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

(21) PI 9904979-1 A

(22) Data de Depósito 29/10/1999
(43) Data de Publicação 19/12/2000
(RPI 1563)

(51) Int. Cl[7].:
G11B 23/28

(54) Título **CONTROLE DE ACESSO A UMA INFORMAÇÃO ARMAZENADA**

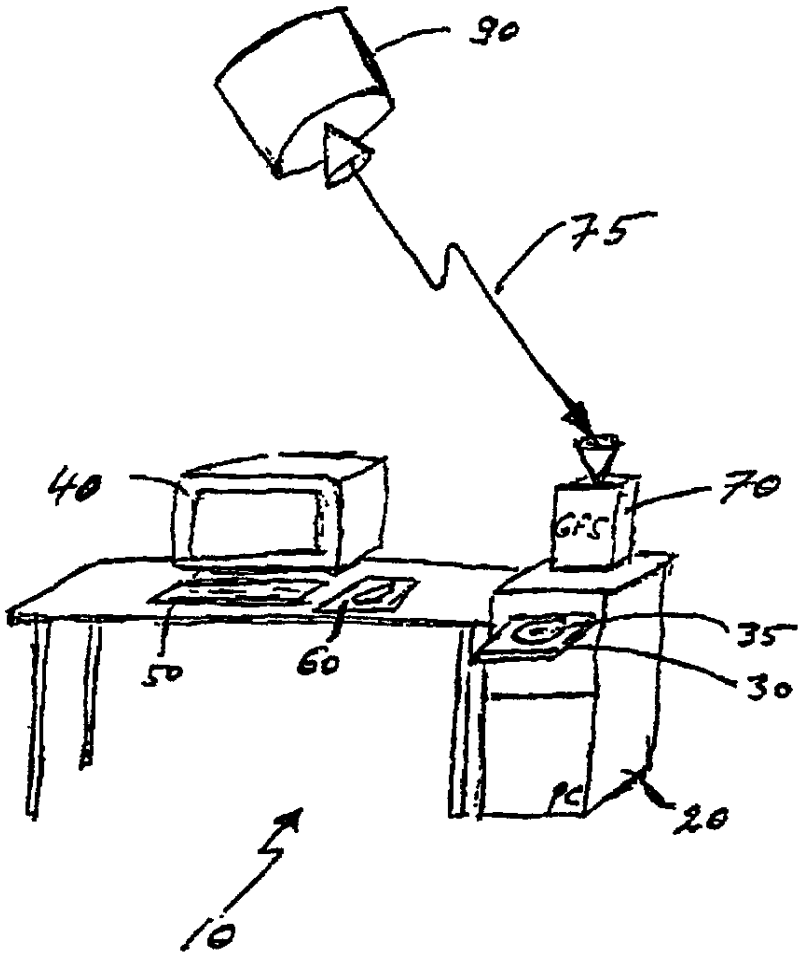
(30) Prioridade Unionista 29/10/1998 US 09/182,342

(71) Depositante(s) Datum Inc (US)

(72) Inventor(es) Thomas Mark Hastings, Michael E Mcnell, Todd S Glassey, Gerald L Willett

(74) Procurador Dannemann, Siemsen, Bigler & Ipanema Moreira

(57) Resumo Patente de Invenção "CONTROLE DE ACESSO A UMA INFORMAÇÃO ARMAZENADA" O acesso a uma informação armazenada por um usuário é controlado comparando-se uma posição geográfica real e/ou uma data / um tempo real com uma região geográfica e/ou um intervalo de data / tempo no qual o acesso à informação armazenada esta autorizado A posição geográfica real onde a informação armazenada está localizada e a data / o tempo real podem ser determinados, por exemplo, baseado em sinais recebidos em um receptor que supre informação de posição e de tempo confiável, tal como um receptor de GPS O acesso à informação armazenada e autorizado se a posição geográfica real e/ou a data / o tempo caírem na região geográfica e/ou no intervalo de data / tempo autorizado A informação de posição e de data / tempo suprida pelo receptor pode ser assinada de forma criptográfica e criptografada



Relatório Descritivo da Patente de Invenção para **"CONTROLE DE ACESSO A UMA INFORMAÇÃO ARMAZENADA".**

Antecedentes

Esta invenção refere-se ao controle de acesso a uma informação armazenada

Meios de distribuição de dados, tais como CD-ROM, podem armazenar um grande número de arquivos O produtor do CD-ROM pode desejar controlar o acesso pelos usuários a arquivos em particular, seja porque eles são confidenciais ou porque o acesso está sujeito a um pagamento pelo usuário

O acesso pode ser controlado requerendo-se que o usuário entre com uma senha obtida a partir do produtor do CD-ROM Senhas diferentes podem desbloquear arquivos diferentes ou subconjuntos diferentes de arquivos Os arquivos podem ser assinados de forma criptográfica e para proteção adicional podem ser criptografados No esquema discutido na Patente U S No 5 646 992, incorporada aqui como referência, cada arquivo é criptografado pelo produtor com uma chave única conhecida apenas pelo produtor O usuário recebe os itens criptografados e, após sua requisição para acesso ser processada pelo produtor, também recebe chaves de descriptografia, isto é, senhas, as quais são usadas para desencriptar os respectivos arquivos criptografados As senhas desbloqueiam apenas aqueles arquivos para os quais o acesso foi requisitado

Sumário

Em geral, em um aspecto da invenção, a invenção caracteriza um controle de acesso a uma informação armazenada determinando uma posição geográfica real onde a informação armazenada está localizada, baseado em sinais recebidos em um receptor que supre uma informação de posição confiável A posição geográfica real é então comparada com uma região geográfica na qual o acesso à informação armazenada está autorizado É permitido acesso do usuário à informação armazenada se a posição geográfica real estiver localizada na região geográfica autorizada

As modalidades da invenção incluem os aspectos a seguir O

receptor que supre a informação de posição pode receber a informação de posição a partir de um sistema de determinação de localização baseado em satélite ou de um sistema de navegação inerte A informação pode ser armazenada em um meio que pode ser lido em computador, tal como um disco de alta capacidade A informação armazenada inclui arquivos, e cada um desses arquivos tem uma região geográfica associada na qual o acesso é permitido O usuário tem acesso a um arquivo específico ou a arquivos se a posição geográfica real estiver localizada na região geográfica autorizada para este arquivo A informação armazenada pode estar criptografada, e o usuário tem acesso à chave de descriptografia apenas se a posição geográfica real estiver localizada na região geográfica autorizada A informação armazenada também pode estar dividida em subconjuntos de informação e onde pelo menos um dos subconjuntos tem uma região autorizada diferente dos outros subconjuntos A associação dos arquivos às regiões geográficas autorizadas pode ser armazenada como um arquivo de política juntamente com a informação armazenada

Em geral, em um outro aspecto, a invenção caracteriza a determinação de uma data ou tempo real no local da informação armazenada baseado em sinais recebidos em um receptor suprindo uma informação de tempo confiável A data ou o tempo real é comparado com um intervalo de data ou tempo predeterminado no qual o acesso à informação armazenada está autorizado O usuário pode ter acesso à informação armazenada se a data ou o tempo real ocorrer no intervalo de data ou tempo autorizado

Em geral, em um outro aspecto, a invenção inclui um receptor que supre informação de posição confiável para determinação de uma posição geográfica real onde a informação armazenada está localizada Um computador recebe a informação de posição com uma região geográfica na qual o acesso à informação armazenada está autorizado, e permite acesso à informação armazenada se a posição geográfica real estiver localizada na região geográfica autorizada As modalidades da invenção incluem os aspectos a seguir O receptor inclui um mecanismo de criptografia de receptor para assinar de forma criptográfica a posição geográfica real com uma cha-

ve de criptografia de receptor e verificando a assinatura do receptor com uma chave de descriptografia de receptor, antes da posição geográfica real ser comparada com a posição geográfica autorizada

Em geral, ainda em um outro aspecto, a invenção inclui um leitor com uma chave de descriptografia de receptor para verificação da posição real assinada de forma criptográfica.

As modalidades da invenção incluem os aspectos a seguir A leitora gera um vetor de inicialização provendo um deslocamento de posição, o qual é transmitido para o receptor e adicionado à posição geográfica autorizada. O leitor assina de forma criptográfica o deslocamento de posição com uma chave de criptografia de leitora O receptor verifica a assinatura de deslocamento de posição com uma chave de descriptografia de leitora correspondente, antes do deslocamento de posição ser adicionado à posição geográfica real

Em geral, em um outro aspecto, a invenção caracteriza a formação de uma política associando a informação às regiões geográficas autorizadas e a intervalos de tempo autorizado e assina de forma criptográfica a política e a informação A política assinada é armazenada juntamente com a informação assinada O usuário obtém do produtor uma senha para desbloquear a política e obtém acesso à informação armazenada se a posição geográfica real e o tempo real caírem nas regiões geográficas autorizadas e no intervalo de tempo autorizado da política

Dentre as vantagens da invenção estão uma ou mais das que se seguem

Um produtor de informação armazenada pode restringir o uso daquela informação a regiões geográficas designadas ou pode excluir regiões designadas onde o uso não é permitido Por exemplo, um manual de serviços para um automóvel armazenado em um CD-ROM pode conter seções diferentes de informação, as quais são aplicáveis a países e/ou regiões específicas correspondentes Pode ser permitido que um usuário veja apenas a porção da informação a qual é aplicável a sua localização geográfica atual Da mesma forma, o acesso a um relatório de corporação delicado

pode ser limitado a um local específico na instalação O acesso a uma informação delicada quanto ao tempo pode ser negado antes ou depois de uma certa data ou limitado a um período permitido Pela associação da informação sobre as regiões geográficas e os intervalos de tempo autorizados aos arquivos de política armazenados no CD-ROM e acessados por uma senha de usuário, o produtor do CD-ROM pode emitir uma nova senha, para permitir que o usuário acesse um conjunto em particular de arquivos de política e, portanto, a informação armazenada, para uma região e data / tempo correspondentes

Outras vantagens e aspectos tornar-se-ão aparentes a partir da descrição a seguir e das reivindicações

Descrição

A FIG 1 é uma vista em perspectiva de um sistema computacional,

A FIG 2 é um diagrama de blocos de um sistema baseado em computador para controle do acesso à informação armazenada,

As FIG 3 a 5 são fluxogramas,

A FIG 6 é um diagrama de blocos de elementos criptográficos

Como visto nas FIG 1 a 3, o acesso à informação a qual está armazenada em um CD-ROM que pode ser lido em computador portátil, o qual serve como um meio de distribuição de dados 35, pode ser controlado baseado em uma posição geográfica real de um sistema computacional 10 no qual a informação deve ser acessada e o tempo em que ela deve ser acessada

