

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

(21) **PI0613308-8 A2**

(22) Data de Depósito: 24/05/2006
(43) Data da Publicação: 28/12/2010
(RPI 2086)



(51) *Int.Cl.:*
G07C 9/00

(54) Título: **PROCEDIMENTO DE ACESSO POR UM TERMINAL DE DADOS A UM DENTRE VÁRIOS OBJETOS DE DADOS ARMAZENADOS EM UM DISPOSITIVO ELETRÔNICO, PRODUTO DE PROGRAMA DE COMPUTADOR, MÍDIA DE ARMAZENAGEM DIGITAL, DISPOSITIVO ELETRÔNICO, TERMINAL DE DADOS E DOCUMENTO DE IDENTIFICAÇÃO**

(30) Prioridade Unionista: 02/06/2005 DE 10 2005 025 806.6

(73) Titular(es): Bundesdruckerei GmbH

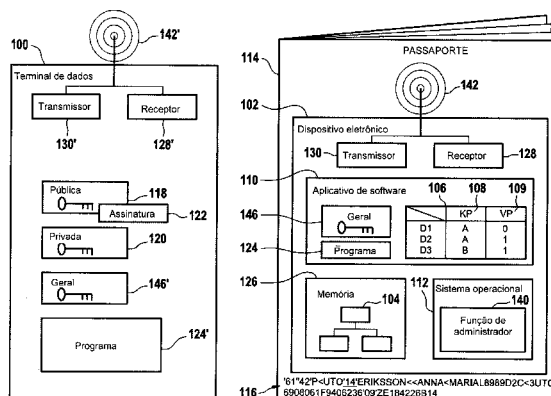
(72) Inventor(es): Kim Nguyen

(74) Procurador(es): Ricci & Associados Propriedade Intelectual S/S Ltda

(86) Pedido Internacional: PCT EP2006062619 de 24/05/2006

(87) Publicação Internacional: WO 2006/128829 de 07/12/2006

(57) Resumo: PROCEDIMENTO DE ACESSO POR UM TERMINAL DE DADOS A UM DENTRE VÁRIOS OBJETOS DE DADOS ARMAZENADOS EM UM DISPOSITIVO ELETRÔNICO, PRODUTO DE PROGRAMA DE COMPUTADOR, MÍDIA DE ARMAZENAGEM DIGITAL, DISPOSITIVO ELETRÔNICO, TERMINAL DE DADOS E DOCUMENTO DE IDENTIFICAÇÃO A presente invenção refere-se a um procedimento de acesso a um objeto de dado por meio de um terminal de dados, de uma pluralidade de objetos de dados armazenados em um dispositivo eletrônico, em que o dito dispositivo eletrônico compreende uma tabela de alocação em que diferentes níveis de segurança de protocolos criptográficos são designados a diferentes objetos de dados. O método da invenção consiste primeiro em transmitir um pedido para um objeto de dado escolhido por um terminal de dados a um dispositivo eletrônico, determinando o protocolo criptográfico para o objeto de dado escolhido, pelo dispositivo eletrônico com o auxílio da tabela de alocação, executando o protocolo criptográfico pelo dispositivo eletrônico e pelo terminal de dados, e transmitindo o objeto de dado escolhido ao terminal de dados, pelo dispositivo eletrônico na condição que o protocolo criptográfico é implementado com sucesso.





PROCEDIMENTO DE ACESSO POR UM TERMINAL DE DADOS
A UM DENTRE VÁRIOS OBJETOS DE DADOS ARMAZENADOS EM UM
DISPOSITIVO ELETRÔNICO, PRODUTO DE PROGRAMA DE
COMPUTADOR, MÍDIA DE ARMAZENAGEM DIGITAL, DISPOSITIVO
5 ELETRÔNICO, TERMINAL DE DADOS E DOCUMENTO DE IDENTIFICAÇÃO
Descrição

A presente invenção refere-se a um procedimento para o acesso a
um dispositivo eletrônico por meio de um terminal de dados, bem como um
produto de programa de computador, uma mídia de armazenagem digital, um
10 dispositivo eletrônico, um documento de identificação e um terminal de dados.

Os procedimentos para se armazenar dados eletronicamente sob
proteção criptográfica já são bem conhecidos desde o mais recente estado da
técnica. Uma forma de armazenagem protegida que encontrou ampla aceitação
ao longo das duas últimas décadas está em cartões de chip eletrônico,
15 padronizados pelas Seções de 1 a 4 da ISO 7816. Uma das áreas de aplicação
mais importantes para a tecnologia de cartões com chips no futuro é a
introdução de documentos de viagem com leitura eletrônica. Os benefícios
previstos incluem um aumento na segurança, bem como maior eficiência no
check-in de passageiros, especialmente em termos de viagens aéreas globais.
20 Ao longo dos últimos anos, a Organização Internacional de Aviação Civil (ICAO)
têm fornecido padrões para documentos de viagem com leitura eletrônica.

A armazenagem segura de dados pessoais em documentos de
viagem com leitura eletrônica anda lado a lado com a meta de se simplificar as
inspeções de segurança pelo maior número possível de organizações
25 governamentais e não-governamentais, além da definição dos dados pessoais
que devem ser protegidos de leituras sem autorização. O equilíbrio adequado
entre as duas necessidades deve permitir tanto as diferenciações nos métodos
de proteção legal de dados, como as variações nos objetos com dados
individuais que devam merecer proteção.

30 Um sistema foi derivado do US 2005/0097320A1, que permite a
comunicação entre um usuário e uma instituição, como um banco, por exemplo.
A comunicação é feita por meio de uma rede. Uma "avaliação de risco na
transação" ocorre [é gerada] toda vez que o usuário acessa o sistema da

instituição, que determina o risco da transação atual.

Um sistema semelhante é conhecido a partir do US 2002/0087894 A1, onde o próprio usuário seleciona o nível de segurança para a transferência de dados.

- 5 Com base no documento "*Machine Readable Travel Documents, Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, 1. October 2004, International Civil Aviation Organization*" [Documentos de Viagem com Leitura Eletrônica, Relatório Técnico, PKI para Documentos de Viagem com Leitura Eletrônica que oferecem
- 10 Acesso ICC Somente-Leitura, Versão 1.1 de 01 de outubro de 2004, Organização Internacional de Aviação Civil], publicado pela Autoridade da Secretaria Geral, páginas de 1 a 57, os procedimentos para o Controle Básico de Acesso são conhecidos e têm a finalidade de garantir que o acesso ao chip de um documento de viagem não possa ocorrer sem o conhecimento do
- 15 portador do documento de identificação. Os procedimentos são também utilizados para proteger a chamada "Troca do Chip". A única revelação relativa ao Controle de Acesso Estendido é a de que isso pode ser baseado em um processo de codificação simétrico ou assimétrico.

- Por outro lado, a invenção tem base na tarefa de se criar melhores
- 20 procedimentos para o acesso a um dispositivo eletrônico por um terminal de dados, um produto de programa de computador, uma mídia de armazenagem digital, um dispositivo eletrônico, um terminal de dados e um documento de identificação.

- Os objetivos da invenção são alcançados pelos aspectos
- 25 apresentados nas reivindicações independentes 1, 10, 13, 14, 28, 36 e 37. As configurações preferidas são especificadas reivindicações dependentes.

- De acordo com a invenção, um procedimento é fornecido para o acesso de um terminal de dados a um dentre vários objetos de dados armazenados em um dispositivo eletrônico, sendo que tal dispositivo eletrônico
- 30 possui uma tabela de alocação na qual um protocolo criptográfico com diferentes níveis de segurança é atribuído a diferentes objetos de dados. Primeiro o terminal de dados transmite uma solicitação ao dispositivo eletrônico para obter um dado específico entre todos os dados. Com o auxílio da tabela de

alocação, o dispositivo eletrônico especifica um protocolo criptográfico para aquele dado específico. O dispositivo eletrônico e o terminal de dados implementam o protocolo criptográfico. Pressupondo-se uma implementação bem sucedida, o dispositivo eletrônico transmite aquele objeto de dado para o
5 terminal de dados.

