

(11) Número de Publicação: **PT 1616291 E**

(51) Classificação Internacional:

G06K 19/77 (2007.10) **G06K 19/14** (2007.10)
G06K 7/00 (2007.10) **G06K 7/10** (2007.10)

(12) FASCÍCULO DE PATENTE DE INVENÇÃO

(22) Data de pedido: 2004.04.13	(73) Titular(es): GIESECKE & DEVRIENT GMBH PRINZREGENTENSTRASSE 159 81677 MUNCHEN DE
(30) Prioridade(s): 2003.04.14 DE 10317257	
(43) Data de publicação do pedido: 2006.01.18	
(45) Data e BPI da concessão: 2009.04.08 134/2009	(72) Inventor(es): HANS GRAF DE KLAUS FINKENZELLER DE ALFRED ROSSMADL DE
	(74) Mandatário: LUÍS MANUEL DE ALMADA DA SILVA CARVALHO RUA VÍCTOR CORDON, 14 1249-103 LISBOA PT

(54) Epígrafe: **SUPORTE DE DADOS SEM CONTACTO**

(57) Resumo:

RESUMO**"SUPORTE DE DADOS SEM CONTACTO"**

O invento diz respeito a um dispositivo bem como a um método para a determinação fiável de instâncias de utilização deliberada de um suporte de dados utilizável na ausência de contacto físico com o mesmo. Consoante os dados que se pretende transmitir, pode ser utilizado entre o dispositivo de leitura e o suporte de dados, além de um canal de transmissão de dados com recurso a uma antena, um canal de transmissão de dados por via óptica.

DESCRIÇÃO

"SUPORTE DE DADOS SEM CONTACTO"

O presente invento diz respeito a um dispositivo bem como a um método para a determinação fiável de instâncias de utilização deliberada de um suporte de dados utilizável na ausência de contacto físico com o mesmo.

As expressões "suporte de dados sem contacto" ou "cartão sem contacto" empregadas no presente texto devem ser entendidas como designando todos os dispositivos providos de um "microchip" (circuito integrado miniatural) e de uma antena ligada ao mesmo e passíveis de envolvimento numa partilha de dados com um dispositivo de leitura adequado. Exemplos destes dispositivos são, além dos cartões providos de um "chip" destinados a efectuar pagamentos, os documentos de identificação passíveis de leitura na ausência de contacto físico com os mesmos, tais como passaportes e cartões de identidade electrónicos nos quais se encontra embutido um "microchip", bem como as etiquetas RFID (acrónimo da expressão inglesa "Radio Frequency IDentification", ou seja, em que a identificação é feita através das respectivas frequências rádio).

Actualmente, os suportes de dados sem contacto são exclusivamente utilizados em transacções de pagamento

electrónico no contexto de aplicações fechadas tais como no pagamento em cantinas ou transportes públicos. Na Alemanha, a razão para tal restrição é a presente inadmissibilidade, por questões de segurança, da utilização de cartões sem contacto em aplicações de pagamento electrónico em geral, por exemplo enquanto versões sem contacto de porta-moedas electrónicos. Determinante neste contexto é o perigo de que terceiros possam proceder a débitos por intermédio do cartão sem contacto sem conhecimento do seu detentor. É imaginável uma situação em que, por exemplo com recurso a um terminal móvel para cartões sem contacto utilizado por múltiplas pessoas (por exemplo em messes, concertos, metropolitano, comboios, etc.), seja debitado dinheiro “electrónico” de carteiras localizadas na vizinhança do referido terminal sem que os proprietários das mesmas tenham conhecimento de tal. Com os cartões cuja utilização requer um contacto físico não se levanta um tal problema, uma vez que uma operação de pagamento é realizada pelo detentor do cartão mediante a introdução deliberada do referido cartão num dispositivo de leitura de cartões.

Além de poderem ser utilizados como meio de pagamento electrónico, os cartões sem contacto também podem funcionar como suportes de dados em documentos de valor tais como, por exemplo, passaportes. Em particular, é possível utilizar os cartões sem contacto como vistos que podem ser apostos ao documento de viagem, nomeadamente colados sobre o mesmo. Para este efeito é adequada a tecnologia designada em inglês por “coil on chip” (CoC,

bobina sobre "chip") em que a antena se encontra integrada no "chip". Contudo, também podem ser usados sistemas sem contacto convencionais, tais como películas nas quais foi disposto um "chip" além de impressa uma bobina.

Também nas aplicações de cartões sem contacto no âmbito dos documentos de valor surge o problema que consiste em assegurar a impossibilidade de uma leitura dos mesmos por parte de terceiros que não seja pretendida pelo detentor do cartão. O mesmo é válido no que respeita à leitura indevida e despercebida de transpositores ("transponders" em inglês) sem contacto utilizados na identificação de produtos.