No sistema computacional 10, um computador 20 é conectado a um teclado 50, um mouse 60, um monitor 40, e um drive de CD-ROM 30 Um receptor de GPS 70 serve como uma fonte de informação de posição e de tempo confiável O receptor 70 está localizado na posição geográfica real do sistema computacional 10 e recebe sinais 75 de um satélite de GPS em órbita 90 (sendo mostrado apenas um) O receptor 70 converte os sinais 75 recebidos em dados de posição geográfica 71 até uma precisão de vários metros de longitude, latitude e altura e em dados de data / tempo 71 até

uma precisão de microssegundos Os dados 71 são transmitidos para o computador 20 via um controlador de dispositivo 72

Uma cripto-placa de receptor 80 pode conter um certificado de chave pública 81 assinado pelo produtor e uma chave privada correspondente 82, como mostrado na FIG 6 Os dados de posição geográfica e de data / tempo 71 podem então ser assinados com uma chave privada 82 para autenticar os dados

A unidade de CD-ROM 30 também pode incluir capacidades de criptografia e de assinatura (decodificador 32), as quais podem ser implementadas em hardware ou em software O decodificador 32 inclui um certificado de chave pública de cripto-placa 83, o qual é idêntico ao certificado 81, um certificado de produtor 84, para verificação da identidade do produtor, e uma chave de descriptografia de política de meio de distribuição 86 assinada pelo produtor, como mostrado na FIG 6 O certificado de cripto-placa 83 verifica a assinatura da cripto-placa 80 assinada com a chave privada 82 A chave de descriptografia de política 86 desencripta a política de acesso 155 armazenada no CD-ROM 35

O sistema computacional 10 pode ter vários níveis de segurança, tais como Nível 1 e Nível 2, descritos nos exemplos a seguir

Em um sistema com segurança de Nível 1, o receptor 70 comunica-se com o computador 20 via um controlador de dispositivo convencional 72 e o drive de CD-ROM 30 é um CD-ROM convencional Nem o receptor 70 nem o drive de CD-ROM 30 têm capacidades de criptografia / descriptografia adicionais Para uma segurança aumentada, o computador 20 em um sistema de Nível 1 pode ser um computador "seguro", o qual pode autenticar e/ou encriptar dados Em um sistema de Nível 2 mais seguro, o receptor 70 pode incluir uma cripto-placa 80 e o drive de CD-ROM 30 pode incluir um decodificador 32 O sistema de Nível 2 é projetado para prover autenticação de dados e transmissão de dados criptografados entre o receptor 70 e o decodificador 32 O computador 20 pode então ser qualquer computador convencional sem autenticação e criptografia de dados

O dados introduzidos via o teclado 50 e o mouse 60 podem in-

cluir uma entrada de comando e dados típica 130 introduzida via uma interface com usuário 95 (provida por um programa aplicativo 34) e uma ou mais senhas 130 que permitem que um usuário tenha acesso a uma informação armazenada no meio de distribuição de dados 35

O CD-ROM 35 armazena tipos diferentes de informação, tal como arquivos com informação 144, uma lista 150 de regiões geográficas autorizadas, uma lista 154 de intervalos de data / tempo autorizados, um ou mais arquivos de chave de descriptografia de arquivo 146, um ou mais arquivos de política 152 e uma assinatura 147 para todo o CD-ROM 35 Como visto na FIG 3, os arquivos 144, 146, 150, 152, 154 e 155 podem ser assinados e criptografados

Os arquivos 144 podem ser agrupados em subconjuntos 141, 142 e 143 Os arquivos podem pertencer a mais de um subconjunto (Na discussão a seguir, o termo arquivo refere-se a ambos arquivos e subconjuntos) Cada arquivo 141, 142 e 143 pode ser criptografado com uma única chave de criptografia 51 (E_1, E_2, E_3) As chaves de descriptografia de arquivo correspondentes 52 (K_1, K_2, K_3) são armazenados no CD-ROM 35 no arquivo de chave de desencriptação de arquivo 146 A informação adicional sobre as chaves de descriptografia e o arquivo de chave de descriptografia são encontrados na Patente U S No 5 646 992

Cada arquivo 141, 142 e 143 no CD-ROM 35 está associado a zero, uma ou mais regiões geográficas autorizadas armazenadas na lista 150 de regiões geográficas autorizadas Por exemplo, uma região pode ser limitada por latitudes e longitudes correspondentes à extensão do Empire State Building na Cidade de Nova York e a uma altitude entre 50 e 60 metros, de modo que o arquivo associado àquela região só possa ser aberto se o receptor 70 estiver localizado em uma certa área de escritório no interior do Empire State Building

Da mesma forma, cada arquivo 141, 142 e 143 está associado a zero, um ou mais dos intervalos de data / tempo autorizados armazenados na lista 154 de intervalos de data / tempo autorizados

Cada satélite de GPS 90 mantém um clock extremamente preci-

so O receptor 70 recebe os sinais de clock de GPS como parte dos sinais 75, ou um clock atômico local pode prover sinais de clock similares Os sinais de clock permitem um controle do acesso à informação baseado no tempo real em que o acesso à informação é tentado Por exemplo, o produtor pode especificar que o acesso seja garantido apenas (1) antes de uma data / um tempo predeterminado, (2) após uma data / um tempo predeterminado, ou (3) apenas durante um período de data / tempo predeterminado

O produtor pode associar os arquivos 141, 142 e 143 a itens específicos nas listas 150 e 154 via uma senha 130, a qual o usuário introduz via o teclado 50 A senha 130 pode ser uma senha de usuário válida por mais de um acesso, ou pode ser uma senha para uma única vez Alternativamente, o produtor pode associar informação específica de região geográfica / data / tempo de listas 150 e 154 com os arquivos 141, 142 e 143 via os arquivos de política 152 Uma senha de usuário válida 130 pode desbloquear um ou mais arquivos de política 152 Se a posição geográfica real do usuário e a data e o tempo atual estiverem na região geográfica autorizada e na data / no tempo autorizado correspondente à senha de usuário 150, então, o usuário pode ter acesso aos arquivos selecionados via a interface de usuário 95 A informação selecionada é então exibida no dispositivo de saída 40

A Tabela 1 mostra, como um exemplo, como cinco arquivos criptografados, A a F, armazenados no CD-ROM 35 e associados a regiões geográficas autorizadas e datas / tempos correspondentes, podem ser acessados Cada arquivo está associado a uma de quatro chaves de descriptografia de arquivo diferentes K1 a K4. L1 e L2 são as duas regiões geográficas autorizadas diferentes e T1, T2, e T3 são três intervalos de data / tempo autorizados O usuário que está de posse da chave de descriptografia de arquivo K1, por exemplo, uma senha, pode desencriptar o Manual A nas regiões geográficas L1 e L3 no tempo T1 O mesmo usuário também pode desencriptar o Manual D no mesmo tempo T1 nas regiões L2 e L3, mas não na região L1 Da mesma forma, o usuário que tem a chave K2 pode desencriptar a Imagem B e a Imagem E na região L2, mas não ao

mesmo tempo O Desenho C pode ser descriptografado com a chave K3 em qualquer lugar, mas apenas no tempo T3, enquanto o Relatório Comercial F requer a chave K4 e pode ser descriptografado em qualquer tempo, mas apenas na região L1

Tabela 1

Arquivo Cripto-grafado	Chave de Des-criptografia de Arquivo	Regiões Geográfi-cas Autorizadas	Intervalos de Data / Tempo Autorizados
Manual A	K1	L1, L3	T1
Imagem B	K2	L2	T1, T3
Figuras C	K3	--	T3
Manual D	K1	L2, L3	T1
Imagem E	K2	L2	T2
Relatório F	K4	L1	--

Como mostrado na FIG 3, para fins de assinatura criptográfica com criptografia opcional, o produtor seleciona arquivos fontes 144' a serem escritos no CD-ROM 35 e especifica uma lista de regiões geográficas autorizadas 150' e uma lista de intervalos de data e tempo autorizados 154' O produtor associa (como mostrado na Tabela 1) cada arquivo ou subconjunto de arquivos com zero, uma ou mais regiões geográficas 150' e zero, um ou mais intervalos de data / tempo 154' e armazena esta associação em um arquivo de política 152' Cada um dos arquivos 144', 150', 152', 154' pode ser assinado e criptografado nas etapas 53, 340, 350 e 360 com as chaves de criptografia correspondentes 51, 345, 355 e 365, respectivamente Os arquivos criptografados correspondentes 150, 152 e 154 são então armazenados juntos no CD-ROM 35 como uma política de acesso a região / tempo / arquivo criptografado assinado 155 Também são armazenados no CD-ROM 35, como mencionado acima, os arquivos assinados / criptografados 144, o arquivo de chave de arquivo simétrico assinado / criptografado 146 e a assinatura 147 usada pelo produtor para assinar todo o CD-ROM 35

Como visto nas FIG 4 e 5, para se ter acesso aos arquivos as-

sinados / criptografados 144, o usuário obtém uma senha 130 (FIG 2) a partir do produtor (etapa 400), e introduz a senha 130 via o teclado 50 (etapa 410) É assumido que a senha 130 seja uma senha para uma única vez, embora as senhas de usuário válidas por mais de uma sessão também possam ser usadas

Como visto na FIG 4, as porções iniciais do fluxo de processo para o Nível 1 e o Nível 3 são quase idênticas

A etapa 420 verifica a senha 130 e o processo então executa a etapa 440 (para o Nível 1, sem nenhuma segurança adicional) ou a 450 (para o Nível 2, com segurança de receptor / drive de CD-ROM), dependendo da configuração do sistema Os detalhes das etapas 440 e 450 são mostradas na FIG 5 e serão discutidos agora

Como visto na FIG 5, no processo 440, a senha de usuário 130 é enviada para o controlador de dispositivo 72 (etapa 510) Em resposta à senha de uso único 130, o controlador de dispositivo 72 gera a partir da senha de usuário 130 sua própria senha de uso único (etapa 520) e verifica (etapa 530) que o usuário de fato introduziu uma senha de uso único correto 130, desse modo autenticando o usuário para a sessão interativa (etapa 532) Caso contrário, o acesso é negado (etapa 535)

Uma vez que a senha 130 tenha autenticado o usuário, o controlador de dispositivo 72 interroga o receptor 70 quanto à posição e à data / tempo atuais (etapa 540) O controlador de dispositivo 72 então compara os dados de tempo e posição retornados pelo receptor 70 com a política 155, a qual se aplica aos arquivos 144 ou a um subconjunto 141, 142 e 143 dos arquivos (etapa 460) Se o usuário estiver autorizado a acessar os arquivos 144, então, o dado é desbloqueado, descriptografado (etapa 470, FIG 3) com as chaves de descriptografia 52 (etapa 480) e suprido para o programa aplicativo de usuário 34 (etapa 490) e exibido