A presente invenção possui uma vantagem particular ao permitir que os objetos de dados classificados como merecedores de diferentes níveis de proteção, que são armazenados juntos em um dispositivo eletrônico que atua como portador de dados, sejam protegidos em diferentes graus e, dessa forma,
10 estejam em conformidade flexível com as demandas conflitantes de acesso aos objetos de dados armazenados.

De acordo com uma configuração desta invenção, o dispositivo eletrônico possui um aplicativo de software que contém a tabela de alocação. Com o auxílio da tabela de alocação, o aplicativo de software determina o
15 protocolo criptográfico, implementa o protocolo criptográfico específico com o terminal de dados e o aplicativo de software e, pressupondo-se o sucesso disso, envia o objeto de dado selecionado para o terminal de dados. Conseqüentemente, todas as etapas do procedimento do dispositivo eletrônico são implementadas pelo aplicativo de software, que possui a vantagem de o
20 dispositivo eletrônico ser desenvolvido com o uso de hardware padronizado e tendo boa relação custo-benefício, além do fato de que o nível de proteção criptográfica dos objetos de dados pode ser facilmente adaptado às exigências individuais.

De acordo com uma configuração desta invenção, o dispositivo eletrônico possui um sistema operacional que evita alterações não autorizadas ou a remoção do aplicativo de software, permitindo apenas o acesso aos objetos de dados por meio do aplicativo de software. Esta função do sistema operacional garante que a proteção dos objetos de dados implementada pelo aplicativo de software não possa ser contornada ou violada por alguém não
25 autorizado. Preferivelmente, no entanto, o sistema operacional permite a alteração ou remoção do aplicativo de software após a autenticação de um administrador do dispositivo eletrônico. Isto é particularmente vantajoso porque a alocação de objetos de dados individuais a protocolos criptográficos ou os
30

próprios protocolos criptográficos podem ser alterados, por exemplo, sem a necessidade de troca do dispositivo eletrônico. De uma maneira preferida, mas não limitada, a invenção diz respeito a um aplicativo de software que implementa o método de um cartão de chip, especialmente um Java-Applet para
5 um cartão de chip com um sistema operacional que inclui uma máquina virtual Java.

De acordo com uma configuração da invenção, o dispositivo eletrônico é integrado a um documento de identificação. Os documentos de identificação podem incluir, por exemplo, cartões de chip no formato de cartões
10 de saque ou documentos de outros formatos, como passaportes ou vistos, nos quais o dispositivo eletrônico é embutido. Especificamente, o documento de identificação pode pertencer a um documento de viagem com leitura eletrônica, de acordo com as padronizações de passaportes eletrônicos (*ePassport*) da Organização Internacional de Aviação Civil, ICAO. A ICAO define um sistema de
15 arquivos de acordo com o padrão de cartões de chip ISO 7816-4 para documentos de viagem com leitura eletrônica que possuam a designação *Logical Data Structure* (LDS) [Estrutura Lógica de Dados], bem como uma estrutura interoperável de dados armazenados no sistema de arquivos.

De acordo com uma configuração da invenção, ao menos um dos
20 objetos de dados inclui dados de biometria pessoal. No caso de um documento de viagem com leitura eletrônica em conformidade com as padronizações de *ePassport*, os nomes dos caminhos e formatos de arquivos de dados pessoais – e também biométricos – são dispostos pelo LDS. Especificamente, a armazenagem de dados de uma fotografia, de impressões digitais e da íris do
25 portador do documento de identificação é padronizada. A configuração possui uma vantagem particular, uma vez que um nível diferente, talvez com menor necessidade de proteção, por exemplo, e, portanto, com um protocolo criptográfico com um nível de segurança menor, pode ser atribuído à fotografia e não aos dados da íris e das impressões digitais.

30 Dependendo da configuração da invenção, o repertório dos protocolos criptográficos disponíveis para o dispositivo eletrônico e para o terminal de dados pode ser composto de diferentes protocolos e a alocação dos objetos de dados individuais contidos no dispositivo eletrônico pode ser definida

de formas diferentes para os protocolos criptográficos individuais disponíveis. De acordo com a invenção, o acesso à leitura pode ser garantido livremente, ligado à implementação de um protocolo criptográfico, ligado à implementação de um dentre diversos protocolos criptográficos disponibilizados para escolha, ou
5 ligado à implementação obrigatória de diversos protocolos criptográficos. Preferivelmente, o acesso livre é atribuído a, pelo menos, um dentre os vários objetos de dados na tabela de alocação, sem um protocolo criptográfico obrigatório.

De acordo com uma configuração da invenção, um protocolo
10 criptográfico com nível de segurança mais alto é atribuído a, pelo menos, um objeto de dado que requer autenticação do terminal de dados para o dispositivo eletrônico por meio de um procedimento de Solicitação-Resposta, o qual se baseia em um algoritmo criptográfico simétrico. Uma chave específica do dispositivo é utilizada aqui, que deve ser derivada pelo terminal de dados a partir
15 dos dados impressos de leitura eletrônica associados ao dispositivo eletrônico. Uma chave geral que deve ser conhecida por todos os dispositivos eletrônicos e terminais de dados pode também ser necessária para se derivar a chave específica do dispositivo.

De acordo com uma configuração da invenção, um protocolo
20 criptográfico de nível de segurança mais alto é atribuído a, no mínimo, um objeto de dado que requer autenticação do terminal de dados, no que diz respeito ao dispositivo eletrônico, por meio de um procedimento de Solicitação-Resposta baseado em um algoritmo criptográfico assimétrico. O terminal de dados possui uma chave pública e uma chave privada nesse caso. O terminal de dados envia
25 ao dispositivo eletrônico sua chave pública, que é preferivelmente fornecida com uma assinatura digital que pode ser verificada pelo dispositivo eletrônico por meio de uma cadeia certificada. Em seguida, o terminal de dados comprova ao dispositivo eletrônico, em uma sequência de Solicitação-Resposta, que também possui uma chave privada associada. Preferivelmente, a implementação do
30 protocolo criptográfico de nível de segurança mais alto é necessária, além do protocolo de nível de segurança elevado.

De acordo com uma configuração da invenção, a comunicação entre o terminal de dados e o dispositivo eletrônico não inclui contato,

preferencialmente por meio de uma interface sem contato que corresponde às normas ISO/IEC 14443, Partes 1 a 4, conforme estipulado pela ICAO no caso de documentos de viagem com leitura eletrônica. Para evitar o monitoramento não autorizado da comunicação sem contato por terceiros, é preferível também atribuir um protocolo de encriptação com um nível de segurança diferente para [os] diferentes objetos de dados na tabela de alocação, segundo o qual o terminal de dados e o dispositivo eletrônico comunicam-se de forma codificada. Dessa forma, o terminal de dados e o dispositivo eletrônico intercambiam, preferivelmente, a chave da sessão de forma segura.

10 Em outros aspectos, as configurações preferíveis da invenção são explicadas em mais detalhes com referências aos desenhos. Eles incluem:

Figura 1 um diagrama de blocos de uma configuração do terminal de dados e o dispositivo eletrônico, de acordo com a invenção,

Figura 2 um fluxograma do método, de acordo com a invenção,

Figura 3 um fluxograma das etapas do procedimento implementadas por uma configuração do dispositivo eletrônico, de acordo com a invenção, e

Figura 4 um fluxograma das etapas do procedimento implementadas por uma configuração do terminal de dados, de acordo com a invenção.

A Figura 1 mostra um diagrama de blocos de uma configuração do terminal de dados 100 e do dispositivo eletrônico 102, o qual está integrado em um documento de identificação 114. O documento de identificação é apresentado como um passaporte em perspectiva, de forma esquemática, e possui uma zona de dados impressos para leitura eletrônica 116. A integração do dispositivo eletrônico dentro do documento de identificação pode ser feita, por exemplo, embutindo-o na capa ou na página principal de um passaporte.