No documento de patente FR 2 770 316 A foi proposto impedir a leitura indesejada de um cartão sem contacto por via do provimento quer do cartão, quer do dispositivo de leitura, com sensores ópticos. Numa primeira etapa é dirigido sobre o cartão um feixe luminoso com origem no dispositivo de leitura, o qual é reflectido de volta para este último por parte de um elemento especial reflector da luz de que o cartão é provido. Quando o dispositivo de leitura capta a radiação devolvida começa a inicialização do cartão. Antes de ter início a leitura do cartão, este detecta por seu lado se recebe ou não radiação proveniente do dispositivo de leitura, sendo a transferência de dados entre este último e o cartão autorizada apenas no caso afirmativo.

No documento de patente US 2003/0057276 A1 foi proposta a realização de uma comprovação da identidade de um objecto mediante a leitura de um primeiro elemento de identificação opticamente legível e de um segundo elemento de identificação legível na ausência de contacto, sendo as respectivas informações identificativas examinadas no que respeita a uma possível coincidência. Na medida em que exista uma coincidência, o objecto individualizado pelos elementos de identificação é correctamente identificado e classificado como autêntico. Neste caso, o segundo elemento de identificação foi configurado como elemento de identificação electronicamente legível e inserido num local não visível do objecto.

Ao presente invento subjazia a disponibilização de um outro dispositivo, bem como de um outro processo, para a determinação fiável da utilização deliberada de um suporte de dados sem contacto por parte do detentor desse cartão.

Este objectivo foi alcançado por via das características constantes das reivindicações independentes. Nas reivindicações subsidiárias são indicadas formas vantajosas de execução do invento e aperfeiçoamentos do mesmo.

Com recurso ao canal de transmissão de dados adicional ocorre uma partilha de dados por via óptica entre o dispositivo de leitura e o suporte de dados, dados esses que são adequados à realização de um procedimento de auten-

ticação entre o dispositivo de leitura e o cartão sem contacto. A autenticação por intermédio do canal de transmissão de dados suplementar impede um accionamento involuntário do cartão sem contacto, na medida em que a informação opticamente legível deixa de estar disponível quando o suporte de dados deixa de estar visível no que respeita ao dispositivo de leitura, ou seja, quando é transportado num bolso ou numa carteira.

De acordo com uma primeira forma de execução do invento, o suporte de dados contém informação opticamente legível, tal como, por exemplo, um código de barras ou um código matricial. Caso o cartão seja apresentado ao dispositivo de leitura, a informação nele contida é lida por um sistema de leitura óptica, por exemplo um digitalizador ("scanner" em inglês) de códigos de barras. A informação lida opticamente pode ser posteriormente utilizada pelo suporte de dados sem contacto para efeito da autenticação a realizar em conjugação com o dispositivo de leitura sem contacto, a fim de por esta via comprovar a legitimidade de uma transacção subsequente.

Um desenvolvimento desta primeira forma de execução do invento consiste na transmissão, por parte do "chip", da informação reproduzida opticamente para um dispositivo de visualização, por exemplo um visor de cristais líquidos (LCD de acordo com o acrónimo inglês para "liquid crystal display"). Deste modo deixa de ser possível a simples cópia de informações, uma vez que elas também podem

conter estruturas de dados geradas de forma aleatória.

De acordo com uma outra forma de execução do invento, o suporte de dados sem contacto foi dotado de um meio luminoso óptico, por exemplo um díodo emissor de radiação infravermelha ou uma película luminosa. Este meio luminoso pode dispor de uma ligação eléctrica ao "chip" ou ser parte integrante deste último. Quando se pretende que seja realizada uma transacção entre um dispositivo de leitura e o suporte de dados, o meio luminoso é utilizado para, por via óptica, enviar dados adicionais do "chip" para o dispositivo de leitura. Estes dados podem fazer parte de um processo de autenticação mútua, sendo utilizados, de acordo com o invento, para autorizar uma transacção subsequente. Sem que o dispositivo de leitura tome conhecimento dos dados transmitidos por via óptica não pode ser efectuada uma transacção entre ele e o suporte de dados.

De preferência, as alterações nas condições ambientais a que se encontra sujeito um suporte de dados resultantes da sua retirada de dentro de uma carteira para efeito da realização de um pagamento deixam-se detectar sobre o mesmo. Por exemplo por intermédio de um componente óptico sensível à luz torna-se neste caso possível determinar se o cartão se encontra dentro ou fora de uma carteira. Este componente sensível à luz pode dispor de uma ligação eléctrica ao "chip" ou ser parte integrante deste. De acordo com o invento, assim que o componente sensível à luz fica exposto a uma claridade mínima é gerado um sinal

de autorização que torna possível a realização de uma transacção entre o "chip" e o dispositivo de leitura sem contacto.