Em um sistema de Nível 2, o receptor 70 inclui a placa de receptor criptográfico 80, a partir deste ponto referida como a "cripto-placa" Como mencionado antes, a cripto-placa 80 pode assinar e encriptar / desencriptar mensagens O drive de CD-ROM 30 inclui o decodificador 32

para decodificar os dados de posição assinados e recebidos a partir da cripto-placa 80

Como visto na FIG 5, no processo 450, a senha de usuário 130 é enviada para o controlador de dispositivo 72, o qual aceita a senha 130 e a passa inalterada para o decodificador 32 (etapa 550) O controlador 32 então gera internamente com a chave privada 86 sua própria senha de uso único correspondente à senha de usuário (etapa 560) e verifica (etapa 570) se a senha correta 130 foi comunicada pelo controlador de dispositivo 72, desse modo autenticando o usuário para a sessão interativa (etapa 572) Caso contrário, o acesso é negado (etapa 575)

Uma vez que o circuito de criptografia 32 tenha autenticado o usuário, o controlador 32 interroga a cripto-placa 80 via o controlador de dispositivo 72 quanto ao tempo atual e à informação de posição do receptor 70 (etapa 580) A unidade de decodificador 30 provê a cripto-placa 80 com um padrão randômico ou de outro bit assinado para formar um "vetor de inicialização" (etapa 590), isto é, um deslocamento de posição, o qual o controlador de dispositivo 72 passa através da cripto-placa 80 juntamente com a requisição pelo tempo e pela posição (etapa 590)

A cripto-placa 80 responde preparando um pacote de acordo com um formato de dados preestabelecido, o qual inclui o tempo atual e a posição geográfica real na latitude e longitude e altitude (etapa 600) Também pode ser incluída uma informação identificando os satélites transmitindo os dados de posição, bem como outros dados necessários para computações A cripto-placa 80 também armazena o vetor de inicialização provido a um deslocamento conhecido no pacote, e aplica uma assinatura criptográfica ao conteúdo do pacote A assinatura criptográfica pode ser, por exemplo, uma mensagem de compilação / reedição do pacote de dados, mais uma criptografia da compilação de mensagem, de acordo com alguma chave predeterminada, e pode ser simétrica ou assimétrica, dependendo da chave ou do certificado armazenado na cripto-placa 80

A cripto-placa 80 então transmite (etapa 605) o pacote de tempo/local assinado para o controlador de dispositivo 72, o qual envia o pa-

cote para o decodificador 32 / o drive de CD-ROM 30 O decodificador 32 compara a assinatura do pacote recebido da cripto-placa 80 com uma assinatura armazenada no decodificador 32 (etapa 610) Se a assinatura for verificada apropriadamente (etapa 620), o vetor de inicialização no pacote é examinado para se determinar se o vetor de inicialização é de fato o mesmo vetor de inicialização o qual o decodificador 32 proveu para a cripto-placa 80 na etapa 590 Se este for o caso, então o pacote recebido pelo decodificador 32 é recente e genuíno, e os dados de tempo e posição são aceitos como válidos

Uma vez que o pacote da cripto-placa 80 esteja autorizado, baseado na assinatura e no vetor de inicialização, o decodificador 32 compara os dados de tempo e posição recebidos da cripto-placa 80 com a política 155, a qual se aplica aos arquivos 144 ou a um subconjunto de arquivos 144 (etapa 460) Se o usuário estiver autorizado a acessar os arquivos 144, então o dado é desbloqueado (etapa 470), descriptografado com as chaves de descriptografia 52 (etapa 480) e suprido para o programa aplicativo do usuário 34 e exibido (etapa 490)

Outras modalidades estão no escopo das reivindicações a seguir Por exemplo, o receptor de GPS não precisa estar localizado na posição exata do leitor de meios de distribuição de dados, mas poderia estar em um local conhecido (tal como uma sala contendo um servidor de controle provendo serviços computacionais para uma rede de área local em um prédio) em relação ao leitor

Os arquivos de política 152' também podem designar regiões geográficas onde o acesso a certos arquivos 144 é negado

O controle sobre acesso a arquivos não precisa estar limitado ao uso de senhas providas pelo produtor e introduzidas via um teclado Por exemplo, certos atributos biométricos, tais como aspectos faciais, impressões digitais e/ou impressões vocais podem ser substituídos ou usados além das senhas

REIVINDICAÇÕES

1 Método para controle de acesso a informação armazenada, que compreende·

determinação de uma posição geográfica real onde a referida informação armazenada está localizada, baseado em sinais recebidos em um receptor suprindo uma informação de posição confiável,

comparação da referida posição geográfica real com uma região geográfica na qual o acesso à referida informação armazenada está autorizado, e

permissão de acesso à referida informação armazenada se a referida posição geográfica real estiver localizada na referida região geográfica autorizada

2 Método, de acordo com a reivindicação 1, onde o referido receptor compreende um receptor de GPS

3. Método, de acordo com a reivindicação 1, onde a referida informação é armazenada em um meio que pode ser lido em computador

4 Método, de acordo com a reivindicação 3, onde o referido meio que pode ser lido em computador é portátil

5 Método, de acordo com a reivindicação 3, onde o referido meio que pode ser lido em computador compreende um disco de alta capacidade

6 Método, de acordo com a reivindicação 1, onde a referida informação armazenada compreende arquivos e cada um dos referidos arquivos tem uma região geográfica associada na qual o acesso é permitido, e ainda permitindo acesso ao referido arquivo se a referida posição geográfica real estiver localizada na referida região geográfica autorizada para o referido arquivo

7 Método, de acordo com a reivindicação 6, que ainda compreende negar o acesso à referida informação armazenada se a referida posição geográfica real não se combinar à referida região geográfica autorizada

8 Método, de acordo com a reivindicação 1, que ainda compreende

criptografia da referida informação armazenada usando-se uma chave de criptografia, e

provisão de uma chave de descriptografia a qual permite a descriptografia da referida informação armazenada se a referida posição geográfica real estiver localizada na referida região geográfica autorizada

9 Método, de acordo com a reivindicação 1, que ainda compreende

assinatura de forma criptográfica da referida posição geográfica real com uma chave de criptografia de receptor, e

verificação da assinatura de receptor com uma chave de descriptografia de receptor antes da posição geográfica real ser comparada com a referida posição geográfica real

10 Método, de acordo com a reivindicação 1, onde a referida informação armazenada é dividida em subconjuntos de informação e onde pelo menos um dos subconjuntos tem uma região autorizada diferente dos outros subconjuntos, de modo que o acesso seja autorizado ao subconjunto cuja região geográfica autorizada esteja localizada na posição geográfica real, mas não aos subconjuntos cuja região geográfica autorizada não esteja localizada na posição geográfica real

11 Método, de acordo com a reivindicação 6, onde a referida associação de arquivos às regiões geográficas autorizadas é armazenada como um arquivo de política juntamente com a referida informação armazenada

12 Aparelho para o controle de acesso à informação armazenada, que compreende

um receptor que supre uma informação de posição confiável para determinação de uma posição geográfica real onde a referida informação armazenada está localizada, e

um computador para comparar a referida posição geográfica real com uma região geográfica na qual o acesso à referida informação armazenada está autorizado,

onde o referido computador permite acesso à referida informa-

ção armazenada se a referida posição geográfica real estiver localizada na referida região geográfica autorizada

13 Aparelho, de acordo com a reivindicação 12, onde o referido receptor é um receptor de GPS

14 Aparelho, de acordo com a reivindicação 12, onde o receptor ainda compreende um mecanismo de criptografia de receptor provendo uma chave de criptografia de receptor para assinar de forma criptográfica a referida posição geográfica real

15 Aparelho, de acordo com a reivindicação 14, que ainda compreende um leitor para leitura da referida informação armazenada, onde o referido leitor compreende uma chave de descriptografia de receptor, para verificação da referida posição real assinada de forma criptográfica

16 Aparelho, de acordo com a reivindicação 15, onde o referido leitor gera um vetor de inicialização provendo um deslocamento de posição o qual é transmitido para o receptor e adicionado à posição geográfica real

17 Aparelho, de acordo com a reivindicação 16, que ainda compreende um mecanismo de criptografia de leitor provendo uma chave de criptografia de leitor para assinar de forma criptográfica o deslocamento de posição, onde a referida assinatura de deslocamento de posição é verificada pelo receptor com uma chave de descriptografia de leitor correspondente, antes do deslocamento de posição ser adicionado à posição geográfica real

18 Método para o controle de acesso a um subconjunto de arquivos pertencentes a um conjunto de arquivos maiores de informação armazenada, que compreende

associação de uma única chave de criptografia de arquivo a cada arquivo do conjunto de arquivos maior e a criptografia dos arquivos usando-se as chaves de criptografia associadas,

associação de cada um dos arquivos de um conjunto de arquivos maior a pelo menos uma região geográfica autorizada na qual o acesso à referida informação armazenada está autorizado,

determinação de uma posição geográfica real onde a referida

informação armazenada está localizada baseado nos sinais recebidos em um receptor que supre uma informação de posição confiável,

comparação da referida posição geográfica real com a referida região geográfica autorizada, e

provisão de uma chave de descriptografia de arquivo, a qual autoriza o acesso e permite a descriptografia dos referidos arquivos pertencentes ao referido subconjunto de arquivos, desde que a posição geográfica real esteja localizada na região geográfica autorizada para os arquivos pertencentes ao referido subconjunto de arquivos

19 Método, de acordo com a reivindicação 18, onde a referida associação dos arquivos às regiões geográficas autorizadas é armazenada como uma política compreendendo arquivos de política, onde cada arquivo de política é acessível com uma senha de usuário e autoriza, se a senha de usuário for válida, o acesso aos arquivos listados no referido arquivo de política, se a posição geográfica real estiver localizada na região geográfica autorizada associada aos arquivos

20 Método, de acordo com a reivindicação 19, onde a referida política está armazenada com a informação armazenada

21 Método para o controle de acesso a uma informação armazenada, que compreende

determinação de uma data ou um tempo real no local da referida informação armazenada baseado em sinais recebidos em um receptor que supre uma informação de tempo confiável,

comparação da referida data ou tempo real com um intervalo de data ou tempo real predeterminado no qual o acesso à referida informação armazenada está autorizado, e

permissão de acesso à referida informação armazenada se a referida data ou o tempo real ocorrer no referido intervalo de data ou tempo autorizado

22 Método, de acordo com a reivindicação 21, que ainda compreende negar o acesso à referida informação armazenada se a referida data ou tempo real não ocorrer no referido intervalo de data ou tempo auto-

rizado

23 Método, de acordo com a reivindicação 21, onde a referida informação compreende arquivos, e cada um dos referidos arquivos tem um intervalo de data ou tempo autorizado associado no qual o acesso é permitido, e ainda permitindo acesso ao referido arquivo se a referida data ou tempo real ocorrer no referido intervalo de data ou tempo autorizado associado