Tanto o dispositivo eletrônico 102 como o terminal de dados 100 podem possuir uma interface sem contato 142 ou 142', a qual é conectada a um transmissor 130 ou 130' e a um receptor 128 ou 128', facilitando a comunicação sem contato entre o terminal de dados e o dispositivo eletrônico. O dispositivo eletrônico 102 pode possuir uma memória 126 para diversos objetos de dados

104. Dados biométricos pessoais, tais como fotografia, impressões digitais, ou dados da íris do proprietário do documento de identificação 114 podem ser armazenados em um ou mais objetos de dados 104. A armazenagem dos objetos de dados 104 na memória 126 pode seguir o padrão de série 9303
5 "*Machine-readable Travel Documents*" [Documentos de Viagem com Leitura Eletrônica] da Organização Internacional de Aviação Civil, ICAO. Sob a designação "*Logical Data Structure*" (LDS) [Estrutura Lógica de Dados], a ICAO define o sistema de arquivos que se conforma ao padrão de cartões de chip ISO 7816-4, bem como uma estrutura interoperável dos objetos de dados
10 armazenados neste sistema de arquivos.

O terminal de dados 100 pode ser programado com instruções executáveis por computador 124', permitindo-lhe o acesso à leitura de objetos de dados 104 armazenados na memória 126 do dispositivo eletrônico 102 por meio de interfaces sem contato 142' e 142. Para proteger os dados biométricos
15 pessoais, especialmente de leituras não autorizadas, o dispositivo eletrônico 102 possui instruções de programa 124 que podem ligar o acesso à leitura de objetos de dados 104 à implementação bem sucedida de um protocolo criptográfico com o terminal de dados 100. Tal medida é recomendada pela ICAO, que menciona também o suporte a diversas opções de proteção de
20 dados como um requisito obrigatório do LDS padronizado.

Diversos tipos de dados biométricos pessoais que merecem proteção em diversos níveis podem ser armazenados em diferentes objetos de dados 104. Por exemplo, apenas uma leve sensibilidade pode ser atribuída a uma fotografia, enquanto as impressões digitais ou os dados da íris possam
25 merecer um alto nível de proteção. As diversas avaliações da necessidade de proteção de diferentes objetos de dados 104 são codificadas pela tabela de alocação 106 do dispositivo eletrônico 102. A cada objeto de dado 104 na tabela de alocação é atribuído um protocolo criptográfico 108 com um nível de segurança diferente. A tabela de alocação pode atribuir livre acesso sem a
30 implementação obrigatória de um protocolo criptográfico a um ou mais objetos de dados 104.

Em operação, o dispositivo eletrônico 102 recebe do terminal de dados 100 uma solicitação para um dos objetos de dados 104 por meio do

receptor 128 e da interface sem contato 142. Em seguida, utilizando-se da tabela de alocação 106, o dispositivo eletrônico especifica um protocolo criptográfico 108, cuja execução bem sucedida é definida como uma condição para o acesso do terminal de dados à leitura de um dos objetos de dados. O

5 dispositivo eletrônico e o terminal de dados executam o protocolo criptográfico e, se bem sucedido, o dispositivo eletrônico transmite o objeto de dado ao terminal de dados.

O dispositivo eletrônico 102 pode conter um aplicativo de software 110, que inclui uma tabela de alocação 106. Sendo assim, o protocolo

10 criptográfico 108 é especificado pelo aplicativo de software, o protocolo criptográfico é executado pelo terminal de dados e pelo aplicativo de software, e o objeto de dado é transmitido pelo aplicativo de software. O dispositivo eletrônico pode conter um sistema operacional 112, o qual, ao trabalhar junto com o hardware do dispositivo eletrônico, previne qualquer alteração não

15 autorizada ou remoção do aplicativo de software, permitindo apenas o acesso aos objetos de dados 104 por meio do aplicativo de software. Dessa forma, é possível implementar o dispositivo eletrônico 102 por produção em massa, com hardware padronizado, enquanto, as especificações dos protocolos criptográficos estão sendo usados e a alocação codificada dos objetos de dados

20 104 na tabela de alocação 126 podem ser adaptadas aos protocolos criptográficos de diferentes requisitos. O dispositivo eletrônico pode ser um cartão Java com uma máquina Java virtual, no qual o aplicativo de software 110 é instalado na forma de um Java Applet.

O sistema operacional 112 pode proteger o aplicativo de software

25 110, incluindo a tabela de alocação 126, de alterações ou remoções não autorizadas, ao mesmo tempo em que possui uma função de administrador 140 que permite a alteração ou remoção do aplicativo de software após a autenticação do administrador do dispositivo eletrônico 102. A função de administrador é particularmente vantajosa, uma vez que o dispositivo eletrônico

30 pode ser adaptado a requisitos revisados, ao invés de substituído por um novo dispositivo eletrônico. Os requisitos revisados podem pertencer, por exemplo, a protocolos criptográficos 108 melhorados, ou a revisão da classificação de merecimento de proteção de diferentes objetos de dados 104.

Vários protocolos de codificação 109 podem também ser atribuídos a diferentes objetos de dados na tabela de alocação 106, segundo o qual o dispositivo eletrônico 102 e terminal de dados 100 podem codificar sua comunicação. A codificação é particularmente vantajosa, uma vez que ela
5 permite evitar que terceiros monitorem as comunicações sem contato entre o dispositivo eletrônico e o terminal de dados.

O dispositivo eletrônico 102 e o terminal de dados 100 podem ter chaves criptográficas adequadas 118, 120 e 146, que são utilizadas na execução de diversos protocolos criptográficos.

10 O terminal de dados 100 pode derivar outra chave específica de dispositivos para o dispositivo eletrônico 102 a partir dos dados impressos de leitura eletrônica 116. Para essa finalidade, o terminal de dados pode possuir um sensor ótico para ler os dados impressos 116 visualmente. Uma chave simétrica para a comunicação com o dispositivo eletrônico 102 pode, dessa
15 forma, ser obtida a partir dos dados assim registrados. Em uma execução, os dados 116 são utilizados como uma chave simétrica. Essa chave simétrica pode ser armazenada de forma protegida ou não protegida no dispositivo eletrônico 102. Alternativamente, o dispositivo eletrônico 102 é desenhado de tal forma que, se necessário, ele possa gerar essa chave simétrica a partir dos dados
20 116, também eletronicamente armazenados no dispositivo eletrônico 102.

Uma chave geral 146 ou 146' também pode ser utilizada, uma vez que é familiar tanto para o dispositivo eletrônico como para o terminal de dados 100. O terminal de dados pode também possuir um par assimétrico de chaves formado pela chave pública 118 e pela chave privada 120, por meio do qual ele
25 transmite sua chave pública para o dispositivo eletrônico como parte de um protocolo criptográfico. A chave pública pode ser fornecida com uma assinatura digital 122, que permite que o dispositivo verifique a autenticidade da chave 118 por meio de uma cadeia certificada.

A chave geral 146' pode ser utilizada a partir do terminal de dados
30 100, por exemplo, para gerar a chave simétrica adicional a partir dos dados registrados de forma ótica 116. Para isso, a chave geral 146' e os dados 116 são ligados entre si.

A Figura 2 é um fluxograma que mostra o método de acordo com a

invenção para que o terminal de dados acesse um dos objetos de dados armazenados no dispositivo eletrônico. Na etapa 216, o terminal de dados transmite uma solicitação ao dispositivo eletrônico para obter um objeto de dado específico. Na etapa 218, o dispositivo eletrônico utiliza sua tabela de alocação para especificar um protocolo criptográfico. Na etapa 222, o dispositivo eletrônico e o terminal de dados executam o protocolo criptográfico. Na etapa 220, o dispositivo eletrônico transmite o objeto de dado para o terminal de dados.

Neste contexto, a informação codificada na tabela de alocação do dispositivo eletrônico, cujo protocolo criptográfico é atribuído a um objeto de dado, pode já ser conhecida pelo terminal de dados mesmo antes da transmissão 216 da solicitação. Por exemplo, a tabela de alocação existente atualmente no dispositivo eletrônico pode conter conteúdos especificados por um padrão, dos quais o terminal de dados também possui uma cópia. Alternativamente, o dispositivo eletrônico pode transmitir uma especificação do protocolo criptográfico para o terminal de dados antes da implementação 222, quando então a especificação deve corresponder a um certo protocolo criptográfico dentre outros vários que o terminal de dados é capaz de implementar. Em outra alternativa, o dispositivo eletrônico pode transmitir a especificação de diversos protocolos criptográficos ao terminal de dados, a partir da qual o terminal de dados pode selecionar qualquer protocolo desejado que possa implementar.

