utiliza um par de chaves. Uma chave é usada para criptografar e a outra é usada para descriptografar. O conhecimento de uma chave não permite conhecer a outra chave. Geralmente, uma chave é mantida em segredo, e, portanto, é chamada de chave privada. Geralmente, a outra chave é de conhecimento público. De acordo com uma concretização exemplificativa da invenção, o certificado é criptografado com a chave privada e descriptografado com a chave pública.

A Figura 3 é uma representação de um certificado exemplificativo 36. O certificado 36 compreende os parâmetros de dispositivo 20 e, opcionalmente, uma marca 34. Os parâmetros de dispositivo 20 compreendem um número de identificação 26 do dispositivo externo, uma número de série 28 do dispositivo externo, um número de modelo 30 do dispositivo externo, a capacidade de memória 32 da memória do dispositivo externo, e uma marca opcional 34. Deve-se enfatizar que a escolha dos parâmetros de dispositivo e do formato do certificado conforme ilustrada na Figura 3 é meramente exemplificativa. Muitos fornecedores de dispositivos externos armazenam informações de parâmetros na memória do dispositivo externo em um local de acesso público.

A inclusão da marca 34 no certificado 36 é opcional. Ou seja, o certificado 36 pode compreender a marca 34, entretanto a inclusão da marca 34 não é necessária. A marca

34 pode compreender qualquer marca apropriada indicando a autenticidade da unidade de disco rígido 14. A marca 34 pode compreender uma imagem, texto ou de uma combinação desses. A marca 34 pode compreender, por exemplo, o texto "Hard Drive by Microsoft®". A marca 34 é uma indicação de que a unidade de disco rígido 14 foi autorizada para uso no console de jogo 12. A marca 34 é uma indicação de que a unidade de disco rígido 14 foi endossada pelo fornecedor/fabricante do console de jogo 12. Em uma concretização exemplificativa da presente invenção, a marca 34 é armazenada no console de jogo 12 na forma não criptografada.

A marca 34 é uma indicação da autenticidade da unidade externa. A marca 34 também serve como uma confirmação do dispositivo externo pelo fornecedor do console de jogo. Conforme descrito abaixo, a marca 34 pode ser exibida quando o dispositivo externo é autenticado, dando uma confirmação para um usuário de que o dispositivo externo foi aprovado para uso com o console de jogo. A marca 34 pode ser uma marca registrada, com ou sem imagem, indicando a fonte do sistema operacional ou o fornecedor do console de jogo.

A Figura 4 e a Figura 5 são um diagrama de fluxo de dados de um processo de autenticação de acordo com uma concretização exemplificativa da presente invenção; O certificado é gerado na etapa 38. A geração do certificado compreende a seleção dos parâmetros de dispositivo externo e a combinação dos parâmetros selecionados e da marca opcional. Os parâmetros selecionados e a marca podem ser combinados de qualquer maneira apropriada, tal como concatenação, por e-

xemplo. Em uma concretização exemplificativa da presente invenção, o fornecedor de console de jogo gera o certificado 36 extraindo os parâmetros selecionados de dispositivo da memória do dispositivo externo e concatenando opcionalmente os parâmetros selecionados de dispositivo com uma de suas marcas, caso sejam usadas.

O certificado é gerado na etapa 40. O certificado é criptografado com a chave privada de um par de chaves do sistema de criptografia de chaves públicas. O certificado criptografado é armazenado na memória do dispositivo externo na etapa 42. O certificado criptografado pode, por exemplo, ser armazenado em um local acessível da memória 16 da unidade de disco rígido 14, conforme ilustrado na Figura 2. A marca é armazenada na forma não criptografada no console de jogo na etapa 44. Em uma concretização exemplificativa, imagina-se que um fornecedor de console de jogo escolherá parâmetros de dispositivo e produzirá o certificado 36 a partir dos parâmetros selecionados e de uma das marcas do fornecedor de console de jogo. Em seguida, o certificado 36 será criptografado e o certificado criptografado será armazenado em um local de memória predeterminado do dispositivo externo.

Em outra concretização exemplificativa, o certificado compreende parâmetros de dispositivo comuns a um tipo, ou subconjunto, de dispositivos externos, tais como número de modelo e capacidade de memória, por exemplo. Esses parâmetros comuns de dispositivo são fornecidos ao fornecedor de console de jogo para incorporação ao certificado. Já que es-

se certificado contém informações comuns a um tipo de dispositivo externo, uma cópia do certificado poderá ser usada em todos os dispositivos externos desse tipo. Independente da logística da geração e gravação de certificado, o certificado criptografado é, no final de tudo, armazenado na memória do dispositivo externo.

Quando um console de jogo detecta um dispositivo externo, o console de jogo lê os parâmetros de dispositivo não criptografados armazenados na memória do dispositivo externo nas etapas 46 e 48. O dispositivo externo pode ser detectado ao ser ligado, durante uma condição de reinicialização, em resposta à ocorrência de um evento predeterminado (por exemplo, condições específicas de erro), ou em uma combinação desses. Conforme descrito acima, em uma concretização exemplificativa da invenção, a comunicação entre o console de jogo e o dispositivo externo está de acordo com a especificação SATA. De acordo com a especificação SATA, ao detectar um dispositivo externo, o console de jogo fornece um sinal de comando "Identificar Dispositivo" para o dispositivo externo (etapa 46). Em resposta a esse sinal de comando, o dispositivo externo fornece ao console de jogo os parâmetros de dispositivo com relação ao dispositivo externo específico (etapa 48). O console de jogo grava os parâmetros de dispositivo recebidos armazenando-os na memória do console de jogo na etapa 50. Conforme usado no presente documento, o termo memória pode incluir registros.

Na etapa 52, o console de jogo tenta ler o certificado criptografado do dispositivo externo. Se um certifi-

cado criptografado não for detectado (etapa 54), o dispositivo externo é determinado como não autorizado (etapa 56). Se o certificado criptografado é detectado (etapa 54), o certificado criptografado é descriptografado na etapa 58. A descriptografia é atingida utilizando a chave pública correspondente do par de chaves de sistema de criptografia de chaves públicas. Em uma concretização exemplificativa da invenção, a chave pública é armazenada no console de jogo e é disponibilizada para uso para determinar a autenticidade de um dispositivo externo acoplado ao console de jogo. Os componentes do certificado descriptografado são divididos em parâmetros de dispositivo e marca opcional na etapa 60. Na etapa 62, é determinado se o certificado descriptografado foi dividido nos componentes esperados (parâmetros de dispositivo e marca opcional). Se os componentes esperados não forem detectados, o dispositivo externo é determinado como não autorizado (etapa 56). A etapa 62 é opcional. Ou seja, o processo de autenticação pode proceder da divisão do certificado descriptografado na etapa 62 para a comparação de componentes divididos na etapa 64, sem determinar inicialmente se todos os componentes esperados foram detectados.