24 Método, de acordo com a reivindicação 21,a onde a referida informação armazenada é dividida em subconjuntos de informação e onde pelo menos um dos subconjuntos tem um intervalo de data ou tempo autorizado diferente dos outros subconjuntos, de modo que o acesso seja autorizado ao subconjunto cujo intervalo de data ou tempo autorizado combinar-se à data ou ao tempo real, mas não aos subconjuntos cujo intervalo de data ou tempo autorizado não se combinar à data ou ao tempo real

25 Método para controle de acesso a uma informação armazenada, que compreende

formação de uma política associando a referida informação nas regiões geográficas autorizadas e os intervalos de tempo autorizados;

assinatura de forma criptográfica da referida política e da referida informação,

armazenamento da referida política assinada juntamente com a referida informação assinada,

provisão de uma senha para desbloquear a referida política, e

determinação de uma posição geográfica real onde a referida informação armazenada está localizada, baseado em sinais recebidos em um receptor que supre uma informação de posição confiável,

determinação de um tempo real,

comparação da referida posição geográfica real e do referido tempo real com as referidas regiões geográficas autorizadas e o intervalo de tempo autorizado da referida política, e

permissão de acesso à referida informação armazenada se a referida posição geográfica real e o tempo real caírem nas referidas regiões

geográficas autorizadas e no intervalo de tempo autorizado da referida política

26 Método, de acordo com a reivindicação 1, onde a fonte de posição e tempo confiáveis é um Sistema de Satélite de Navegação de Órbita Global

27 Método, de acordo com a reivindicação 1, onde a referida fonte de posição e tempo confiáveis é um sistema de navegação inerte

28 Método, de acordo com a reivindicação 1, onde a referida fonte de posição e tempo confiáveis é um sistema de determinação de localização baseado em satélite

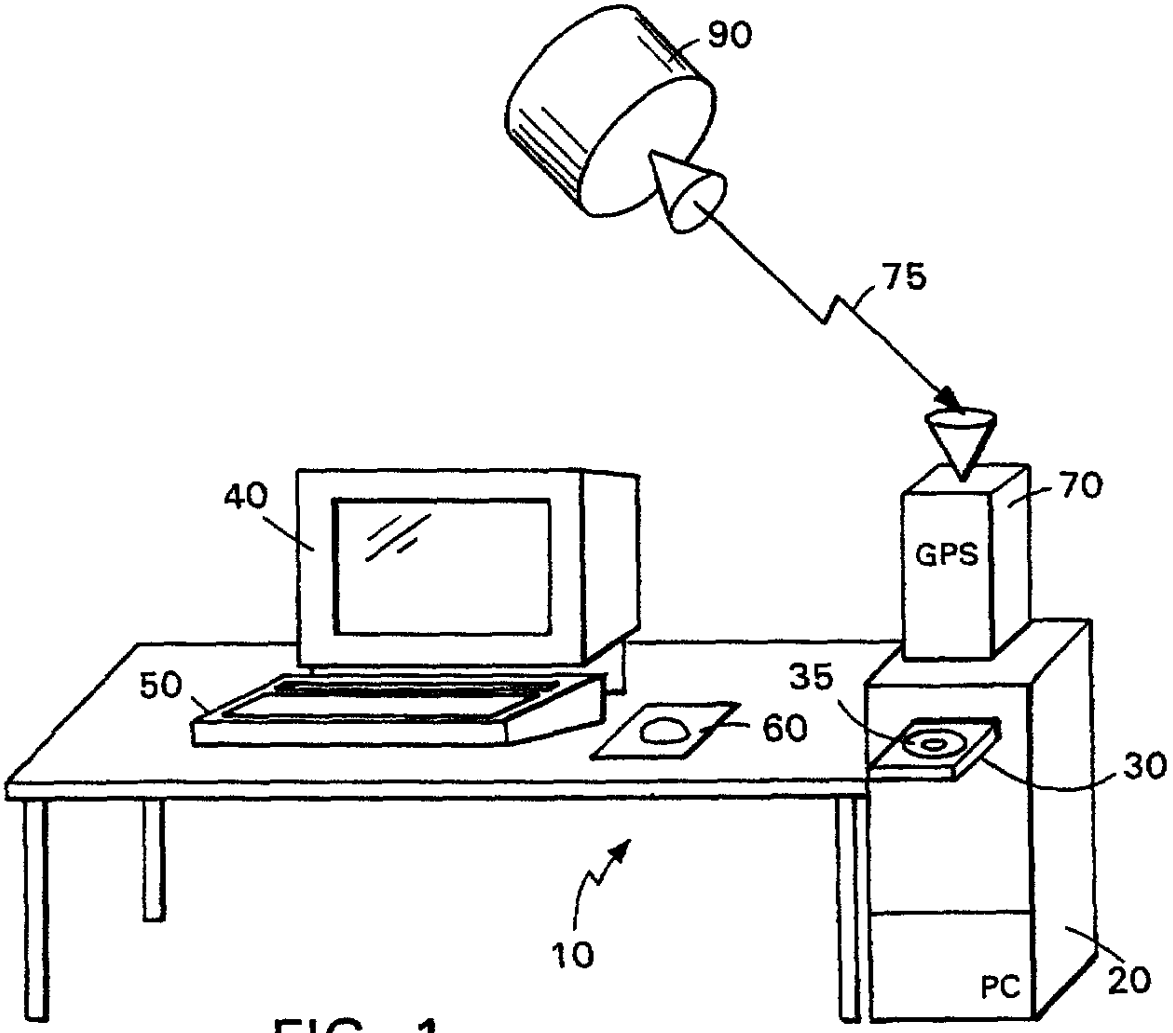
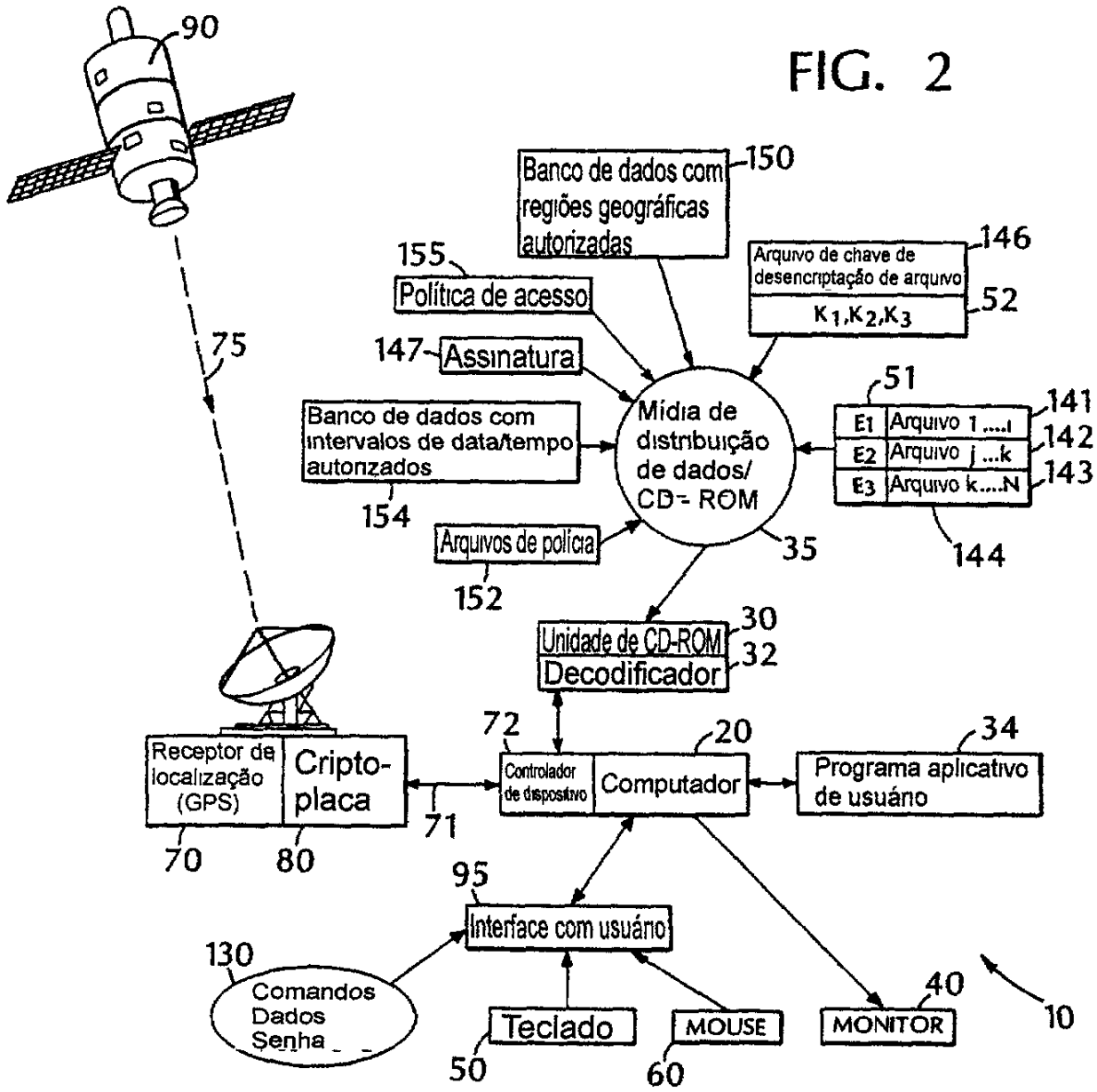


FIG. 1

FIG. 2


90
75
Banco de dados com regiões geográficas autorizadas
150
155
Política de acesso
146
Arquivo de chave de desencriptação de arquivo
K1,K2,K3
52
147
Assinatura
51
Banco de dados com intervalos de data/tempo autorizados
154
Mídia de distribuição de dados/ CD-ROM
35
E1 Arquivo 1 I
E2 Arquivo j ...k
E3 Arquivo k....N
141
142
143
144
Arquivos de polícia
152
Unidade de CD-ROM
Decodificador
30
32
72
20
34
Receptor de localização (GPS)
Cripto-placa
70
80
71
Controlador de dispositivo
Computador
Programa aplicativo de usuário
95
Interface com usuário
130
Comandos
Dados
Senha
Teclado
50
MOUSE
60
MONITOR
40
10