A vantagem desta variante de execução do invento reside na dispensa do recurso a terminais sem contacto especiais, permitindo que continue a ser utilizada a infra-estrutura que já se encontra disponível (por exemplo terminais sem contacto análogos aos correntemente utilizados em sistemas fechados tais como, por exemplo, cantinas).

Um aperfeiçoamento desta ideia consiste em ser o próprio dispositivo de leitura a gerar um sinal luminoso óptico. É concebível que, para efeito da autorização de uma transacção, seja conferida ao sinal luminoso óptico uma modulação marcante, por exemplo um sinal de 1 kHz, ou que por intermédio do sinal luminoso óptico sejam transferidos para o "chip" dados que serão utilizados no processo de autenticação entre o suporte de dados e o dispositivo de leitura.

Uma combinação das formas de execução precedentemente descritas consiste na disponibilização, sobre o cartão, tanto de um meio de iluminação óptico como de um meio receptor óptico e na ligação dos mesmos ao "chip", ou na disponibilização destes meios enquanto partes integrantes do "chip". Neste caso poderia ser realizada, além de uma transmissão bidireccional de dados entre o cartão e o dispositivo de leitura realizada na ausência de contacto

físico, uma segunda transmissão bidireccional de dados entre os mesmos, mas esta realizada por via óptica.

Uma outra vantagem desta forma de execução do invento consiste em extrair a energia necessária ao funcionamento dos meios ópticos de comunicação do canal de transmissão sem contacto (por exemplo um acoplamento magnético ou capacitivo). Adicionalmente, fica obviamente subentendido que na comunicação por via óptica pode ser utilizada, além de luz visível, radiação infravermelha ou ultravioleta ou uma mistura de radiações incluídas nestes domínios de frequências ("uplink" vs. "downlink" em inglês).

De um modo análogo àquele em que são utilizadas as informações ópticas, também podem ser usadas informações acústicas, por exemplo sob a forma da transmissão de um sinal acústico codificado, o qual pode ser gerado por exemplo por intermédio de um altifalante (nomeadamente um altifalante piezoeléctrico) integrado no cartão.

Além disso, um altifalante localizado no cartão também é adequado para assinalar a ocorrência de cada uma das transacções por via da emissão de um sinal que indica ao detentor do cartão estar, nesse preciso momento, a ser efectuado um pagamento. Caso seja utilizada uma tal forma de execução do invento, e embora continue a ser possível a retirada indevida de dinheiro do cartão com recurso a um terminal móvel sem contacto, esta transacção deixa de passar despercebida.

Pode ainda ter sido prevista a presença alternativa ou adicional no suporte de dados de um alarme vibratório.

Seguidamente o invento será descrito em mais pormenor com recurso aos exemplos de execução representados nos desenhos anexos. Nestes são mostrados:

Figura 1 uma forma de execução do presente invento em que um suporte de dados contém informação óptica;

Figura 2 uma outra forma de execução do invento em que o suporte de dados foi provido de um meio luminoso;

Figura 3 uma outra forma de execução do invento em que o suporte de dados foi provido de um meio receptor óptico;

Figura 4 uma outra forma de execução do invento em que o suporte de dados foi provido de um componente estrutural óptico;

Figura 5 um exemplo de realização de um processo para a derivação de uma chave criptográfica; e

Figura 6 um exemplo de realização de um processo de autenticação.

Na Figura 1 encontra-se representado um suporte

de dados 1a no qual se encontram dispostos uma antena 2 e um "chip" 3 electricamente ligado à mesma. Uma zona do suporte de dados contém informações opticamente legíveis 4, por exemplo um código de barras ou um código matricial, as quais são passíveis de ser transmitidas por via de um canal de transmissão de dados por via óptica 5 para um dispositivo de leitura 1. O canal de transmissão de dados por via óptica 5 é disponibilizado em suplemento ao canal de transmissão de dados com recurso a uma antena no qual consiste o canal de transmissão de dados sem contacto 15.

Na Figura 2 encontra-se representado um suporte de dados sem contacto no qual foi montado um meio luminoso óptico 6. O meio luminoso, configurado como díodo emissor de luz (LED de acordo com o acrónimo inglês), díodo emissor de luz orgânico (OLED) ou ainda como díodo emissor de radiação infravermelha (IR-LED, "InfraRed LED" em inglês), encontra-se, tal como indica a seta 7, electricamente ligado ao "chip" 3, sendo comandado por este último. Também neste caso ocorre uma transmissão de dados por via óptica, por intermédio do canal 8 de transmissão de dados.