Na etapa 64, os componentes (parâmetros de dispositivo e marca opcional) do certificado descriptografado dividido são comparados aos componentes gravados com antecedência (parâmetros de dispositivo lidos do dispositivo externo e a marca opcional armazenada no console de jogo). Se os componentes correspondentes não se corresponderem (etapa 66), o dispositivo externo é determinado como não autorizado

(etapa 56). Se os componentes correspondentes se corresponderem (etapa 66), a marca pode ser exibida na etapa 68. A exibição da marca é opcional. Prefigura-se que a exibição da marca dê ao usuário certeza de que o dispositivo externo está autorizado para uso no console de jogo, e de que as operações de jogo ocorrerão conforme o esperado. Se os componentes correspondentes se corresponderem (etapa 66), o dispositivo externo é determinado como autêntico na etapa 70.

Se um dispositivo externo for determinado como autêntico, permite-se ao sistema que opere normalmente. Se um dispositivo externo não for determinado como autêntico, o sistema pode se desligar, exibir uma mensagem de erro, proibir interações subseqüentes entre o console de jogo e o dispositivo externo, ou uma combinação desses.

Embora a descrição da presente invenção tenha sido apresentada no contexto de um sistema de jogo exemplificativo, ela também pode ser aplicada a ambientes de computação mais gerais em que a autenticidade de um dispositivo periférico deve ser determinada. A Figura 6 ilustra um exemplo de um ambiente de sistema de computação adequado 600, no qual uma concretização exemplificativa da presente invenção pode ser implementada. O ambiente de sistema de computação 600 é apenas um exemplo de um ambiente de computação adequado e não tem a intenção de implicar em qualquer limitação ao âmbito de uso ou à funcionalidade da invenção. Tampouco se deve interpretar o ambiente de computação 600 como tendo qualquer dependência ou exigência com relação a qualquer um dos componentes ilustrados, ou combinação desses, no ambiente

operacional exemplificativo 600.

A invenção é operacional com vários ambientes ou configurações diferentes de sistema de computação de uso geral ou específico. Exemplos de sistemas, ambientes e/ou configurações de computação bem conhecidos que podem ser adequados para uso com a invenção incluem, sem a isto se restringir, computadores pessoais, computadores servidores, dispositivos portáteis ou laptop, sistemas multiprocessadores, sistemas baseados em microprocessador, decodificadores de sinais, componentes eletrônicos programados pelo consumidor, PCs de rede, microcomputadores, computadores de grande porte, ambientes de computação distribuída que incluem qualquer um dos sistemas ou dispositivos acima, telefones, PDAs, equipamentos de áudio, equipamentos fotográficos, equipamentos de teste, produtos automotivos, entre outros.

A invenção pode ser descrita no contexto geral de instruções executadas por computador, tais como módulos de programa sendo executados por um computador. Geralmente, os módulos de programa incluem rotinas, programas, objetos, estruturas de dados etc., que efetuam tarefas específicas ou implementam tipos de dados abstratos específicos. A invenção pode também ser praticada em ambientes de computação distribuída onde se efetuam tarefas por dispositivos de processamento remoto ligados por meio de uma rede de comunicações ou por outro meio de transmissão de dados. Em um ambiente de computação distribuída, os módulos de programa e outros dados podem ser localizados tanto em meios de armazenamento de computador remotos quanto locais, incluindo dispositivos de

armazenamento em memória.

Com referência à Figura 6, um sistema exemplificativo para implementação da invenção inclui um dispositivo de computação de uso geral na forma de um computador 610. Em uma concretização exemplificativa da presente invenção, um console de jogo compreende o computador 610. Os componentes do computador 610 podem incluir, sem a isto se restringir, uma unidade de processamento 620, um memória de sistema 630 e um barramento de sistema 621 que acopla vários componentes do sistema, incluindo a memória do sistema à unidade de processamento 620. O barramento de sistema 621 pode possuir qualquer um dos diferentes tipos de estrutura de barramento, incluindo um barramento de memória ou controlador de memória, um barramento periférico e um barramento local usando qualquer uma das diferentes arquiteturas de barramento. A título exemplificativo, sem limitação, tais arquiteturas incluem barramento da Arquitetura Padrão da Indústria (ISA), barramento da Arquitetura de Microcanal (MCA), barramento ISA Aperfeiçoada (EISA), barramento local da Associação de Padrões Eletrônicos de Vídeo (VESA) e barramento de Interconexão de Componentes Periféricos (PCI) (também chamado de barramento Mezanino).

O computador 610 geralmente inclui uma variedade de meios legíveis por computador. Meios legíveis por computador podem ser qualquer meio disponível que pode ser acessado por computador 610 e que inclui tanto meios voláteis e não voláteis, quanto meios removíveis e não removíveis. A título exemplificativo, sem limitação, meios legíveis por

computador podem compreender meios de armazenamento e meios de comunicação de computador. Os meios de armazenamento de computador incluem tanto meios voláteis e não voláteis, quanto removíveis e não removíveis implementados em qualquer método ou tecnologia para armazenamento de informações, tais como instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados. Os meios de armazenamento incluem, sem a isto se restringir, RAM, ROM, EEPROM, memória flash ou outra tecnologia de memória, CD-ROM, discos versáteis digitais (DVD) ou outro armazenamento em disco óptico, cassetes magnéticos, fita magnética, armazenamento em disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outro meio que possa ser usado para armazenar as informações desejadas e que possa ser acessado pelo computador 610. Os meios de comunicação geralmente abrangem instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados em um sinal de dados modulado tal como uma onda portadora ou outro mecanismo de transporte, e incluem quaisquer meios de distribuição de informações. O termo "sinal de dados modulados" significa um sinal que uma ou mais de suas características ajustadas ou alteradas de tal maneira a codificar as informações no sinal. A título exemplificativo, e sem limitação, os meios de comunicação incluem meios com fio, tal como uma rede com fio ou conexão direta com fio, e meios sem fio, tal como acústico, RF, infravermelho e outros meios sem fio. Combinações de qualquer um dos elementos anteriores também deverão ser incluídas no âmbito de meios legíveis por compu-

tador.