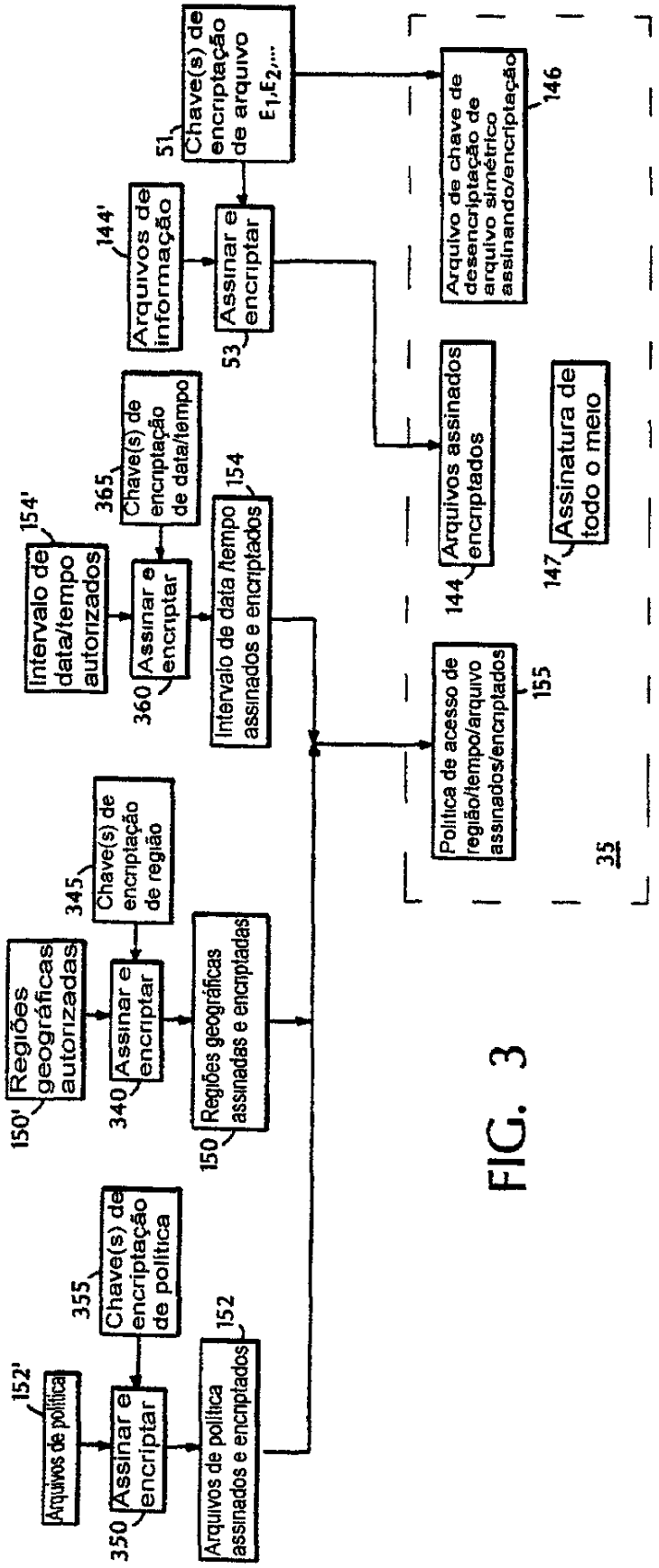
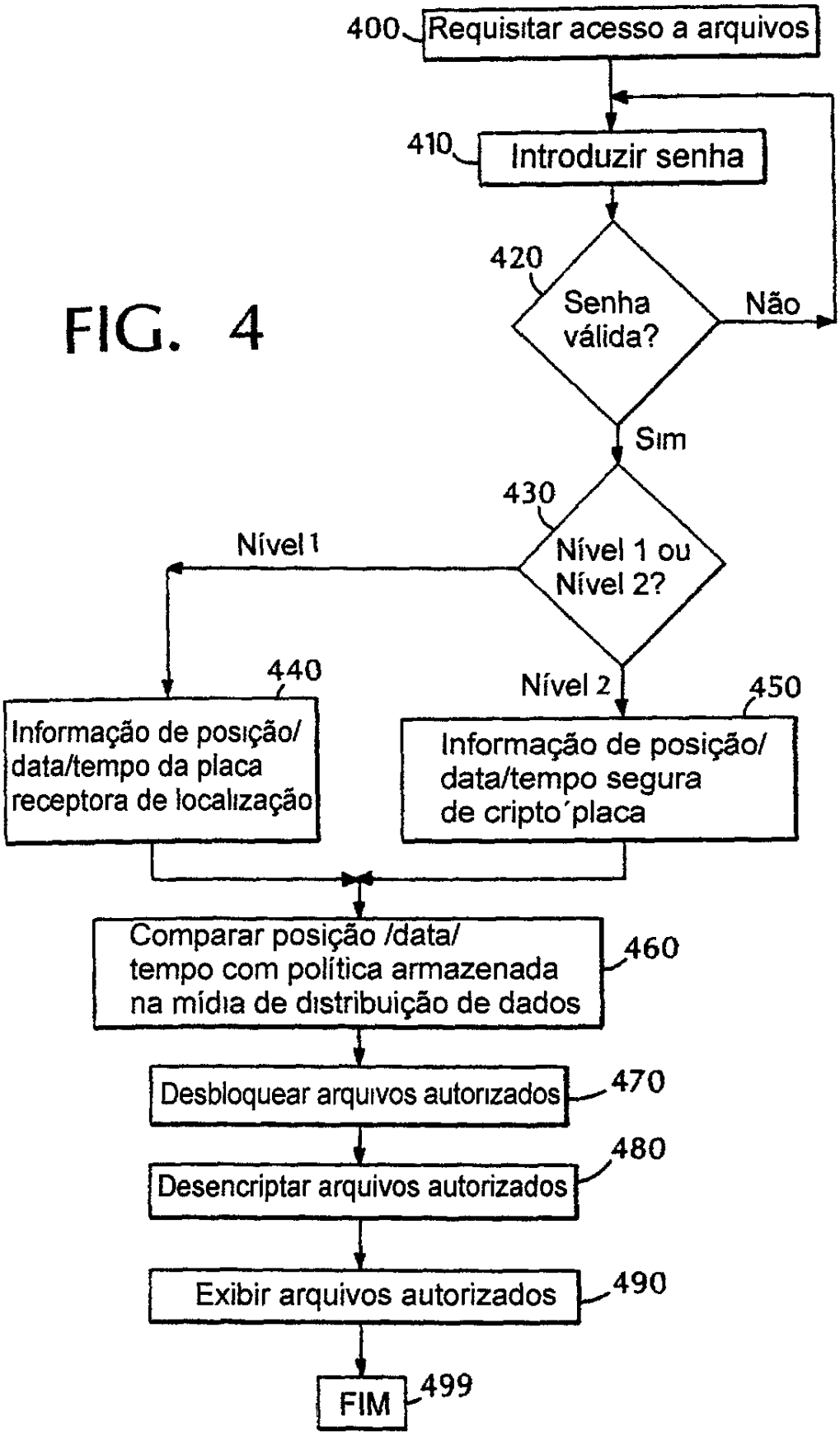

Arquivos de política
152'
Assinar e encriptar
350
Chave(s) de encriptação de política
355
Arquivos de política assinados e encriptados
152
Regiões geográficas autorizadas
150'
Assinar e encriptar
340
Chave(s) de encriptação de região
345
Regiões geográficas assinadas e encriptadas
150
Intervalo de data/tempo autorizados
154'
Assinar e encriptar
360
Chave(s) de encriptação de data/tempo
365
Intervalo de data /tempo assinados e encriptados
154
Política de acesso de região/tempo/arquivo assinados/encriptados
155
Arquivos de informação
144'
Assinar e encriptar
53
Chave(s) de encriptação de arquivo $E_1, E_2, \ldots$
51
Arquivos assinados encriptados
144
Assinatura de todo o meio
147
Arquivo de chave de desencriptação de arquivo simétrico assinando/encriptação
146
35

FIG. 3

FIG. 4


400
Requisitar acesso a arquivos
410
Introduzir senha
420
Senha válida?
Não
Sim
430
Nível 1 ou Nível 2?
Nível 1
Nível 2
440
Informação de posição/ data/tempo da placa receptora de localização
450
Informação de posição/ data/tempo segura de cripto´placa
Comparar posição /data/ tempo com política armazenada na mídia de distribuição de dados
460
Desbloquear arquivos autorizados
470
Desencriptar arquivos autorizados
480
Exibir arquivos autorizados
490
FIM
499