Na Figura 3 encontra-se representada uma outra forma de execução em que no suporte de dados 1a foi montado um meio receptor óptico 9, o qual se encontra electricamente ligado ao "chip" 3, possibilitando uma transmissão bidireccional de dados por via óptica entre o dispositivo de leitura 1 e o suporte de dados 1a. Neste caso, o "chip" 3 assume o comando da transmissão de dados tanto no caso da

transmissão de dados sem contacto 15, como no caso da transmissão de dados por via óptica 10. Estes dois canais de transmissão de dados podem funcionar alternadamente ou em simultâneo. Os referidos canais de transmissão de dados podem ainda funcionar numa situação de paridade ou de forma hierárquica (dita dono-escravo, "master-slave" em inglês).

Com recurso ao componente estrutural óptico representado na Figura 4, o qual exhibe uma ligação eléctrica 11 ao "chip" 3, e caso seja suficiente a quantidade de luz incidente 13, pode ser autorizada a transmissão de dados (assinalada com a seta 12) por via da interface sem contacto, com recurso à antena.

O processo de autorização da comunicação de informações secretas armazenadas no suporte de dados pode ser realizado, por exemplo, do modo seguinte. Tal como se encontra representado na Figura 5, a memória 21 do "chip" 3 exhibe diversas zonas de memória 24 ou 22 cuja leitura é parcialmente livre, mas parte de cujos conteúdos se encontra segura contra uma leitura indevida com o auxílio de chaves criptográficas adequadas. A zona de memória segura 22 contém pelo menos um conjunto de dados 23 constituído por informações secretas, tais como dados biométricos ou o número de identificação pessoal (PIN de acordo com o acrónimo inglês). A zona de memória de leitura livre 24 contém pelo menos um conjunto de dados 25 inequivocamente associado ao conjunto de dados 23 e representa um valor de compressão, por exemplo uma verificação de redundância

cíclica (CRC, "cyclic redundancy check" em inglês), uma dispersão ("hashing" em inglês), uma soma de conferência criptográfica. Fica excluída possibilidade de, a partir do conteúdo do conjunto de dados de leitura livre 25, retirar conclusões acerca do conteúdo do conjunto de dados secretos 26.

Para realizar a leitura de um dos conjuntos de dados 23 foi previsto, de acordo com o invento, que numa primeira etapa processual fosse lidos o conjunto de dados 25 a ele correspondente, por intermédio do canal de transmissão de dados com recurso à antena 15, bem como as informações opticamente legíveis 20, por exemplo um código de barras ou uma zona mecanicamente legível (MRZ, "machine readable zone" em inglês) do suporte de dados, neste caso com recurso ao dispositivo de leitura 1.

Numa segunda etapa do processo é derivada uma chave criptográfica 26 do conjunto de dados 25 e das informações ópticamente legíveis 20. Para este efeito pode ser utilizado qualquer um dos processos de derivação de chaves criptográficas amplamente conhecidos dos especialistas neste campo, tais como a derivação de uma chave com recurso a uma chave-mestra, etc. A chave criptográfica individual de um dado suporte de dados, a qual foi derivada da chave-mestra secreta, já se encontra guardada em memória no suporte de dados. A chave-mestra encontra-se guardada no dispositivo de leitura para efeito da derivação da chave criptográfica 26 por intermédio das informações 20 lidas

por via óptica e do conjunto de dados 26 lidos na ausência de contacto.

Uma terceira etapa do processo prevê que seja realizado um processo de autenticação 27 entre o dispositivo de leitura 1 e o "chip" 3 integrante do suporte de dados 1a por intermédio da chave criptográfica derivada. É deste modo verificado se a chave de que o dispositivo de leitura 1 tem conhecimento é idêntica à guardada em memória no suporte de dados 1a. Um processo de autenticação conhecido da técnica anterior funciona de acordo com o princípio de desafio e resposta ("challenge-response" em inglês) amplamente utilizado no âmbito dos cartões providos de um "chip". Através de um comando cuja designação inglesa é "getChallenge" (requisição de um desafio), o dispositivo de leitura recebe do "chip" 3 um número aleatório destinado à sua subsequente autenticação perante o "chip" com recurso aos dados de um comando cuja designação inglesa é "External Authenticate" (autenticação externa), os quais são derivados do número aleatório e da chave. Podem, evidentemente, ser utilizadas outras etapas de autenticação, por exemplo para efeito de uma autenticação mútua, bem como outros processos de autenticação.

Num processo simplificado, o dispositivo de leitura limitar-se-á, na terceira etapa processual, a autenticar-se como tal, com recurso a ambos os canais de transmissão de dados, sem dar prova do conhecimento de uma chave secreta. Na segunda etapa processual 26 é então por exemplo

derivado um valor, que, embora seja utilizado como chave para a terceira etapa 27, não é secreto ou derivado de uma chave-mestra.