A memória do sistema 630 inclui meios de armazenamento de computador na forma de memória volátil e/ou não volátil, tal como ROM 631 e RAM 632. Um sistema básico de entrada/saída 633 (BIOS), contendo as rotinas básicas para ajudar a transferir informações entre os elementos dentro do computador 610, tal como durante a inicialização, é geralmente armazenado na ROM 631. A RAM 632 geralmente contém dados e/ou módulos de programa que podem ser acessados a qualquer momento e/ou que estão sendo operados pela unidade de processamento 620. A título exemplificativo, e sem limitação, a Figura 6 ilustra o sistema operacional 634, programas aplicativos 635, outros módulos de programa 636, e dados de programa 637.

O computador 610 também inclui outros meios de armazenamento de computador removíveis/não removíveis e voláteis/não voláteis. A título meramente exemplificativo, a Figura 6 ilustra uma unidade de disco rígido 641 que lê ou grava em meios magnéticos não removíveis e não voláteis, uma unidade de disco magnético 651 que lê ou grava em um disco magnético removível e não volátil 652, e uma unidade de disco óptica 655 que lê ou escreve em um disco óptico removível e não volátil 656, tal como um CD-ROM ou outros meios ópticos. Outros meios de armazenamento de computador removíveis/não removíveis e voláteis/não voláteis que podem ser usados no ambiente operacional exemplificativo incluem, mas sem a isto se restringir, cassetes de fita magnética, cartões de memória flash, discos versáteis digitais, fitas de

vídeo digital, RAM de estado sólido, ROM de estado sólido, entre outros. A unidade de disco rígido 641 é geralmente conectada ao barramento do sistema 621 por meio de uma interface de memória não removível, tal como a interface 640, e a unidade de disco magnético 651 e a unidade de disco óptico 655 são geralmente conectadas ao barramento de sistema 621 por uma interface de memória removível, tal como a interface 650.

As unidades e seus meios de armazenamento de computador associados fornecem o armazenamento de instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o computador 610. Na Figura 6, por exemplo, a unidade de disco rígido 641 é ilustrada armazenando o sistema operacional 644, os programas aplicativos 645, outros módulos de programa 646, e dados de programa 647. Observe que esses componentes podem ou ser os mesmos ou ser diferentes do sistema operacional 634, dos programas aplicativos 635, dos outros módulos de programa 636, e dos dados de programa 637. O sistema operacional 644, os programas aplicativos 645, os outros módulos de programa 646, e os dados de programa 647 recebem diferentes números neste documento para mostrar que se tratam, no mínimo, de cópias diferentes.

Um usuário pode entrar com comandos e informações no computador 610 por meio de dispositivos de entrada, tal como um teclado 662 e o dispositivo de apontamento 661, normalmente chamado de mouse, trackball ou superfície de toque. Outros dispositivos de entrada (não ilustrados) podem inclu-

ir um microfone, joystick, controle de jogo, antena de satélite, scanner, entre outros. Esses e outros dispositivos de entrada são geralmente conectados à unidade de processamento 620 por meio de uma interface de entrada do usuário 660 que é acoplada ao barramento do sistema, mas que pode ser conectada por outra interface e estruturas de barramento, tal como uma porta paralela, porta de jogo ou um barramento serial universal (USB).

Um monitor 691, ou outro tipo de dispositivo de exibição, também é conectado ao barramento do sistema 621 por meio de uma interface, tal como uma interface de vídeo, que pode compreender uma unidade de processamento de gráficos (GPU) e memória de vídeo 690. Além do monitor, os computadores também podem incluir outros periféricos de saída, tais como alto-falantes 697 e impressora 696, que podem ser conectados por meio de uma interface periférica de saída 695.

O computador 610 pode operar em um ambiente em rede usando conexões lógicas com um ou mais computadores remotos, tal como o computador remoto 680. O computador remoto 680 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo não hierarquizado ou outro nó comum da rede, e geralmente inclui muitos ou todos os elementos supramencionados com relação ao computador 610, apesar de apenas um dispositivo de armazenamento em memória 681 haver sido ilustrado na Figura 6. As conexões lógicas representadas incluem uma LAN 671 e uma WAN 673, mas podem incluir outras redes. Tais ambientes de rede são comuns em

escritórios, redes de computador a nível empresarial, intranets e a Internet.

Quando usado em uma ambiente em rede LAN, o computador 610 é conectado à LAN 671 por meio de uma interface de rede ou adaptador 670. Quando usado em um ambiente em rede WAN, o computador 610 geralmente inclui um modem 672 ou outros meios para estabelecer comunicações pela WAN 673, tal como a Internet. O modem 672, que pode ser interno ou externo, pode ser conectado ao barramento do sistema 621 por meio da interface de entrada do usuário 660, ou por outro mecanismo apropriado. Em um ambiente em rede, os módulos de programa representados com relação ao computador 610, ou partes deles, podem ser armazenados no dispositivo de armazenamento em memória remoto. A título exemplificativo, e sem limitação, a Figura 6 ilustra programas aplicativos remotos 685 residindo no dispositivo de memória 681. Será apreciado que as conexões de rede ilustradas são exemplificativas e que outros meios para estabelecer uma ligação de comunicações entre os computadores podem ser usados.

Conforme mencionado acima, embora as concretizações exemplificativas da presente invenção tenham sido descritas com relação a vários dispositivos de computação, os conceitos subjacentes podem ser aplicados a qualquer dispositivo ou sistema de computação no qual se deseje a autenticação de periféricos.

As várias técnicas descritas no presente documento podem ser implementadas em hardware ou software ou, quando apropriado, em uma combinação de ambos. Sendo assim, os mé-

todos e os aparelhos da presente invenção, ou certos aspectos ou partes deles, podem assumir a forma de código de programa (isto é, instruções) incorporado em meios tangíveis, tais como discos flexíveis, CD-ROMs, unidades de disco rígido, ou qualquer outro meio de armazenamento legível por máquina, em que, quando o código de programa é carregado e executado por uma máquina, tal como um computador, a máquina de torna um aparelho para pratica da invenção. No caso da execução de código de programa em computadores programáveis, o dispositivo de computação incluirá em geral um processador, um meio de armazenamento legível pelo processador (incluindo memória volátil e não volátil e/ou elementos de armazenamento), pelo menos um dispositivo de entrada, e pelo menos um dispositivo de saída. O(s) programa(s) pode(m) ser implementado(s) em linguagem assembly ou de máquina, se desejado. Seja qual for o caso, a linguagem pode ser uma linguagem compilada ou interpretada, e combinada com implementações de hardware.