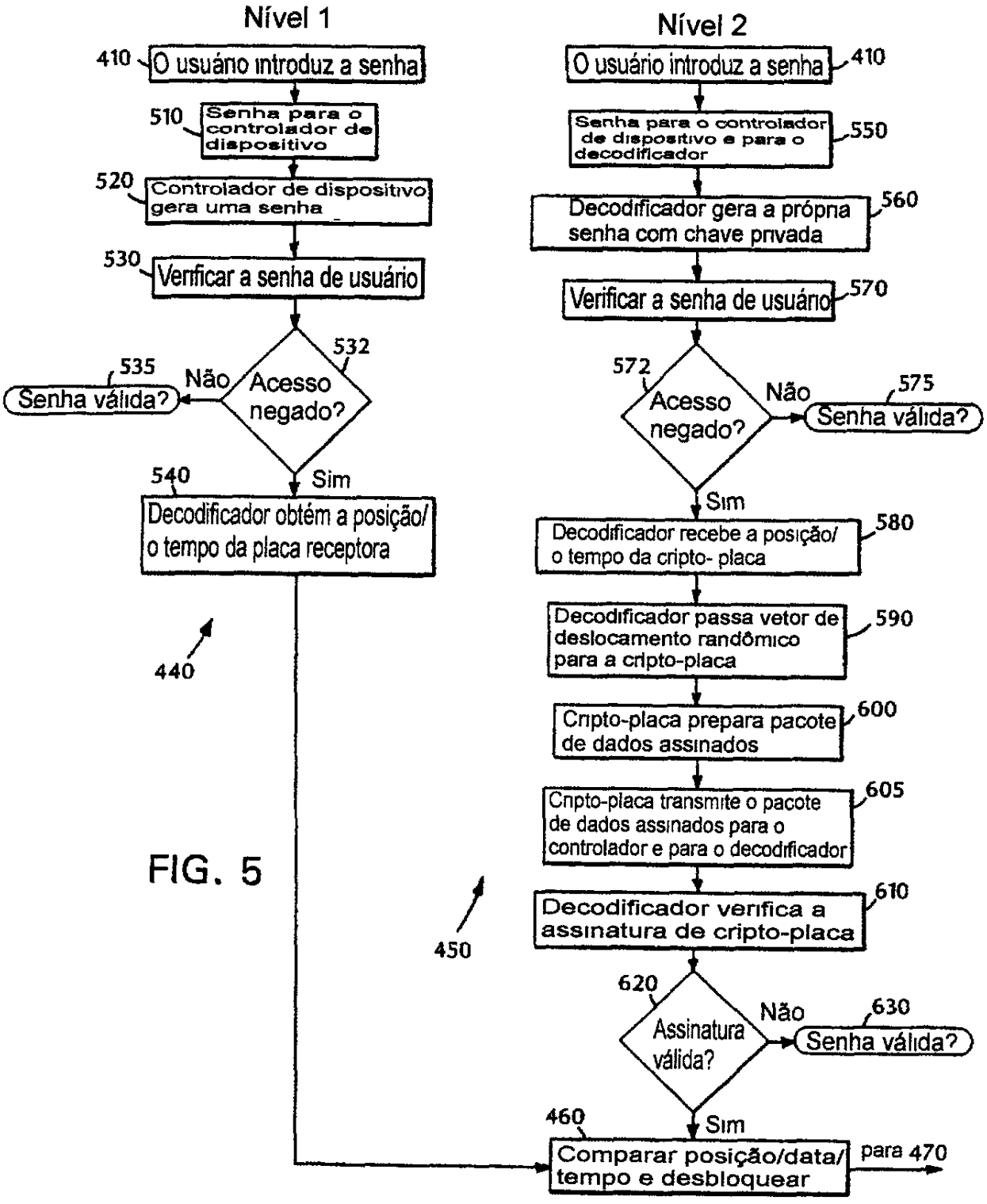

Nível 1
410
O usuário introduz a senha
510
Senha para o controlador de dispositivo
520
Controlador de dispositivo gera uma senha
530
Verificar a senha de usuário
532
Acesso negado?
Não
535
Senha válida?
Sim
540
Decodificador obtém a posição/ o tempo da placa receptora
440
Nível 2
O usuário introduz a senha
410
Senha para o controlador de dispositivo e para o decodificador
550
Decodificador gera a própria senha com chave privada
560
Verificar a senha de usuário
570
572
Acesso negado?
Não
575
Senha válida?
Sim
Decodificador recebe a posição/ o tempo da cripto- placa
580
Decodificador passa vetor de deslocamento randômico para a cripto-placa
590
Cripto-placa prepara pacote de dados assinados
600
Cripto-placa transmite o pacote de dados assinados para o controlador e para o decodificador
605
Decodificador verifica a assinatura de cripto-placa
610
450
620
Assinatura válida?
Não
630
Senha válida?
Sim
460
Comparar posição/data/ tempo e desbloquear
para 470

FIG. 5

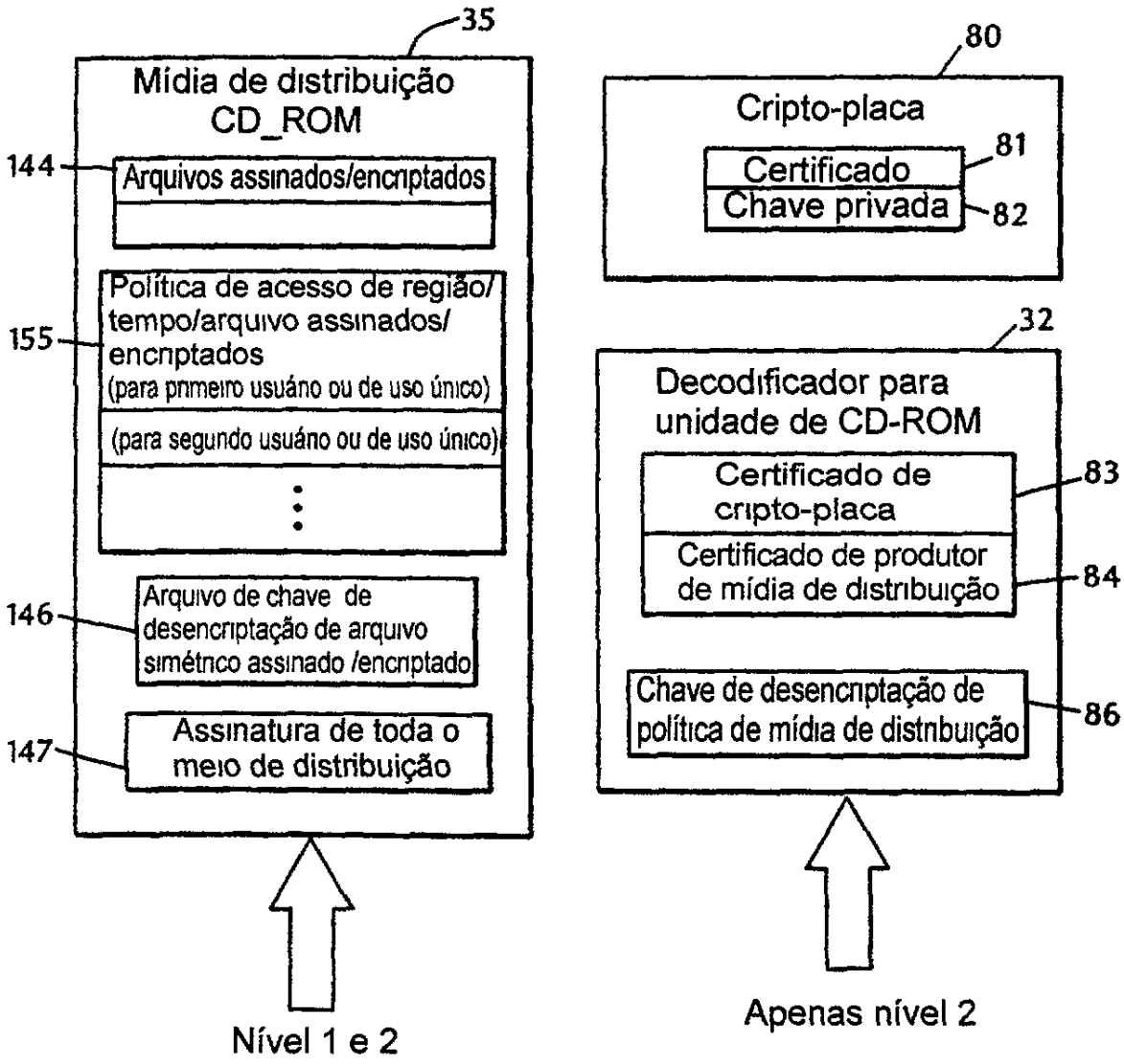

35
Mídia de distribuição CD_ROM
144
Arquivos assinados/encriptados
155
Política de acesso de região/ tempo/arquivo assinados/ encriptados
(para primeiro usuáno ou de uso único)
(para segundo usuáno ou de uso único)
146
Arquivo de chave de desencriptação de arquivo simétrico assinado /encriptado
147
Assinatura de toda o meio de distribuição
Nível 1 e 2
80
Cripto-placa
Certificado
81
Chave privada
82
32
Decodificador para unidade de CD-ROM
Certificado de cripto-placa
83
Certificado de produtor de mídia de distribuição
84
Chave de desencriptação de política de mídia de distribuição
86
Apenas nível 2