Numa última etapa facultativa do processo é obtido um valor de compressão a partir do conjunto de dados secreto 23, o qual é comparado com o conteúdo do conjunto de dados 25 cuja leitura é livre (ver Figura 5, verificação 28). Caso os dois valores de compressão sejam distintos, deve partir-se do princípio de que o conjunto de dados 23 foi clandestinamente alterado. Após uma autenticação bem sucedida, o conjunto de dados 23 pode ser lido.

O processo representado na Figura 6 prevê também que o acesso a pelo menos uma parte dos dados armazenados no transpositor ("transponder" em inglês) apenas seja possível após uma autenticação bem sucedida. O processo também funciona de acordo com o princípio de desafio e resposta ("challenge-response" em inglês).

Numa primeira etapa 30, o dispositivo de leitura solicita um número aleatório do suporte de dados 1a por via do canal de transmissão de dados com recurso à antena 15. Numa forma de execução de acordo com o invento, um número aleatório gerado pelo suporte de dados 1a é transmitido ao dispositivo de leitura 1 por via do canal de transmissão de dados por via óptica 5, por exemplo um LED emissor de radiação infravermelha ou ultravioleta (etapa 31: resposta). Uma outra possibilidade consiste em fornecer o número

aleatório sob a forma de código de barras, código de “pixels”, zonas mecanicamente legíveis (MRZ, “machine readable zones” em inglês) no visor 4 do suporte de dados sem contacto 1a. Também pode ser simultaneamente enviada uma resposta por via do canal de transmissão de dados com recurso à antena 15, resposta essa que se distingue no que respeita ao conteúdo dos dados transmitidos sem contacto, por via óptica, mas evita um intervalo de expiração (“time-out” em inglês) no canal de transmissão de dados, e portanto no dispositivo de leitura em particular. Por um lado, um potencial atacante não pode retirar conclusões no que respeita ao conteúdo ao quando da sua audição não autorizada do canal 15 de transmissão de dados com recurso à antena; por outro lado, também não é requerido um tratamento especial dos comandos individuais da aplicação, pelo que o “software” do dispositivo de leitura 1 não tem de ser sujeito a alterações. Pode, por exemplo, enviar-se o código “90 00” (comando executado com sucesso). Para confundir potenciais agressores também podem ser transmitidos dados falsos.

Também é concebível a requisição do número aleatório através do canal de transmissão de dados por via óptica e a sua transmissão por via do canal de transmissão de dados com recurso à antena.

O algoritmo de autenticação corre em seguida de acordo com o processo conhecido para efeito da autenticação unilateral ou mútua (“External Authenticate” 32). Caso o

processo de autenticação tenha sido concluído com sucesso, a comunicação propriamente dita pode ter início e o conjunto de dados 23 pode ser lido.

O processo descrito com recurso à Figura 6 pode ser utilizado isoladamente ou em combinação com o processo descrito com recurso à Figura 5.

Uma vantagem dos processos descritos precedentemente consiste na dificultação considerável da falsificação ou partilha de dados resultante da utilização de dois canais de transmissão de dados distintos, o canal de transmissão de dados por via óptica 5 e o canal de transmissão de dados 15 com recurso à antena. Por este motivo, estes processos são particularmente adequados para a partilha de dados sensíveis, nomeadamente pessoais. Uma autenticação unilateral ou uma autenticação mútua são melhoradas pela utilização conjunta de dois canais de transmissão de dados.

Caso se pretenda processar dados sensíveis com recurso ao mesmo suporte de dados 1a, será imprescindível utilizar para tal ambos os canais de transmissão de dados quando da leitura por parte do dispositivo de leitura. A comutação entre um único e dois canais de transmissão pode ser realizada de forma automática após introdução de uma bandeira ("flag" em inglês).

Um dispositivo de leitura 1 de acordo com o invento consiste num aparelho inteligente que dispõe não só

de um meio de leitura com recurso à antena e portanto sem contacto 2, como de meios de leitura óptica. Numa sua forma preferida de execução, o dispositivo de leitura 1 foi configurado como terminal móvel, por exemplo como telemóvel, computador de bolso (PDA, "Personal Digital Assistant" em inglês), computador portátil ("laptop" em inglês), etc., exibindo uma interface destinada à comunicação sem contacto, nomeadamente uma interface de comunicação numa zona de proximidade (NFC, "Near Field Communication" em inglês). Como meio óptico de comunicação pode ser utilizada a interface IRDA para a transmissão de dados mediante radiação infravermelha de acordo com o padrão da organização IRDA ("InfraRed Data Association" em inglês) presente na maioria dos aparelhos. Como meio óptico de leitura pode ser utilizada uma câmara. De preferência, os dados opticamente legíveis, tais como o número de série do "chip" 3 de que é provido o suporte de dados 1a, são reproduzidos sob uma forma mecanicamente legível (código de barras, dados passíveis de reconhecimento óptico de caracteres [OCR, em inglês]). Um tal dispositivo de leitura 1 é particularmente adequado para a realização de um controlo de documentos de viagem por parte da polícia ou dos funcionários aduaneiros, caso em que, por intermédio de uma eventual ligação em linha adicional, pode proceder-se a um questionário complementar.