Os métodos e os aparelhos da presente invenção podem também ser praticados por meio de comunicações incorporadas na forma de código de programa que é transmitido por algum meio de transmissão, tal como por fiação ou cabeamento elétrico, por meio de fibras óticas, ou por meio de qualquer outra forma de transmissão, em que, quando o código de programa é recebido ou carregado e executado pela máquina, tal como uma EPROM, uma matriz de portas, um dispositivo lógico programável (PLD), um computador cliente, entre outros, a máquina se torna um aparelho para pratica da invenção. Quan-

do implementado em um processador de uso geral, o código de programa de com o processador para fornecer um aparelho único que opera para invocar a funcionalidade da presente invenção. Ademais, quaisquer técnicas de armazenamento usadas com relação à presente invenção podem ser invariavelmente uma combinação de hardware e software.

Embora a presente invenção tenha sido descrita com relação às concretizações preferidas das várias figuras, deve-se compreender que outras concretizações semelhantes podem ser usadas ou modificações e acréscimos podem ser feitos às concretizações descritas para a execução da mesma função da presente invenção sem se desviarem dela. Portanto, a presente invenção não deve ser limitada a qualquer concretização individual, mas, em vez disso, deve ser interpretada em amplitude e no âmbito de acordo com as reivindicações em anexo.

REIVINDICAÇÕES

1. Método para autenticação de um periférico de console de jogo, o referido método **CARACTERIZADO** por compreender:

receber, do referido periférico de console de jogo, pelo menos um parâmetro de identificação de periférico;

receber, do referido periférico de console de jogo, um certificado criptografado, o referido certificado sendo criptografado com uma chave privada de um par de chaves criptográficas de chave pública;

descriptografar o referido certificado criptografado com uma chave pública correspondente do referido par de chaves criptográficas; o referido certificado descriptografado compreendendo o referido pelo menos um parâmetro de identificação de periférico;

comparar o referido pelo menos um parâmetro de identificação de periférico recebido do referido periférico de console de jogo com o referido pelo menos um parâmetro de identificação de periférico do referido certificado descriptografado; e

autenticar o referido periférico de console de jogo de acordo com um resultado da referida comparação.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por adicionalmente compreender:

determinar o referido periférico de console de jogo como autêntico se o pelo menos um parâmetro de identificação de periférico recebido do referido periférico de console de jogo corresponder ao referido pelo menos um parâme-

tro de identificação de periférico do referido certificado descriptografado.

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que:

o referido certificado adicionalmente compreende uma marca que indica a autenticidade do referido periférico de console de jogo;

o referido console de jogo compreende a referida marca; e

a referida etapa de comparação adicionalmente compreende comparar a referida marca do referido certificado descriptografado com a referida marca do referido console de jogo.

4. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que a referida marca compreende uma representação de uma marca registrada.

5. Método, de acordo com a reivindicação 3, **CARACTERIZADO** por adicionalmente compreender:

exibir a referida marca como uma indicação de que o referido periférico de console de jogo é determinado como autêntico.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o referido periférico de console de jogo compreende uma unidade de disco rígido.

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o referido parâmetro de identificação de periférico compreende pelo menos um dentre um número de série do referido periférico de console de jogo,

um modelo do referido periférico de console de jogo, e uma capacidade de memória da memória do referido periférico de console de jogo.

8. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o referido certificado criptografado é recebido em resposta à detecção do referido periférico de console de jogo pelo referido console de jogo.

9. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por adicionalmente compreender:

combinar pelo menos um dentre um parâmetro de identificação de periférico e uma marca que indica a autenticidade do referido periférico para formar o referido certificado; e

criptografar o referido certificado com a referida chave privada.

10. Sistema para autenticação de um periférico de console de jogo, o referido sistema **CARACTERIZADO** por compreender:

o referido periférico de console de jogo compreendendo um certificado criptografado armazenado nele, em que:

o referido certificado criptografado é criptografado com uma chave privada de um par de chaves criptográficas de chave pública;

um console de jogo para:

receber, do referido periférico de console de jogo, um certificado criptografado, em que o referido certificado compreende pelo menos um parâmetro de identificação de periférico;

descriptografar o referido certificado criptografado com uma chave pública correspondente do referido par de chaves criptográficas; o referido certificado descriptografado compreendendo o referido pelo menos um parâmetro de identificação de periférico;

comparar o referido pelo menos um parâmetro de identificação de periférico recebido do referido periférico de console de jogo com o referido pelo menos um parâmetro de identificação de periférico do referido certificado descriptografado; e

autenticar o referido periférico de console de jogo de acordo com um resultado da referida comparação.

11. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que:

o referido console de jogo determina o referido periférico de console de jogo como autêntico se o referido pelo menos um parâmetro de identificação de periférico recebido do referido periférico de console de jogo corresponder ao referido pelo menos um parâmetro de identificação de periférico do referido certificado descriptografado.

12. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que:

o referido certificado adicionalmente compreende uma marca que indica a autenticidade do referido periférico de console de jogo;

o referido console de jogo compreende a referida marca; e

o referido console de jogo compara a referida mar-

ca do referido certificado descriptografado com a referida marca do referido console de jogo.

13. Sistema, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que a referida marca compreende uma representação de uma marca registrada.

14. Sistema, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que o referido console de jogo exibe a referida marca como uma indicação de que o referido periférico de console de jogo é determinado como autêntico.

15. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o referido periférico de console de jogo compreende uma unidade de disco rígido.

16. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o referido parâmetro de identificação de periférico compreende pelo menos um dentre um número de série do referido periférico de console de jogo, um modelo do referido periférico de console de jogo, e uma capacidade de memória da memória do referido periférico de console de jogo.

17. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o referido certificado criptografado é recebido em resposta à detecção do referido periférico de console de jogo do referido console de jogo.