FIG. 6

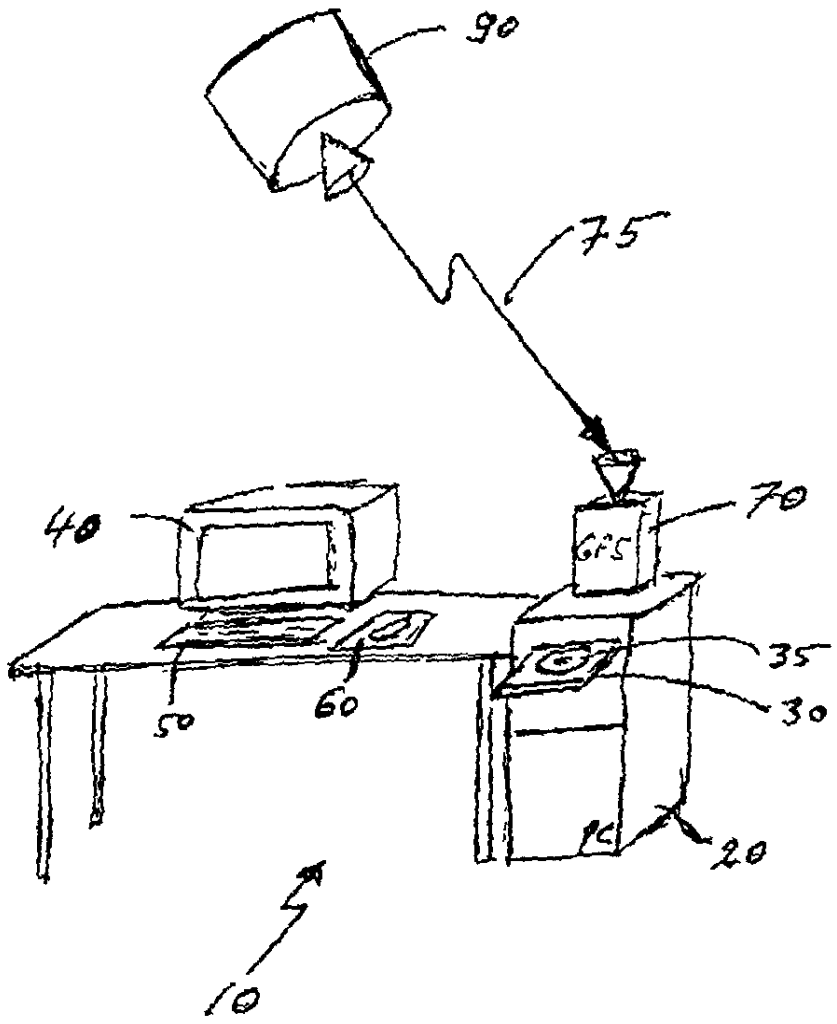


Fig. 1

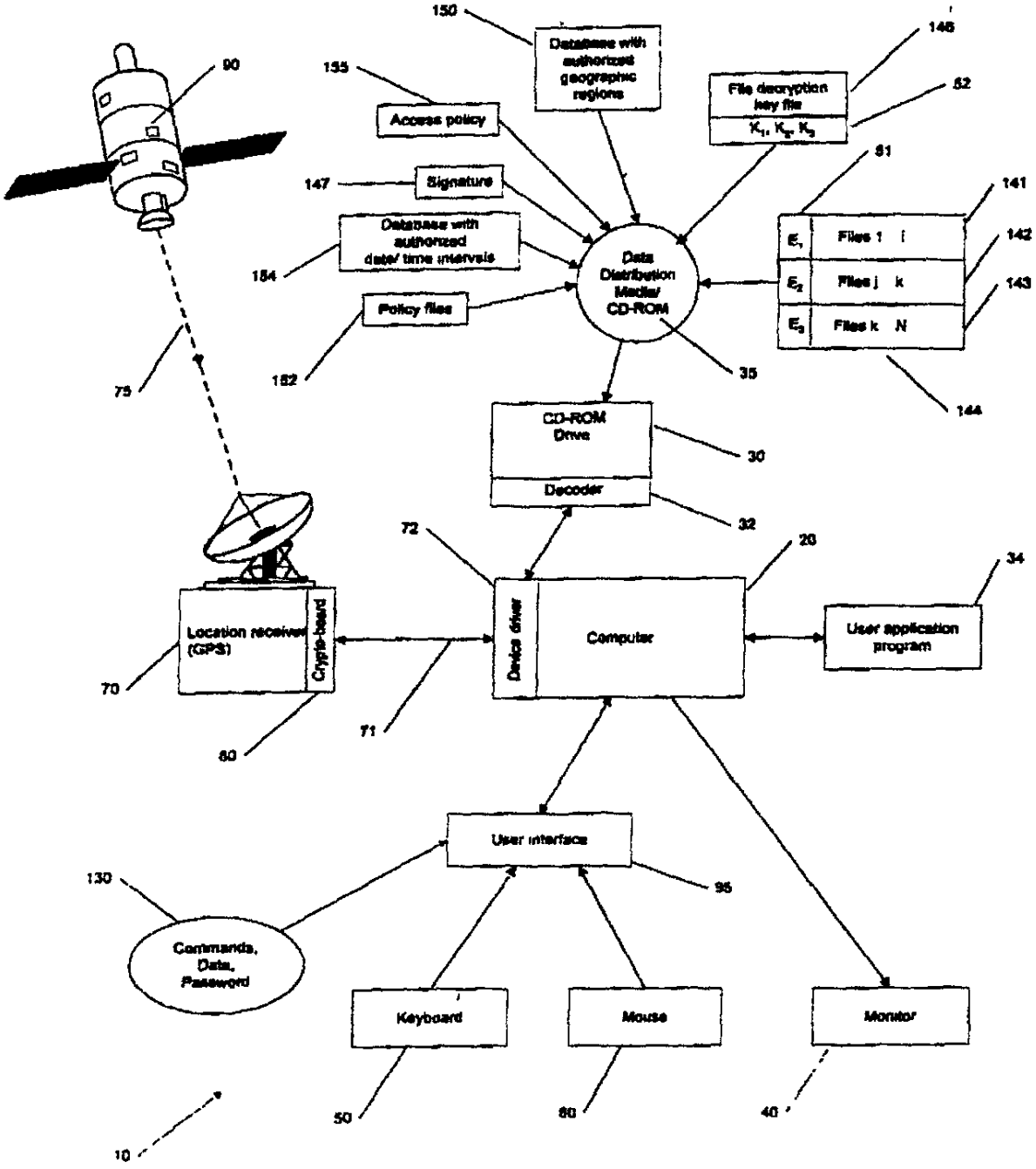

150
Database with authorized geographic regions
146
155
Access policy
File decryption key file
K_1, K_2, K_3
52
147
Signature
81
141
Database with authorized date/ time intervals
154
Data Distribution Media/ CD-ROM
E_1 Files 1 i
142
E_2 Files j k
143
Policy files
152
E_3 Files k N
35
144
75
CD-ROM Drive
30
Decoder
32
72
28
34
Location receiver (GPS)
Crypto-board
Device driver
Computer
User application program
70
71
60
User interface
130
95
Commands, Data, Password
Keyboard
Mouse
Monitor
50
80
40
10

FIG 2

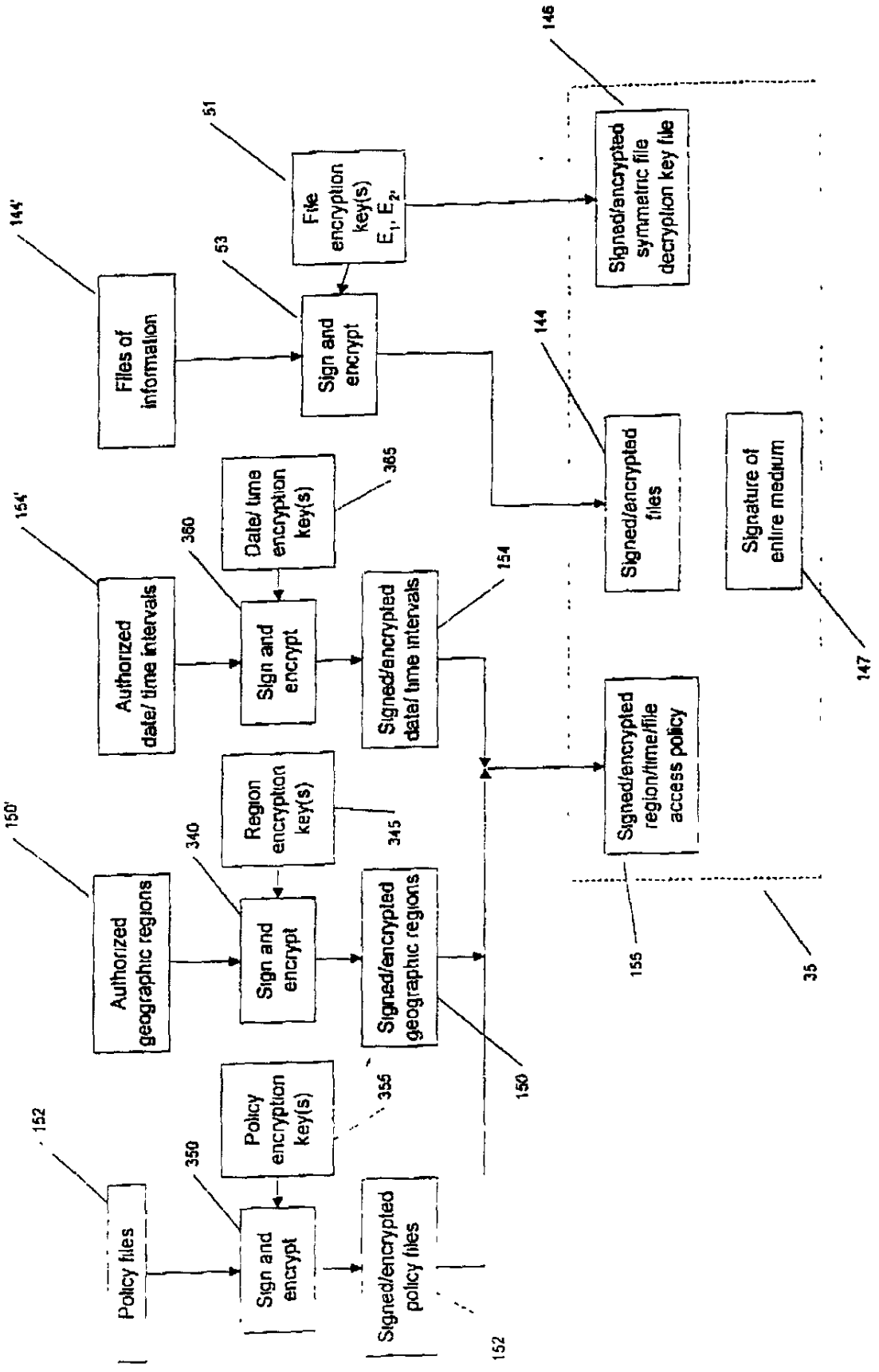

Policy files
Sign and encrypt
Signed/encrypted policy files
Policy encryption key(s)
Authorized geographic regions
Sign and encrypt
Signed/encrypted geographic regions
Region encryption key(s)
Authorized date/ time intervals
Sign and encrypt
Signed/encrypted date/ time intervals
Date/ time encryption key(s)
Files of information
Sign and encrypt
File encryption key(s) E_1, E_2,
Signed/encrypted symmetric file decryption key file
Signed/encrypted files
Signed/encrypted region/time/file access policy
Signature of entire medium
152
350
356
150'
340
345
154'
360
365
144'
53
51
146
144
154
150
155
147
35

FIG. 3

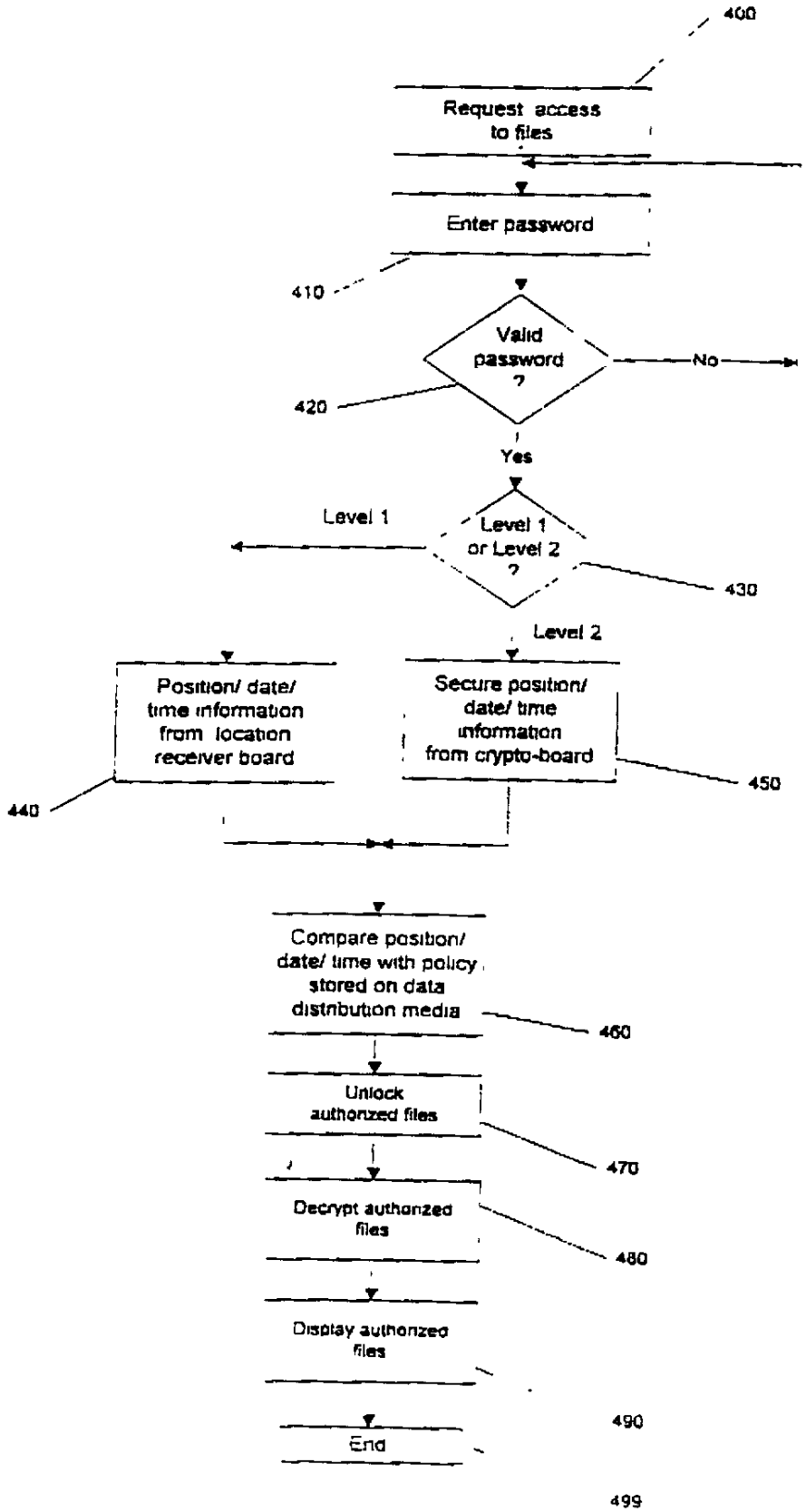

400
Request access to files
Enter password
410
Valid password ?
No
420
Yes
Level 1
Level 1 or Level 2 ?
430
Level 2
Position/ date/ time information from location receiver board
Secure position/ date/ time information from crypto-board
440
450
Compare position/ date/ time with policy stored on data distribution media
460
Unlock authorized files
470
Decrypt authorized files
480
Display authorized files
490
End
499