Para aumentar a segurança pode estar previsto que o "chip" 3 de que o suporte de dados 1a é provido proceda adicionalmente à geração, a título de número de série, de

um número aleatório, o qual transmite ao dispositivo de leitura 1 por intermédio do canal de transmissão de dados com recurso à antena. A utilização destes números de série aleatórios encontra-se descrita, por exemplo, na norma ISO 14443 (capítulo 6.4.4 intitulado "UID contents and cascade levels"). O número de série do suporte de dados 1a, número que é necessário ao desenvolvimento do algoritmo anti-colisão, não consiste, como é usual, numa cifra inequívoca e inconfundível, mas num número aleatório gerado sucessivamente quando de cada nova transacção. Esta medida impede que a identidade do suporte de dados possa ser retro-activamente inferida a partir do número de série utilizado. Pode deste modo ser eficazmente impedido um eventual ataque mediante repetição ("replay" em inglês) de uma comunicação entre o suporte de dados e o terminal escutada num instante anterior.

Os dados opticamente legíveis podem ser disponibilizados de um modo não estático pelo suporte de dados 1a, prestando-se a ser dinamicamente alterados por intermédio de um visor, por exemplo. Deixam-se este modo gerar e reproduzir códigos ou senhas ("passwords" em inglês) utilizáveis uma única vez, números de série aleatórios, etc. São ainda concebíveis quaisquer combinações de dados gerados dinamicamente e transmissíveis ou com recurso à antena ou por via óptica. Lisboa, 6 de Julho de 2009

REIVINDICAÇÕES

1. Suporte de dados sem contacto provido de uma antena e de um "chip", em que o suporte de dados contém dados legíveis com recurso a uma antena, os quais podem ser transmitidos para um dispositivo de leitura por intermédio de um canal de transmissão de dados com recurso à antena, em em que o suporte de dados contém dados opticamente legíveis que podem ser transmitidos para um dispositivo de leitura por intermédio de um canal de transmissão de dados por via óptica e são adequados para fazer parte de um processo de autenticação entre o suporte de dados e o dispositivo de leitura, **caracterizado por** o suporte de dados ter sido configurado de modo a que sejam obrigatoriamente utilizados ambos os canais de transmissão para efeito de uma tal autenticação, de modo a que seja possível a derivação de um valor a partir de pelo menos uma primeira parte dos dados legíveis com recurso à antena, bem como a partir dos dados opticamente legíveis, e a que o acesso a pelo menos uma segunda parte dos dados legíveis com recurso à antena apenas seja possível depois de bem sucedida uma autenticação com recurso ao valor derivado.

2. Suporte de dados de acordo com a reivindicação 1, caracterizado por o "chip" exhibir zonas de memória, das quais pelo menos uma é de leitura livre, sendo pelo menos uma outra legível apenas uma vez concluída a autenticação entre o suporte de dados e o dispositivo de lei-

tura.

3. Suporte de dados de acordo com a reivindicação 1, caracterizado por a segunda zona de memória, que apenas pode ser lida após uma autenticação, exibir pelo menos um primeiro conjunto de dados e a zona de memória que é de leitura livre exibir pelo menos um segundo conjunto de dados inequivocamente associado ao primeiro conjunto de dados, do qual o segundo conjunto de dados pode ser derivado.

4. Suporte de dados de acordo com uma das reivindicações 2 ou 3, caracterizado por os conjuntos de dados guardados em memória serem armazenados sob a forma de conjuntos de dados encriptados com recurso a uma chave criptográfica.

5. Suporte de dados de acordo com as reivindicações 3 ou 4, caracterizado por o segundo conjunto de dados constituir um valor de compressão do primeiro conjunto de dados.

6. Suporte de dados de acordo com uma das reivindicações 1 a 5, caracterizado por sobre o suporte de dados se encontrar disposto um componente estrutural sensível à luz, o qual comanda o funcionamento do "chip" em função da claridade detectada.

7. Suporte de dados de acordo com uma das rei-

vindicações 1 a 6, caracterizado por sobre o suporte de dados conter informações opticamente legíveis.