A Figura 3 mostra um fluxograma das etapas do procedimento implementado por uma execução preferível do dispositivo eletrônico de acordo com a invenção. Depois de o dispositivo eletrônico ter recebido do terminal de dados na etapa 216 uma solicitação para obter um objeto de dado, ele especifica, na etapa 218, com o auxílio da tabela de alocação, um protocolo criptográfico (CP), cuja implementação obrigatória deve estar ligada ao acesso de leitura pelo terminal de dados. Três disposições possíveis são apresentadas como exemplos, incluindo a ligação a um protocolo criptográfico com nível elevado de segurança, iniciando na etapa 200, a ligação a um protocolo criptográfico com nível de segurança mais alto, iniciando na etapa 210, e livre acesso, sem ligação a um protocolo criptográfico.

Ao especificar o protocolo criptográfico de nível de segurança elevado para o objeto de dado, o terminal de dados deve autenticar a si mesmo para o dispositivo eletrônico em um procedimento Solicitação-Resposta baseado em um algoritmo criptográfico simétrico, tal como o algoritmo de codificação 3DES ou AES. Para isso, o dispositivo eletrônico envia uma solicitação (o interpelador) ao o terminal de dados na etapa 200, o qual deve responder corretamente à solicitação e devolver uma resposta ao dispositivo eletrônico. Na etapa 204, o dispositivo eletrônico recebe a resposta do terminal de dados e certifica-se de sua precisão. Vice-versa, na etapa 206, o dispositivo eletrônico pode receber uma solicitação do terminal de dados, à qual responde na etapa 208 para autenticar a si mesmo perante o terminal de dados. Esta respectiva autenticação unilateral pode também acontecer em uma etapa na forma de uma autenticação mútua.

Ao especificar o protocolo criptográfico com nível de segurança mais alto para o objeto de dado, o terminal de dados deve autenticar a si mesmo para o dispositivo eletrônico em um procedimento de Solicitação-Resposta baseado em um algoritmo criptográfico assimétrico, tal como o RSA ou um sistema de codificação elíptica. Para isso, o dispositivo eletrônico recebe a chave pública do terminal de dados na etapa 210. Isto pode ser fornecido com uma assinatura digital, verificada pelo dispositivo eletrônico na etapa 300. A verificação pode também ser baseada em uma cadeia certificada, em cujo final deve estar a maior autoridade de certificação, cuja chave pública é disponível no dispositivo eletrônico. Se o dispositivo eletrônico for integrado a um documento de identificação, a maior autoridade de certificação pode ser a autoridade nacional emissora ou uma organização internacional. Na etapa 212, o dispositivo eletrônico envia uma solicitação ao terminal de dados baseada na chave pública recebida e, através da resposta, o terminal de dados deve provar que também possui a chave privada associada. Na etapa 214, o dispositivo eletrônico recebe a resposta do terminal de dados e, portanto, é assegurada sua precisão.

Na etapa 302, com o auxílio da tabela de alocação, o dispositivo eletrônico pode especificar um protocolo de codificação segundo o qual o terminal de dados e o dispositivo eletrônico se comunicam de forma codificada.

Possíveis disposições, apresentadas como exemplos, incluem tanto uma codificação da comunicação com uma chave de sessão, que é intercambiada na etapa 304, como uma comunicação livre e não codificada que contorna a etapa 304. Assim, o intercâmbio de chaves Diffie-Hellman, ou um procedimento semelhante, é utilizado na etapa 304, permitindo que o dispositivo eletrônico e o terminal de dados derivem uma chave de sessão de alta magnitude e de maneira segura.

A Figura 4 mostra um fluxograma das etapas do procedimento implementado por uma execução preferível do terminal de dados de acordo com a invenção. Depois de o terminal de dados ter solicitado ao dispositivo eletrônico um objeto de dado na etapa 216, ele segue o protocolo criptográfico na ramificação 218, a cuja implementação obrigatória o dispositivo eletrônico liga o acesso à leitura do objeto de dado. De forma semelhante à Figura 3, três possíveis disposições mostram exemplos de ligações a um protocolo criptográfico com nível de segurança elevado, com início na etapa 200, ligação a um protocolo criptográfico de nível de segurança mais alto, com início na etapa 210, e com livre acesso, sem ligação a um protocolo criptográfico.

Ao especificar o protocolo criptográfico de nível de segurança elevado para o objeto de dado, o terminal de dados deve autenticar-se perante o dispositivo eletrônico em um procedimento de Solicitação-Resposta baseado em um algoritmo criptográfico simétrico, como o algoritmo de codificação 3DES ou AES. Na etapa 200, o terminal de dados recebe uma solicitação do dispositivo eletrônico. A chave específica do dispositivo, que deve ser derivada pelo terminal de dados a partir dos dados impressos de leitura eletrônica do dispositivo eletrônico para responder à solicitação da etapa 202, pode ser utilizada para o algoritmo criptográfico simétrico. Dessa forma, o terminal de dados comprova que isso foi visivelmente apresentado com um passaporte, por exemplo, ao qual o dispositivo eletrônico está integrado. Uma chave geral pode também ser necessária para se derivar a chave específica do dispositivo a partir dos dados impressos de leitura eletrônica. Na etapa 204, o terminal de dados envia a resposta ao dispositivo eletrônico. De forma inversa, na etapa 206, um terminal de dados pode enviar uma solicitação ao dispositivo eletrônico e receber a resposta na etapa 208.

Ao especificar o protocolo criptográfico de nível de segurança mais alto para o objeto de dado, o terminal de dados deve autenticar-se perante o dispositivo eletrônico em um procedimento de Solicitação-Resposta baseado em um algoritmo criptográfico assimétrico, tal como o RSA ou um criptosistema de curva elíptica. Para isso, o terminal de dados envia sua chave pública ao dispositivo eletrônico na etapa 210. Na etapa 212, o terminal de dados recebe uma solicitação do dispositivo eletrônico baseada na chave pública transmitida e, através da resposta a tal solicitação, o terminal de dados comprova, na etapa 214, possuir também a chave privada associada.

Por exemplo, suponhamos que o dispositivo eletrônico gere um número aleatório. Isto é codificado com a chave pública do terminal de dados e a cifra resultante é transmitida ao terminal de dados pelo dispositivo eletrônico. O terminal de dados decodifica a cifra com sua chave secreta e envia o resultado da decodificação de volta para o dispositivo eletrônico. O dispositivo eletrônico então compara o número aleatório gerado originalmente com o resultado da decodificação recebido do terminal de dados. Se ambos concordarem, o terminal de dados é classificado como autêntico e autorizado.

O dispositivo eletrônico pode, ainda, ligar a transmissão do objeto de dado à execução obrigatória das etapas do protocolo criptográfico de nível de segurança mais alto, com as etapas do protocolo de nível de segurança elevado.

Na etapa 302 o dispositivo eletrônico pode especificar, com o auxílio da tabela de alocação, um protocolo de codificação segundo o qual o terminal de dados e o dispositivo eletrônico possam se comunicar de forma codificada. Os exemplos de execuções possíveis apresentados abaixo mostram a codificação da comunicação com uma chave de sessão, a qual é intercambiada na etapa 304, e uma comunicação livre e não codificada, pela qual a etapa 304 é contornada.