FIG. 4

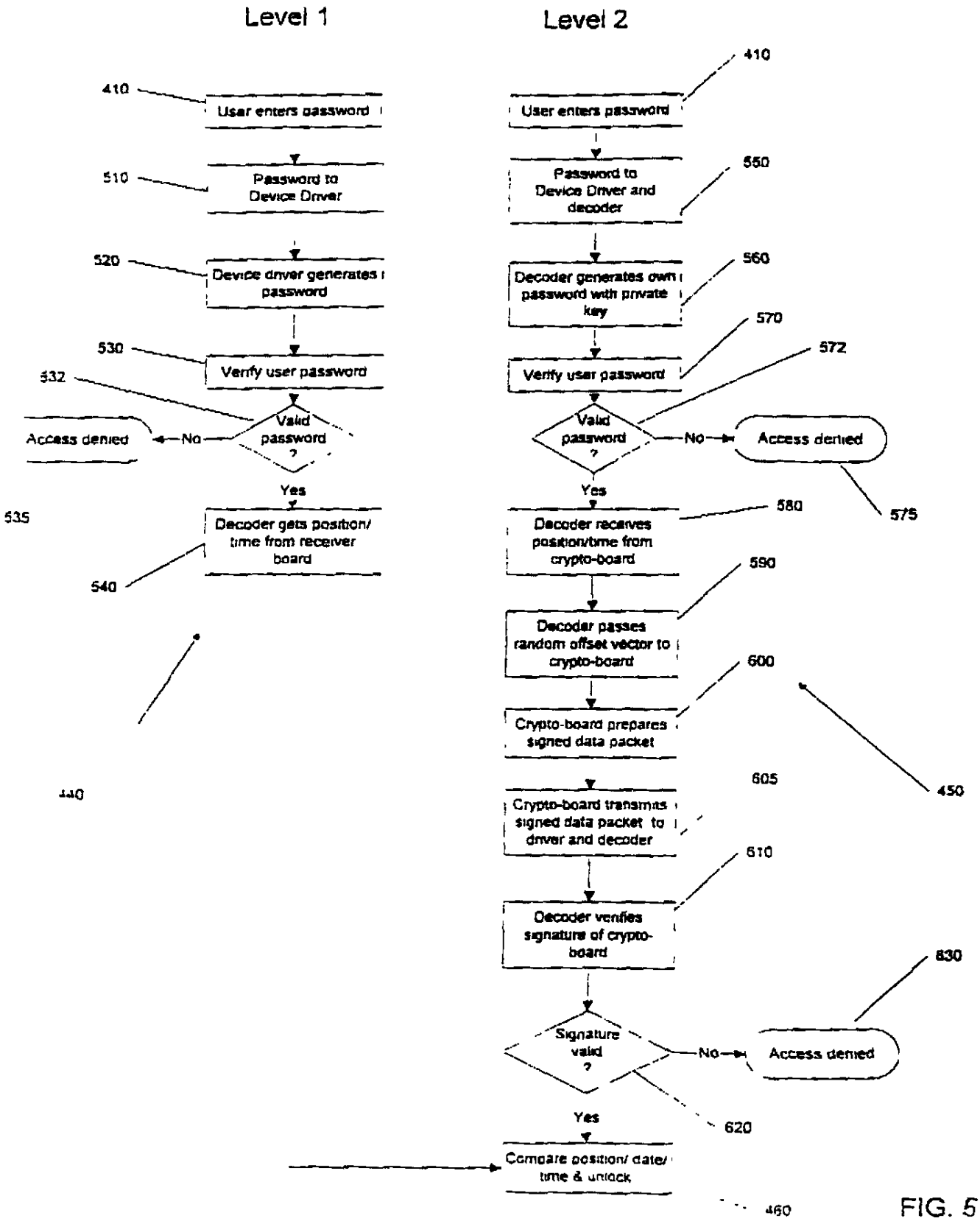

Level 1
Level 2
410
User enters password
510
Password to Device Driver
520
Device driver generates password
530
Verify user password
532
Valid password ?
No
Access denied
Yes
535
Decoder gets position/ time from receiver board
540
440
410
User enters password
550
Password to Device Driver and decoder
560
Decoder generates own password with private key
570
572
Verify user password
Valid password ?
No
Access denied
575
Yes
580
Decoder receives position/time from crypto-board
590
Decoder passes random offset vector to crypto-board
600
Crypto-board prepares signed data packet
605
Crypto-board transmits signed data packet to driver and decoder
610
Decoder verifies signature of crypto-board
830
Signature valid ?
No
Access denied
Yes
620
Compare position/ date/ time & unlock
460
450
470

FIG. 5

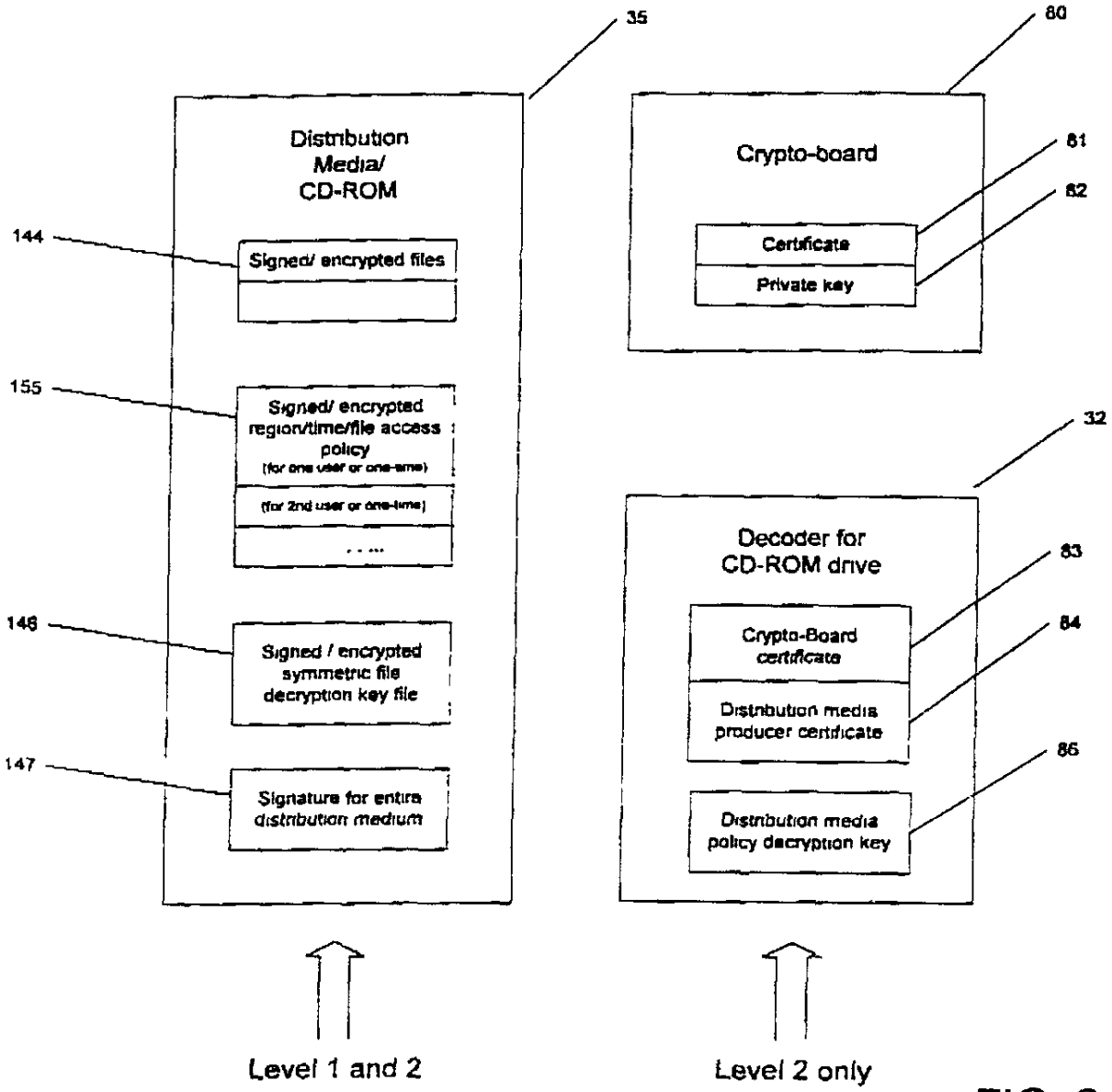

35
Distribution
Media/
CD-ROM
144
Signed/ encrypted files
155
Signed/ encrypted region/time/file access policy
(for one user or one-time)
(for 2nd user or one-time)
. . ...
148
Signed / encrypted symmetric file decryption key file
147
Signature for entire distribution medium
Level 1 and 2
80
Crypto-board
81
82
Certificate
Private key
32
Decoder for CD-ROM drive
83
Crypto-Board certificate
84
Distribution media producer certificate
86
Distribution media policy decryption key
Level 2 only

FIG. 6

RESUMO

Patente de Invenção **"CONTROLE DE ACESSO A UMA INFORMAÇÃO ARMAZENADA".**

O acesso a uma informação armazenada por um usuário é controlado comparando-se uma posição geográfica real e/ou uma data / um tempo real com uma região geográfica e/ou um intervalo de data / tempo no qual o acesso à informação armazenada está autorizado A posição geográfica real onde a informação armazenada está localizada e a data / o tempo real podem ser determinados, por exemplo, baseado em sinais recebidos em um receptor que supre informação de posição e de tempo confiável, tal como um receptor de GPS O acesso à informação armazenada é autorizado se a posição geográfica real e/ou a data / o tempo caírem na região geográfica e/ou no intervalo de data / tempo autorizado A informação de posição e de data / tempo suprida pelo receptor pode ser assinada de forma criptográfica e criptografada