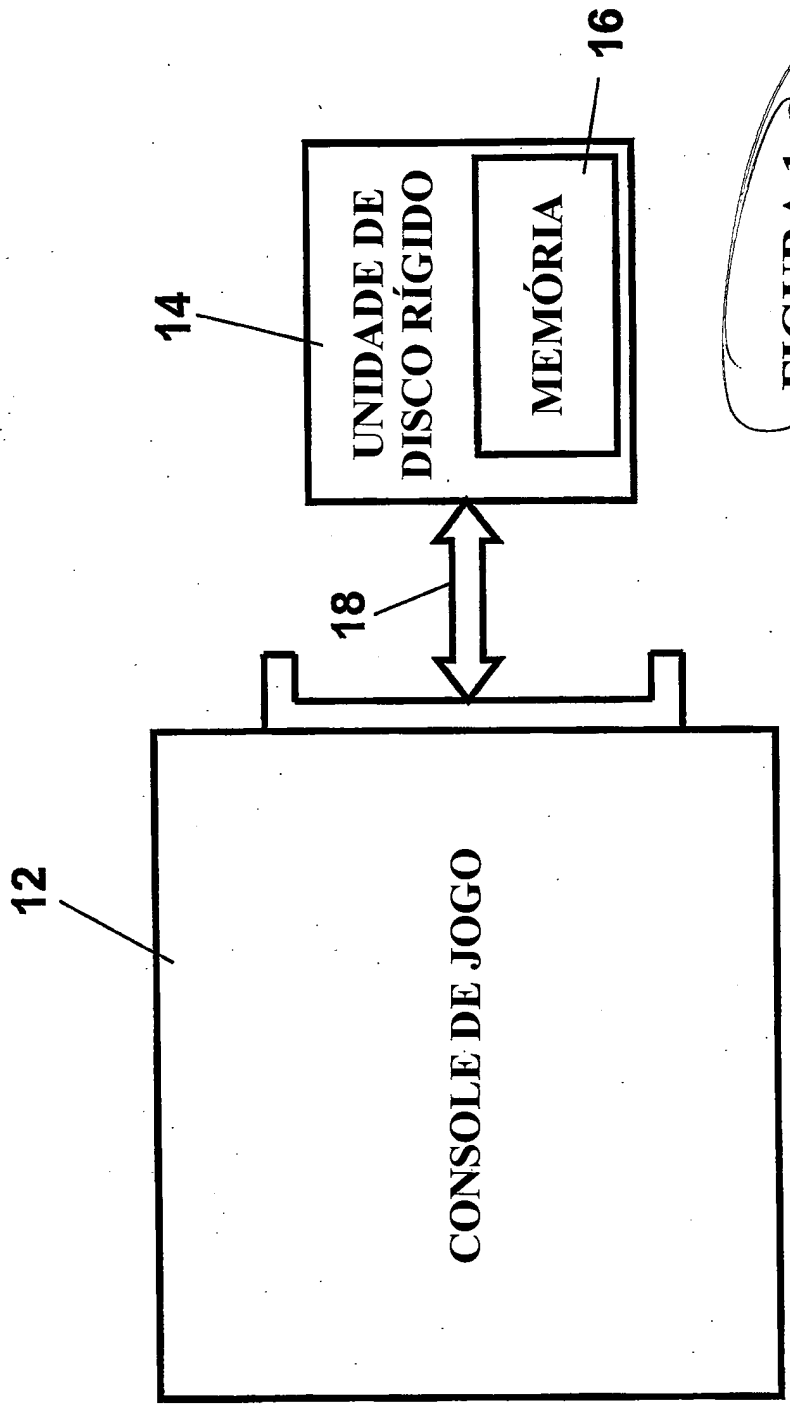


FIGURA 1

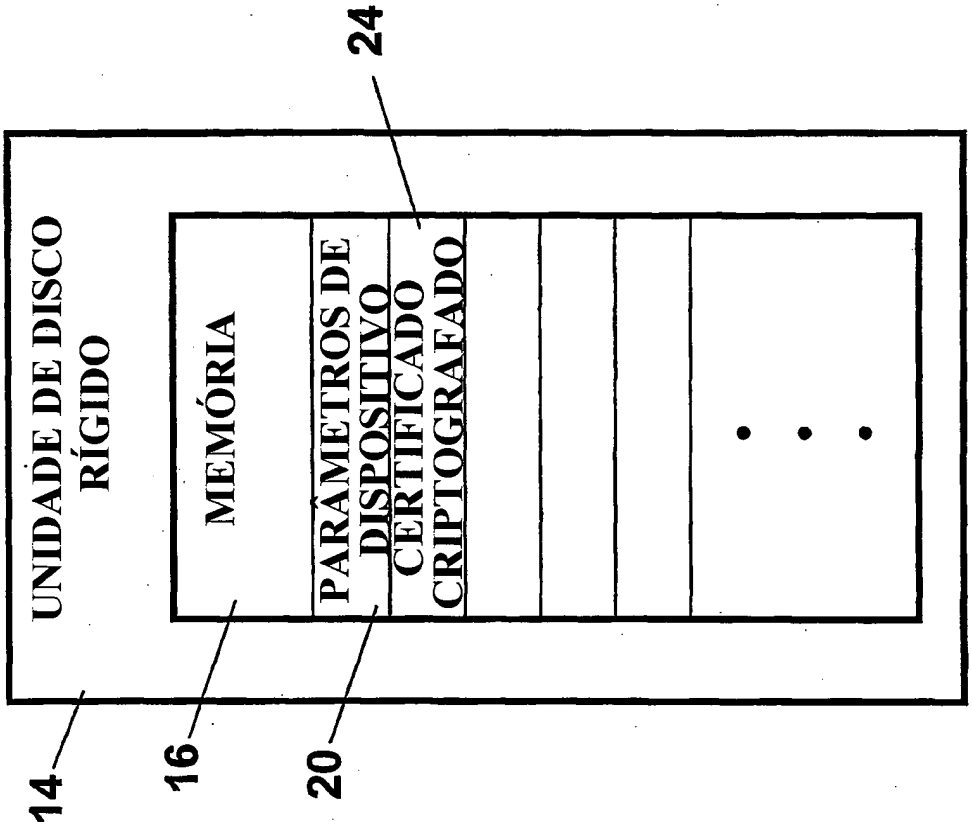

UNIDADE DE DISCO RÍGIDO
MEMÓRIA
PARÂMETROS DE DISPOSITIVO
CERTIFICADO CRIPTOGRAFADO
14
16
20
24

FIGURA 2

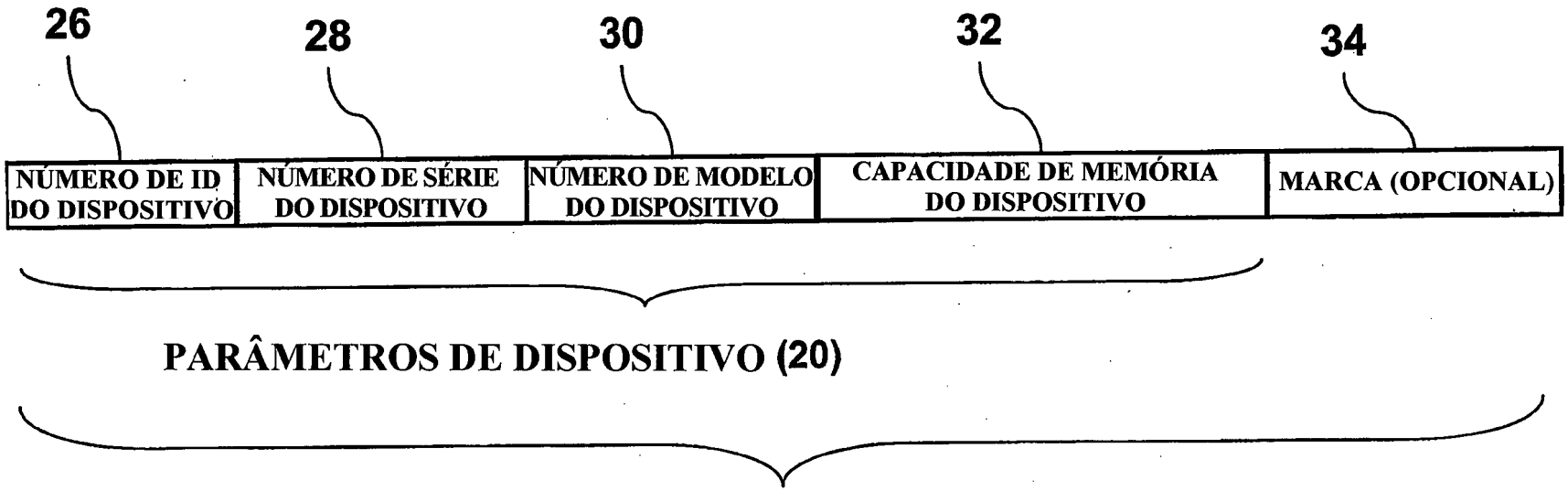

26
28
30
32
34
NÚMERO DE ID DO DISPOSITIVO
NÚMERO DE SÉRIE DO DISPOSITIVO
NÚMERO DE MODELO DO DISPOSITIVO
CAPACIDADE DE MEMÓRIA DO DISPOSITIVO
MARCA (OPCIONAL)
PARÂMETROS DE DISPOSITIVO (20)
CERTIFICADO (36)