Lista de Números de Referência

- 100 Terminal de dados
- 102 Dispositivo eletrônico
- 104 Objetos de dados
- 106 Tabela de alocação

- 108 Protocolo criptográfico
- 109 Protocolo de codificação
- 110 Aplicativo de software
- 112 Sistema operacional
- 5 114 Documento de identificação
- 116 Dados impressos de leitura eletrônica
- 118 Chave pública
- 120 Chave privada
- 122 Assinatura digital
- 10 124, 124' Instruções executáveis por computador
- 126 Memória [armazenagem]
- 128, 128' Receptor
- 130, 130' Transmissor
- 140 Função de administrador
- 15 142, 142' Interface sem contato
- 146, 146' Chave geral

REIVINDICAÇÕES

1. PROCEDIMENTO DE ACESSO POR UM TERMINAL DE DADOS A UM DENTRE VÁRIOS OBJETOS DE DADOS ARMAZENADOS EM UM DISPOSITIVO ELETRÔNICO, caracterizado pelo fato de que o dispositivo
- 5 eletrônico (102) é integrado a um documento de identificação (114) e que o dispositivo eletrônico possui uma tabela de alocação (106) na qual um protocolo criptográfico (108) com um nível de segurança diferente é atribuído a cada um dos diferentes objetos de dados, e que o documento de identificação possui
- 10 dados impressos de leitura eletrônica (116), onde na tabela de alocação (106), um protocolo criptográfico (108) com um nível de segurança elevado é atribuído, pelo menos, ao primeiro de vários objetos de dados (104) e um protocolo criptográfico com nível de segurança elevado compreendendo as seguintes etapas:
- Colocação (200) de uma solicitação ao terminal de dados (100) com base em
 - 15 um algoritmo criptográfico simétrico que utiliza uma chave específica do dispositivo (144), a qual pode ser derivada a partir dos dados impressos de leitura eletrônica, pelo dispositivo eletrônico;
 - Derivação (202) da chave específica do dispositivo a partir dos dados impressos de leitura eletrônica pelo terminal de dados;
 - 20 - Resposta (204) do terminal de dados à solicitação para autenticar-se perante o dispositivo eletrônico;
- e em que o terminal de dados (100) possui uma chave pública (118) e uma chave privada (120), em que, na tabela de alocação (106), um protocolo criptográfico (108) com um nível de segurança mais alto é atribuído, pelo menos,
- 25 ao segundo de vários objetos de dados, em que o protocolo criptográfico com nível de segurança mais alto compreende as seguintes etapas:
- Transmissão (210) da chave pública para o dispositivo eletrônico pelo terminal de dados;
 - Colocação (212) de uma solicitação ao terminal de dados pelo dispositivo
 - 30 eletrônico utilizando a chave pública, cuja resposta do dispositivo eletrônico requer o uso da chave privada;
 - Resposta (214) do terminal de dados à solicitação para autenticar-se ao dispositivo eletrônico,

sendo que, pelo menos, o primeiro e o segundo objeto de dados contêm dados biométricos pessoais, e que, na tabela de alocação, pelo menos um dos vários objetos de dados (104) é atribuído com livre acesso sem um protocolo criptográfico (108),

5 sendo que o procedimento compreende as seguintes etapas:

- Transmissão (216) pelo terminal de dados (100) de uma solicitação ao dispositivo eletrônico (102) para um objeto de dado específico;

- Especificação (218) de um protocolo criptográfico pelo dispositivo eletrônico para o objeto de dado com o auxílio da tabela de alocação;

10 - Implementação (222) do protocolo criptográfico com nível de segurança elevado pelo dispositivo eletrônico (102) e pelo terminal de dados (100) quando o objeto de dado pertence ao objeto de dado, e implementação (222) do protocolo criptográfico de nível de segurança mais alto pelo dispositivo eletrônico e pelo terminal de dados quando o objeto de dado pertence ao

15 segundo objeto de dado;

- Transmissão (220) de um objeto de dado pelo dispositivo eletrônico.

2. PROCEDIMENTO de acordo com a reivindicação 1, caracterizado pelo fato de que o dispositivo eletrônico (102) possui um aplicativo de software (110), sendo que o aplicativo de software contém uma tabela de
20 alocação (106) em que um protocolo criptográfico (108) é especificado pelo aplicativo de software, e que o protocolo criptográfico é implementado pelo terminal de dados e pelo aplicativo de software, e que o objeto de dado é transmitido pelo aplicativo de software.

3. PROCEDIMENTO de acordo com a reivindicação 2,
25 caracterizado pelo fato de que o dispositivo eletrônico (102) possui um sistema operacional (112) que previne qualquer alteração ou remoção não autorizada do aplicativo de software (110), permitindo apenas o acesso aos objetos de dados (104) por meio do aplicativo de software.

4. PROCEDIMENTO de acordo com a reivindicação 3,
30 caracterizado pelo fato de que o sistema operacional (112), após a autenticação como administrador do dispositivo eletrônico (102), permite a alteração ou remoção do aplicativo de software.

5. PROCEDIMENTO de acordo com uma qualquer das

reivindicações de 1 a 4, caracterizado pelo fato de que o terminal de dados (100) e o dispositivo eletrônico (102) comunicam-se sem contato.

5 6. PROCEDIMENTO de acordo com a reivindicação 5, caracterizado pelo fato de que na tabela de alocação (106), um protocolo de codificação (109) com um nível de segurança diferente é, ainda, atribuído a diferentes objetos de dados (104), de acordo com o qual o terminal de dados e o dispositivo eletrônico comunicam-se de forma codificada.

10 7. PROCEDIMENTO de acordo com uma qualquer das reivindicações de 1 a 6, caracterizado pelo fato de que uma chave geral (146), conhecida pelo dispositivo eletrônico (102) e pelo terminal de dados (100), é necessária para se derivar a chave específica do dispositivo (144) a partir dos dados impressos de leitura eletrônica (116).

15 8. PROCEDIMENTO de acordo com uma qualquer das reivindicações de 1 a 7, caracterizado pelo fato de que o protocolo criptográfico com nível de segurança elevado (108) compreende, ainda, as seguintes etapas:
- Colocação (206) de uma solicitação pelo terminal de dados (100) para o dispositivo eletrônico (102) com base em um algoritmo criptográfico simétrico, utilizando a chave específica do dispositivo;
- Resposta (208) à solicitação pelo dispositivo eletrônico, para autenticar-se
20 perante o terminal de dados.

9. PROCEDIMENTO de acordo com uma qualquer das reivindicações de 1 a 8, caracterizado pelo fato de que a chave pública (118) é caracterizada por uma assinatura eletrônica (122), e em que o dispositivo eletrônico verifica (300) a assinatura eletrônica.

25 10. PRODUTO DE PROGRAMA DE COMPUTADOR com uma tabela de alocação (106) caracterizado pelo fato de que diferentes objetos de dados (104) são atribuídos com um protocolo criptográfico (108) com um nível de segurança diferente, sendo que cada um dos protocolos criptográficos é utilizado para autenticar um terminal de dados, e sendo que a implementação do
30 protocolo criptográfico atribuído a cada um dos objetos de dado na tabela de alocação é uma condição para o acesso do terminal de dados a tal objeto de dado, além de instruções executáveis por computador para:
- Receber uma solicitação de um terminal de dados (100) por um dentre vários

objetos de dados (104);

- Especificar um protocolo criptográfico para um objeto de dado específico com o auxílio da tabela de alocação;

- Implementar o protocolo criptográfico com o terminal de dados,

5 - Enviar o objeto de dado específico para o terminal de dados.

11. PRODUTO DE PROGRAMA DE COMPUTADOR de acordo com a reivindicação 10, caracterizado pelo fato de que a tabela de alocação (106) e as instruções executáveis por computador (124) podem ser instaladas em um dispositivo eletrônico com um sistema operacional, de tal forma que o
10 sistema operacional evite qualquer alteração ou remoção não autorizada da tabela de alocação ou das instruções executáveis por computador .

12. PRODUTO DE PROGRAMA DE COMPUTADOR de acordo com a reivindicação 11, caracterizado pelo fato de que inclui também instruções executáveis por computador (124) e em que o acesso a objetos de dados (104)
15 só é possível por meio do instruções executáveis por computador.

13. MÍDIA DE ARMAZENAGEM DIGITAL, caracterizada pelo fato de que inclui um produto de programa de computador, de acordo com uma qualquer das reivindicações 10, 11 ou 12.

14. DISPOSITIVO ELETRÔNICO (102) caracterizado pelo fato
20 de compreender:

- Uma memória (126) para vários objetos de dados (104);

- Um receptor (128) para receber uma solicitação de um terminal de dados (100) para um dos objetos de dados;

- Uma tabela de alocação (106), na qual um protocolo criptográfico (108) com
25 um nível de segurança diferente é atribuído a diferentes objetos de dados, sendo que cada um dos protocolos criptográficos é utilizado para autenticar o terminal de dados, e em que a implementação do protocolo criptográfico atribuído a um objeto de dado na tabela de alocação é uma condição para o acesso do terminal de dados a tal objeto de dado.

30 - Instruções de programa (124) para especificar um protocolo criptográfico para um objeto de dado com o auxílio da tabela de alocação;

- Instruções de programa (124) para implementar o protocolo criptográfico com o terminal de dados;

- Um transmissor (130) para enviar o objeto de dado para o terminal de dados.

15. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 14, caracterizado pelo fato de que possui um aplicativo de software (110) que inclui instruções de programa (124), caracterizado pelo fato de que o aplicativo de software inclui uma tabela de alocação (106) e que um protocolo criptográfico (108) pode ser selecionado pelo aplicativo de software, sendo que o protocolo criptográfico pode ser implementado pelo terminal de dados (100) e pelo aplicativo de software, e que o objeto de dado específico (104) pode ser transmitido por meio do aplicativo de software.

16. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 15, caracterizado pelo fato de que possui um sistema operacional (112) desenvolvido para evitar qualquer alteração ou remoção não autorizada do aplicativo de software (110) e para evitar o acesso aos objetos de dados (104) sem o uso do aplicativo de software.

17. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 16, caracterizado pelo fato de que o sistema operacional (112) possui uma função de administrador (140) para autenticar-se como administrador, em que, após a autenticação como administrador do dispositivo eletrônico, é possível alterar ou remover o aplicativo de software (110).

18. DISPOSITIVO ELETRÔNICO (102), de acordo com uma qualquer das reivindicações 14 a 17, caracterizado pelo fato de que o dispositivo eletrônico é integrado a um documento de identificação (114).

19. DISPOSITIVO ELETRÔNICO (102), de acordo com uma qualquer das reivindicações 14 a 18, caracterizado pelo fato de que pelo menos um dos objetos de dados (104) inclui dados biométricos pessoais.

20. DISPOSITIVO ELETRÔNICO (102), de acordo com uma qualquer das reivindicações 14 a 19, caracterizado pelo fato de que possui uma interface (142) para comunicação sem contato com o terminal de dados (100).

21. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 20, caracterizado pelo fato de que, na tabela de alocação (106), um protocolo de codificação (109) com um nível de segurança diferente é também atribuído a diferentes objetos de dados, segundo o qual o terminal de dados (100) e o dispositivo eletrônico podem comunicar-se de forma codificada.

22. DISPOSITIVO ELETRÔNICO (102), de acordo com uma qualquer das reivindicações 14 a 21, caracterizado pelo fato de que, na tabela de alocação (106), pelo menos um dos vários objetos de dados (104) é atribuído com livre acesso sem protocolo criptográfico (108).

5 23. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 22, caracterizado pelo fato de que o dispositivo eletrônico possui dados impressos de leitura eletrônica (116), e em que, na tabela de alocação (106), um protocolo criptográfico (108) com nível de segurança elevado é atribuído a pelo menos um dos vários objetos de dados, incluindo as seguintes etapas:

- Colocação (200) de uma solicitação ao terminal de dados (100) com base em um algoritmo criptográfico simétrico, utilizando uma chave específica do dispositivo (144) que pode ser derivada pelo dispositivo eletrônico a partir dos dados impressos de leitura eletrônica;
- 15 - Derivação (202) da chave específica do dispositivo a partir dos dados impressos de leitura eletrônica pelo terminal de dados;
- Resposta (204) do terminal de dados à solicitação para autenticar-se perante o dispositivo eletrônico.

24. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 23, caracterizado pelo fato de que uma chave geral (146), conhecida pelo dispositivo eletrônico e pelo terminal de dados (100), é necessária para se derivar a chave específica do dispositivo a partir dos dados impressos de leitura eletrônica (116).

25. DISPOSITIVO ELETRÔNICO (102) de acordo com uma qualquer das reivindicações 23 ou 24, caracterizado pelo fato de que o protocolo criptográfico (108) com nível de segurança elevado compreende também as seguintes etapas:

- Colocação (206) de uma solicitação pelo terminal de dados (100) para o dispositivo eletrônico com base em um algoritmo criptográfico simétrico, em que se utiliza a chave específica do dispositivo (144);
- 30 - Resposta (208) do dispositivo eletrônico à solicitação para autenticar-se ao terminal de dados (100).

26. DISPOSITIVO ELETRÔNICO (102), de acordo com uma

qualquer das reivindicações 22 a 25, caracterizado pelo fato de que o terminal de dados (100) possui uma chave pública (118) e uma chave privada (118), sendo que, na tabela de alocação (106), pelo menos um dos vários objetos de dados (104) é atribuído com um protocolo criptográfico (108) de nível de

5 segurança mais alto que compreende as seguintes etapas:

- Transmissão (210) da chave pública para o dispositivo eletrônico pelo terminal de dados;

- Colocação (212) de uma solicitação ao terminal de dados pelo dispositivo eletrônico utilizando a chave pública, cuja resposta do dispositivo eletrônico

10 requer o uso da chave privada,

- Resposta (214) à solicitação de autenticação para o dispositivo eletrônico pelo terminal de dados.

27. DISPOSITIVO ELETRÔNICO (102) de acordo com a reivindicação 26, caracterizado pelo fato de que a chave pública (118) é

15 caracterizada por uma assinatura eletrônica (122), e em que o dispositivo eletrônico (102) verifica a assinatura eletrônica.

28. TERMINAL DE DADOS (100) para leitura de um objeto de dado (104) a partir de uma memória (126) de um dispositivo eletrônico (102) integrado a um documento de identificação (114) caracterizado pelo fato de que

20 compreende:

- Um transmissor (130') para transmitir uma solicitação por um objeto de dado (104) a um dispositivo eletrônico em que vários objetos de dados (104) estão armazenados;

- Um receptor (128') para receber do dispositivo eletrônico a especificação de

25 um protocolo criptográfico para o objeto de dado solicitado, sendo que o protocolo criptográfico é utilizado para autenticar o terminal de dados, e sendo que a implementação do protocolo criptográfico é uma condição para que o terminal de dados acesse o objeto de dado;

- Instruções de programa (124) para implementar o protocolo criptográfico; e

30 considerando-se que o receptor (128') é utilizado para receber objeto de dado.

29. TERMINAL DE DADOS (100) de acordo com a reivindicação 28, caracterizado pelo fato de que possui uma interface (142') para comunicação sem contato com dispositivo eletrônico (102).

30. TERMINAL DE DADOS (100) de acordo com a reivindicação 29, caracterizado pelo fato de que o receptor (128) é também desenvolvido para receber a especificação de um protocolo de codificação (109), e em que o terminal de dados possui um meio de comunicação com o dispositivo eletrônico (102), codificada de acordo com o protocolo de codificação.

31. TERMINAL DE DADOS (100), de acordo com uma qualquer das reivindicações 28 a 30, caracterizado pelo fato de que o dispositivo eletrônico (102) possui dados impressos de leitura eletrônica (116), sendo que o receptor (128) recebe a especificação de um protocolo criptográfico (108) com nível de segurança elevado que compreende as seguintes etapas:

- Colocação (200) de uma solicitação ao terminal de dados (100) com base em um algoritmo criptográfico simétrico, em que é utilizada uma chave específica do dispositivo (144) que pode ser derivada pelo dispositivo eletrônico a partir dos dados impressos de leitura eletrônica;
- Derivação (202) da primeira chave criptográfica a partir dos dados impressos de leitura eletrônica pelo terminal de dados;
- Resposta (204) do terminal de dados à solicitação para autenticar-se perante o dispositivo eletrônico.

32. TERMINAL DE DADOS (100) de acordo com a reivindicação 31, caracterizado pelo fato de que uma segunda chave criptográfica, conhecida pelo dispositivo eletrônico (102) e pelo terminal de dados, é necessária para se derivar a chave específica do dispositivo (144) a partir dos dados impressos de leitura eletrônica (116).

33. TERMINAL DE DADOS (100) de acordo com uma qualquer das reivindicações 31 ou 32, caracterizado pelo fato de que o protocolo criptográfico (108) com nível de segurança elevado compreende também as seguintes etapas:

- Colocação (206) de uma solicitação ao dispositivo eletrônico (102) pelo terminal de dados com base em um algoritmo criptográfico simétrico, em que se utiliza a chave específica do dispositivo pelo terminal de dados;
- Resposta (208) do dispositivo eletrônico à solicitação para autenticar-se ao terminal de dados.