8. Suporte de dados de acordo com a reivindicação 7, caracterizado por o suporte de dados conter um código matricial.

9. Suporte de dados de acordo com a reivindicação 7, caracterizado por o suporte de dados conter um código de barras.

10. Suporte de dados de acordo com uma das reivindicações precedentes caracterizado por o suporte de dados ter sido provido de um visor destinado à reprodução opticamente legível de dados.

11. Suporte de dados de acordo com uma das reivindicações precedentes caracterizado por o suporte de dados ter sido provido de um meio luminoso destinado a emitir sinais ópticos.

12. Suporte de dados de acordo com uma das reivindicações precedentes caracterizado por o suporte de dados ter sido provido de um meio receptor óptico destinado à recepção de sinais ópticos.

13. Suporte de dados de acordo com uma das reivindicações precedentes caracterizado por o suporte de dados ter sido provido de um altifalante.

14. Suporte de dados de acordo com uma das reivindicações precedentes caracterizado por o suporte de dados ter sido provido de um alarme vibratório.

15. Processo para a determinação fiável da utilização deliberada de um suporte de dados sem contacto, em que, consoante os dados a serem transaccionados entre o suporte de dados e um dispositivo de leitura, é realizada, além de uma transmissão sem contacto, com recurso a uma antena, de dados passíveis de serem lidos a partir do suporte de dados com recurso à antena, uma transmissão de dados por via óptica, em que esta última é realizada com recurso a um dispositivo de leitura a partir de dados opticamente legíveis pelo mesmo que se encontram dispostos sobre o suporte de dados, **caracterizado por** se proceder a uma autenticação entre o suporte de dados e o dispositivo tal que é de molde a que, para derivar um valor de pelo menos uma primeira parte dos dados passíveis de serem lidos com recurso à antena, bem como a partir dos dados opticamente legíveis, têm de ser utilizados tanto o canal de transmissão de dados com recurso à antena como o canal de transmissão de dados por via óptica e em que o acesso a pelo menos uma segunda parte dos dados que podem ser lidos com recurso à antena somente é possível depois de bem sucedida uma autenticação com recurso ao valor derivado.

16. Processo de acordo com a reivindicação 15, caracterizado por a transmissão de dados se realizar bidireccionalmente.

17. Processo de acordo com as reivindicações 15 ou 16, caracterizado por poder ocorrer discricionariamente uma comutação entre as transmissões de dados por via óptica, por um lado, e com recurso à antena, por outro.

18. Processo de acordo com as reivindicações 15 a 17, caracterizado por ocorrer uma autenticação pelo menos unilateral (27, 32) entre o dispositivo de leitura e o suporte de dados.

19. Processo de acordo com a reivindicação 18, caracterizado por a autenticação ser realizada mediante uma transmissão de dados por via óptica.

20. Processo de acordo com uma das reivindicações 15 a 19, caracterizado por ser requisitado um número aleatório por intermédio de um dos dois canais de transmissão de dados, o de transmissão por via óptica e o de transmissão com recurso a uma antena, e por esse número ser transmitido por intermédio do outro dos dois canais de transmissão de dados.

21. Processo de acordo com as reivindicações 15 a 20, caracterizado por, no intuito de realizar uma leitura de um primeiro conjunto de dados (23), se começar, numa primeira etapa processual e por intermédio do dispositivo de leitura, por proceder à leitura de um segundo conjunto de dados (25) associado ao primeiro conjunto de dados e dos dados (20) opticamente reproduzidos sobre o suporte de

dados.

22. Processo de acordo com a reivindicação 21, caracterizado por, numa segunda etapa processual (26), o dispositivo de leitura gerar o valor derivado a partir dos dados lidos e de uma chave secreta, por, numa terceira etapa processual e com base no valor derivado, ocorrer um processo de autenticação (27) entre o dispositivo de leitura e o suporte de dados, e por, numa quarta etapa processual, se proceder à leitura do primeiro conjunto de dados (23) por intermédio do dispositivo de leitura.

23. Processo de acordo com as reivindicações 21 ou 22, caracterizado por, numa quinta etapa processual, ser gerado a partir do primeiro conjunto de dados um valor de compressão e, numa etapa processual subsequente, ser realizada uma comparação do valor de compressão gerado desse modo com o segundo conjunto de dados.

24. Processo de acordo com uma das reivindicações 18 a 23, caracterizado por a autenticação (27, 32) ser realizada na modalidade de desafio e resposta.