FIGURA 3

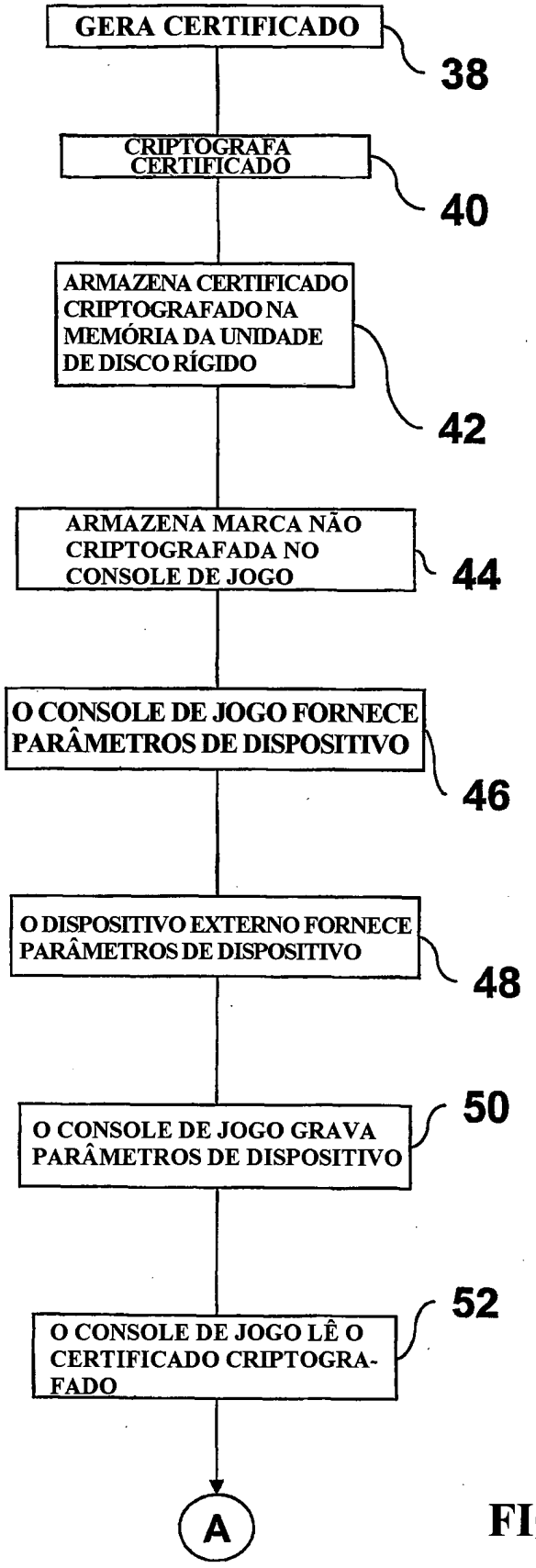

GERA CERTIFICADO
38
CRIPTOGRAFA CERTIFICADO
40
ARMAZENA CERTIFICADO CRIPTOGRAFADO NA MEMÓRIA DA UNIDADE DE DISCO RÍGIDO
42
ARMAZENA MARCA NÃO CRIPTOGRAFADA NO CONSOLE DE JOGO
44
O CONSOLE DE JOGO FORNECE PARÂMETROS DE DISPOSITIVO
46
O DISPOSITIVO EXTERNO FORNECE PARÂMETROS DE DISPOSITIVO
48
O CONSOLE DE JOGO GRAVA PARÂMETROS DE DISPOSITIVO
50
O CONSOLE DE JOGO LÊ O CERTIFICADO CRIPTOGRAFADO
52
A