34. TERMINAL DE DADOS (100), de acordo com uma qualquer

das reivindicações 28 a 33, caracterizado pelo fato de que o terminal de dados possui uma chave pública (118) e uma chave privada (120), e em que o receptor (128) pode receber a especificação de um protocolo criptográfico (108) de nível de segurança mais alto, compreendendo as seguintes etapas:

- 5 - Transmissão da chave pública ao dispositivo eletrônico (102) pelo terminal de dados;
- Colocação de uma solicitação ao terminal de dados pelo dispositivo eletrônico utilizando a chave pública, cuja resposta pelo dispositivo eletrônico requer o uso da chave privada;
- 10 - Resposta à solicitação para autenticação do dispositivo eletrônico pelo terminal de dados.

35. TERMINAL DE DADOS (100) de acordo com a reivindicação 34, caracterizado pelo fato de que a chave pública (118) é caracterizada por uma assinatura eletrônica (122), e em que o dispositivo eletrônico (102) verifica a assinatura eletrônica.

36. DOCUMENTO DE IDENTIFICAÇÃO caracterizado pelo fato de que compreende um dispositivo eletrônico integrado, de acordo com uma das Reivindicações 14 a 27.

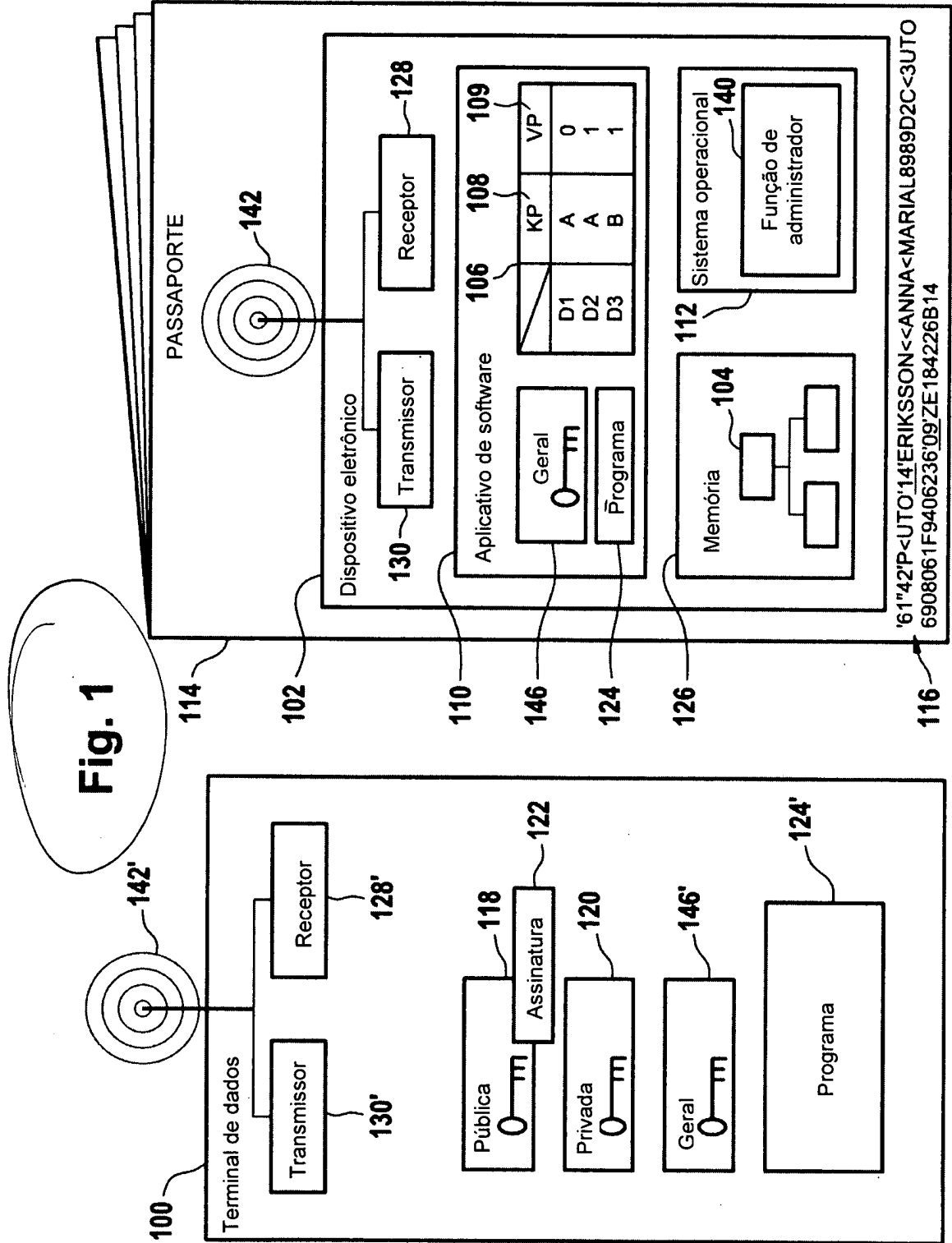
37. PROCEDIMENTO DE ACESSO POR UM TERMINAL DE DADOS A UM DENTRE VÁRIOS OBJETOS DE DADOS ARMAZENADOS EM UM DISPOSITIVO ELETRÔNICO, caracterizado pelo fato de que o dispositivo eletrônico possui uma tabela de alocação (106) na qual protocolos criptográficos (108) com níveis de segurança diferentes são atribuídos aos diferentes objetos de dados, sendo que cada um dos protocolos criptográficos é utilizado para autenticar o terminal de dados (100), e sendo que a implementação do protocolo criptográfico atribuído a um dos objetos de dados na tabela de alocação é uma condição para o acesso do terminal de dados a tal objeto de dado, com as seguintes etapas:

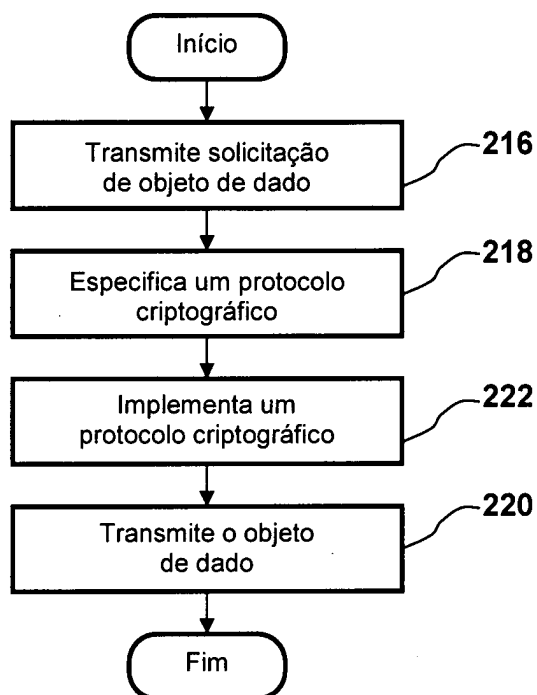
- Transmissão (216) de uma solicitação pelo terminal de dados (100) para o dispositivo eletrônico para um objeto de dado específico;
- Especificação (218) de um protocolo criptográfico para um objeto de dado específico com o auxílio da tabela de alocação, pelo dispositivo eletrônico;
- Implementação (222) do protocolo criptográfico pelo dispositivo eletrônico e

pelo terminal de dados (100); e

- Transmissão (220) do objeto de dado pelo dispositivo eletrônico.

sendo que o dispositivo eletrônico (102) é integrado a um documento de identificação (114).





3/4

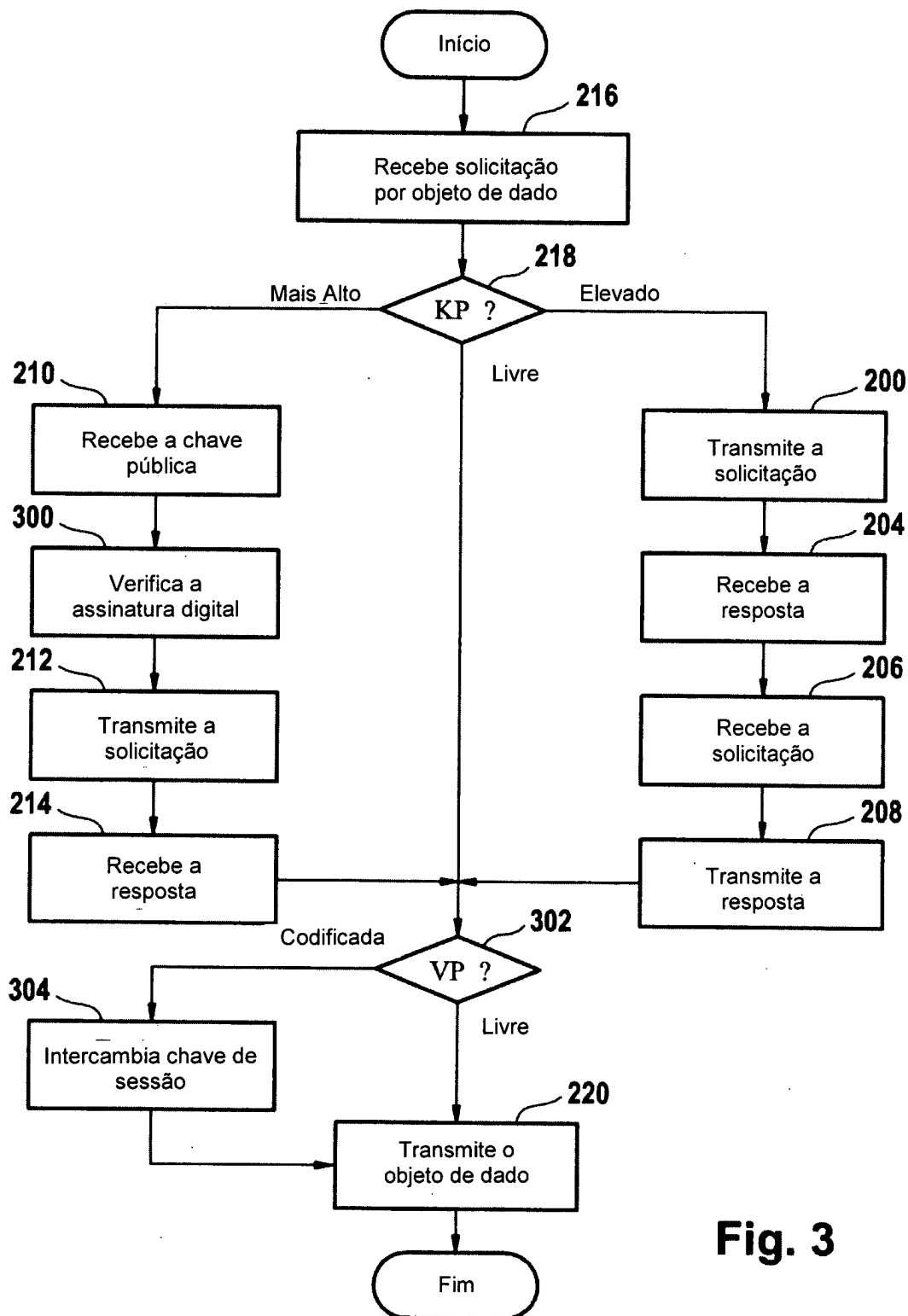


Fig. 3

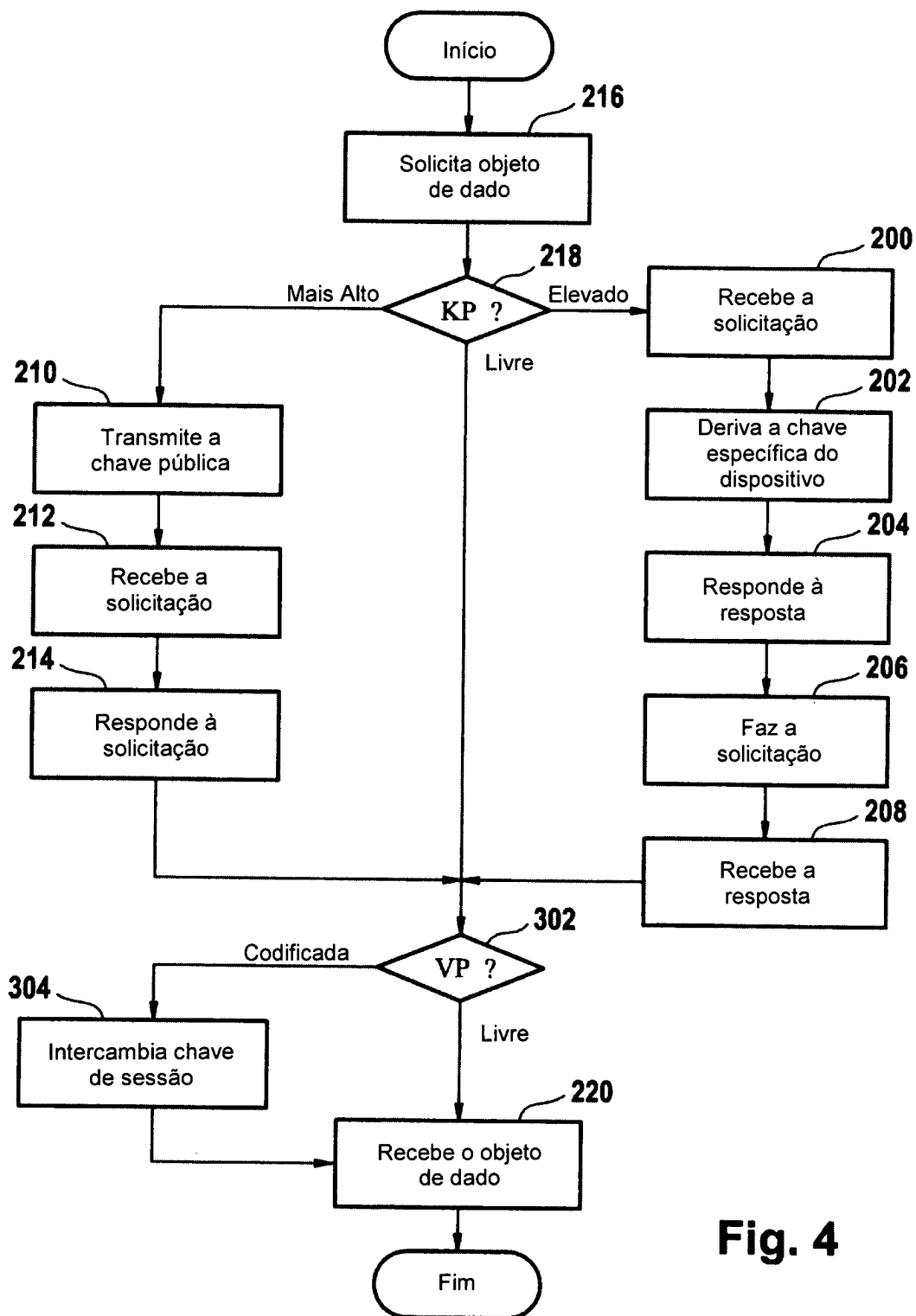


Fig. 4

RESUMO

PROCEDIMENTO DE ACESSO POR UM TERMINAL DE DADOS
A UM DENTRE VÁRIOS OBJETOS DE DADOS ARMAZENADOS EM UM
DISPOSITIVO ELETRÔNICO, PRODUTO DE PROGRAMA DE
5 COMPUTADOR, MÍDIA DE ARMAZENAGEM DIGITAL, DISPOSITIVO
ELETRÔNICO, TERMINAL DE DADOS E DOCUMENTO DE IDENTIFICAÇÃO

A presente invenção refere-se a um procedimento de acesso a um
objeto de dado por meio de um terminal de dados, de uma pluralidade de
objetos de dados armazenados em um dispositivo eletrônico, em que o dito
10 dispositivo eletrônico compreende uma tabela de alocação em que diferentes
níveis de segurança de protocolos criptográficos são designados a diferentes
objetos de dados. O método da invenção consiste primeiro em transmitir um
pedido para um objeto de dado escolhido por um terminal de dados a um
dispositivo eletrônico, determinando o protocolo criptográfico para o objeto de
15 dado escolhido, pelo dispositivo eletrônico com o auxílio da tabela de alocação,
executando o protocolo criptográfico pelo dispositivo eletrônico e pelo terminal
de dados, e transmitindo o objeto de dado escolhido ao terminal de dados, pelo
dispositivo eletrônico na condição que o protocolo criptográfico é implementado
com sucesso.