FIGURA 4

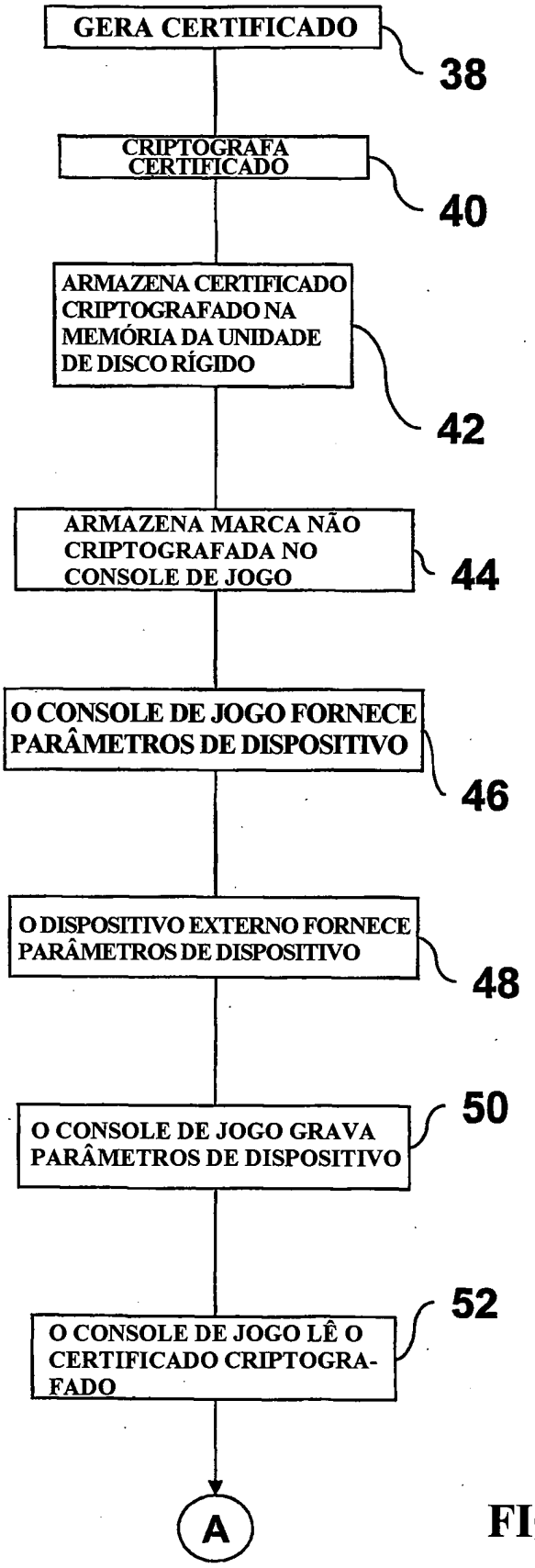

GERA CERTIFICADO
38
CRIPTOGRAFA CERTIFICADO
40
ARMAZENA CERTIFICADO CRIPTOGRAFADO NA MEMÓRIA DA UNIDADE DE DISCO RÍGIDO
42
ARMAZENA MARCA NÃO CRIPTOGRAFADA NO CONSOLE DE JOGO
44
O CONSOLE DE JOGO FORNECE PARÂMETROS DE DISPOSITIVO
46
O DISPOSITIVO EXTERNO FORNECE PARÂMETROS DE DISPOSITIVO
48
O CONSOLE DE JOGO GRAVA PARÂMETROS DE DISPOSITIVO
50
O CONSOLE DE JOGO LÊ O CERTIFICADO CRIPTOGRA-FADO
52
A

FIGURA 4

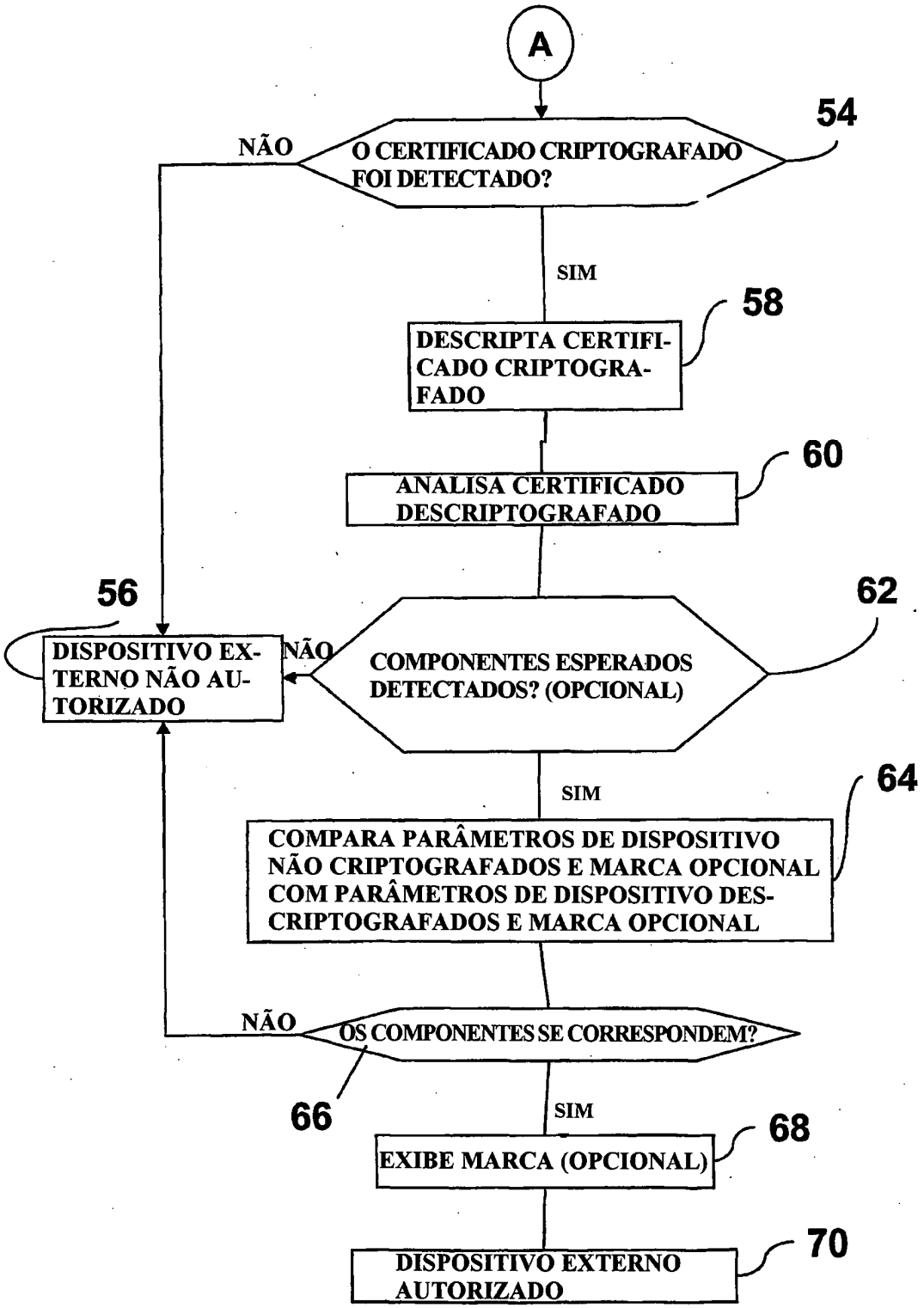

A
54
NÃO
O CERTIFICADO CRIPTOGRAFADO FOI DETECTADO?
SIM
58
DESCRIPTA CERTIFICADO CRIPTOGRAFADO
60
ANALISA CERTIFICADO DESCRIPTOGRAFADO
56
62
DISPOSITIVO EXTERNO NÃO AUTORIZADO
NÃO
COMPONENTES ESPERADOS DETECTADOS? (OPCIONAL)
SIM
64
COMPARA PARÂMETROS DE DISPOSITIVO NÃO CRIPTOGRAFADOS E MARCA OPCIONAL COM PARÂMETROS DE DISPOSITIVO DESCRIPTOGRAFADOS E MARCA OPCIONAL
NÃO
OS COMPONENTES SE CORRESPONDEM?
66
SIM
68
EXIBE MARCA (OPCIONAL)
70
DISPOSITIVO EXTERNO AUTORIZADO

FIGURA 5

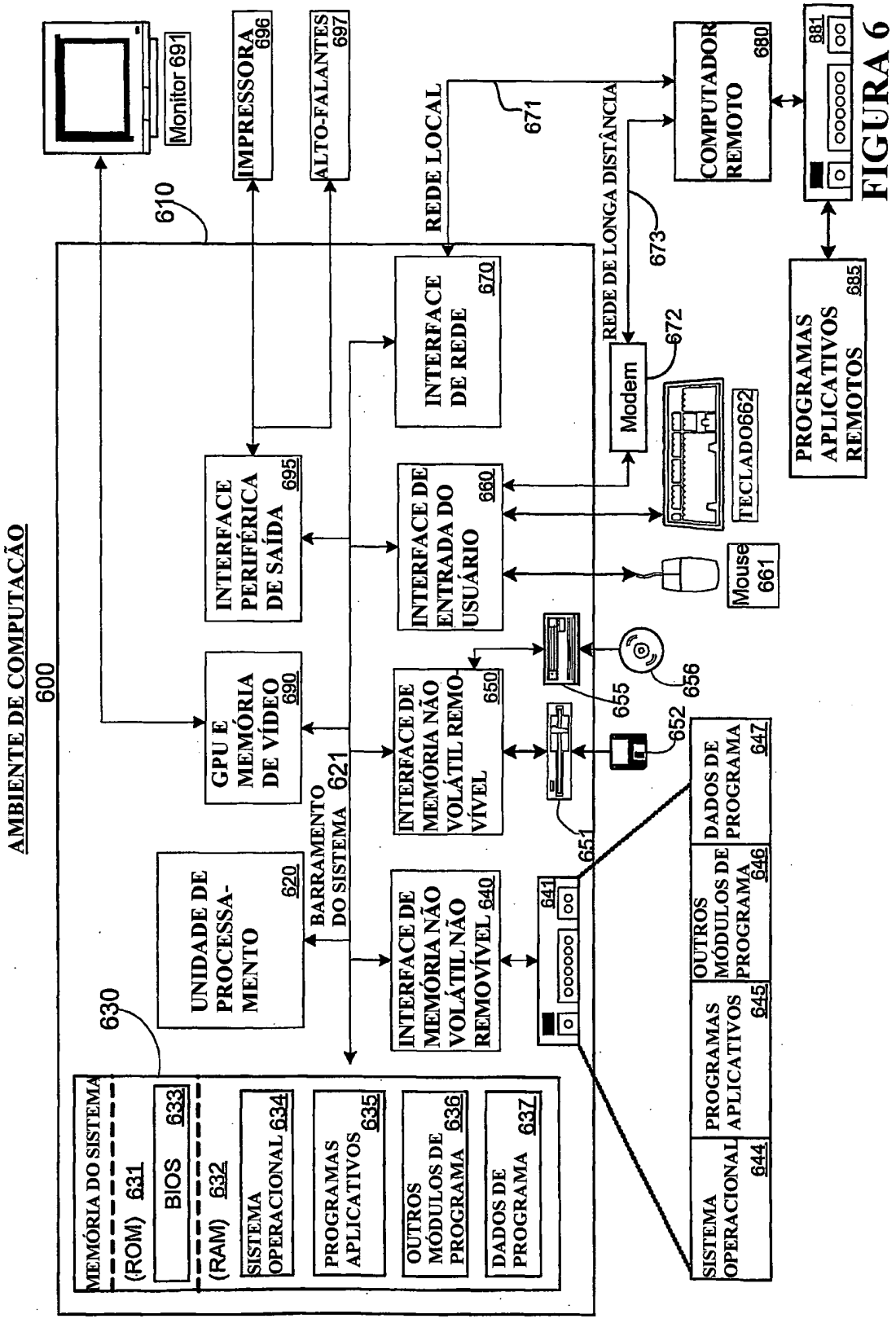

AMBIENTE DE COMPUTAÇÃO
600
610
Monitor 691
IMPRESSORA 696
ALTO-FALANTES 697
REDE LOCAL
671
REDE DE LONGA DISTÂNCIA
673
COMPUTADOR REMOTO 680
881
PROGRAMAS APLICATIVOS REMOTOS 685
INTERFACE DE REDE 670
672
Modem
TECLADO662
Mouse 661
INTERFACE PERIFÉRICA DE SAÍDA 695
INTERFACE DE ENTRADA DO USUÁRIO 660
GPU E MEMÓRIA DE VÍDEO 690
INTERFACE DE MEMÓRIA NÃO VOLÁTIL REMOVÍVEL 650
655
656
652
651
UNIDADE DE PROCESSAMENTO 620
BARRAMENTO DO SISTEMA 621
INTERFACE DE MEMÓRIA NÃO VOLÁTIL NÃO REMOVÍVEL 640
641
630
MEMÓRIA DO SISTEMA
(ROM) 631
BIOS 633
(RAM) 632
SISTEMA OPERACIONAL 634
PROGRAMAS APLICATIVOS 635
OUTROS MÓDULOS DE PROGRAMA 636
DADOS DE PROGRAMA 637
SISTEMA OPERACIONAL 644
PROGRAMAS APLICATIVOS 645
OUTROS MÓDULOS DE PROGRAMA 646
DADOS DE PROGRAMA 647

FIGURA 6

PI0609123-7

RESUMO

"AUTENTICAÇÃO DE UNIDADE DE DISCO RÍGIDO"

Trata-se de um console de jogo que determina, pela análise de um certificado criptografado, se uma unidade de disco rígido está autorizada para uso com o console de jogo. O certificado criptografado é armazenado na memória da unidade. Quando a unidade é detectada, o console de jogo recebe o certificado criptografado e o descriptografa. O certificado contém parâmetros com relação à unidade, tal como o número de série da unidade, o número de modelo da unidade, a capacidade de memória da unidade, e uma marca registrada que indica a autenticidade da unidade, por exemplo. O console de jogo também recebe esses parâmetros da unidade na forma não criptografada. Os parâmetros extraídos do certificado criptografado são comparados com os parâmetros lidos da memória da unidade de disco rígido. Se os parâmetros se corresponderem, a unidade é determinada como autêntica. O certificado é criptografado com uma chave privada de um par de chaves pública-privada e descriptografado com a chave pública correspondente de acordo com as técnicas criptográficas de chave pública bem conhecidas.