25. Dispositivo de leitura com meios para a transmissão de dados com recurso a uma antena de pelo menos dados legíveis com recurso à antena a partir de um suporte de dados sem contacto e com meios para a leitura óptica de dados opticamente legíveis constantes do suporte de dados, **caracterizado por** o dispositivo de leitura ter sido con-

figurado de modo a que, para efeito de uma autenticação entre o dispositivo de leitura e o suporte de dados, tenham de ser obrigatoriamente utilizados ambos os canais de transmissão de dados a fim de derivar um valor a partir de pelo menos uma primeira parte dos dados legíveis com recurso à antena, bem como a partir dos dados opticamente legíveis, valor esse que é adequado para, uma vez concluída com sucesso a autenticação por intermédio do valor derivado, facultar o acesso a pelo menos uma segunda parte dos dados legíveis com recurso à antena.

26. Dispositivo de leitura de acordo com a reivindicação 25, caracterizado por exibir meios para o envio de um sinal óptico.

27. Dispositivo de leitura de acordo com a reivindicação 25, caracterizado por exibir meios para modular o sinal óptico.

28. Dispositivo de leitura de acordo com a reivindicação 25, caracterizado por exibir uma interface infravermelha.

29. Dispositivo de leitura de acordo com uma das reivindicações 25 a 28, caracterizado por ter sido configurado como terminal móvel.

30. Dispositivo de leitura de acordo com uma das reivindicações 25 a 29, caracterizado por exibir uma inter-

face para a comunicação de proximidade.

31. Dispositivo de leitura de acordo com uma das reivindicações 25 a 30, caracterizado por estar adaptado à leitura de um suporte de dados sem contacto de acordo com uma das reivindicações 1 a 14.

Lisboa, 6 de Julho de 2009

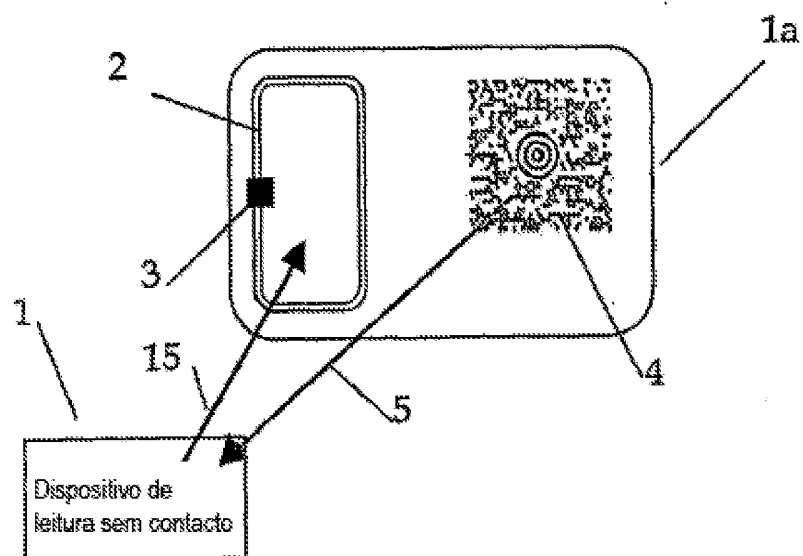


Fig. 1

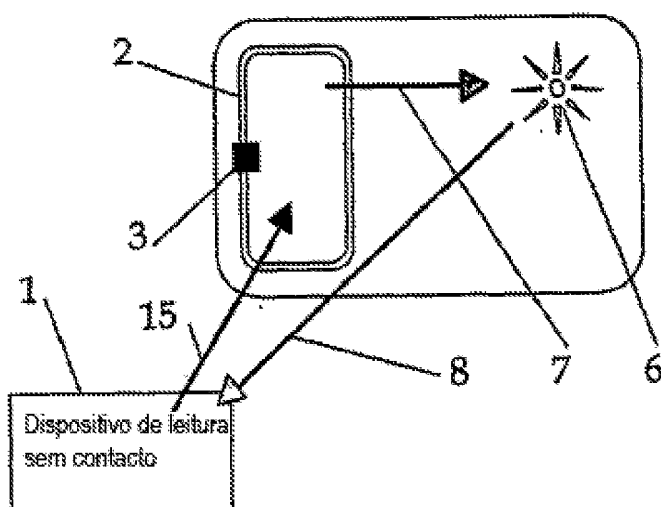


Fig. 2

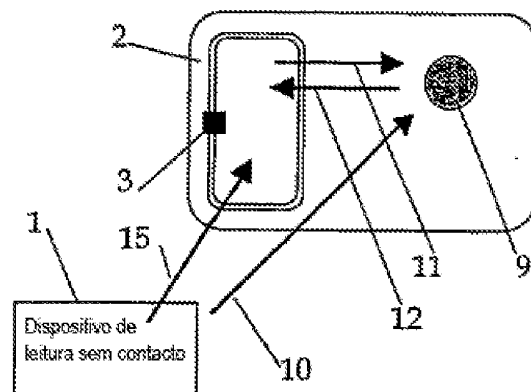


Fig. 3

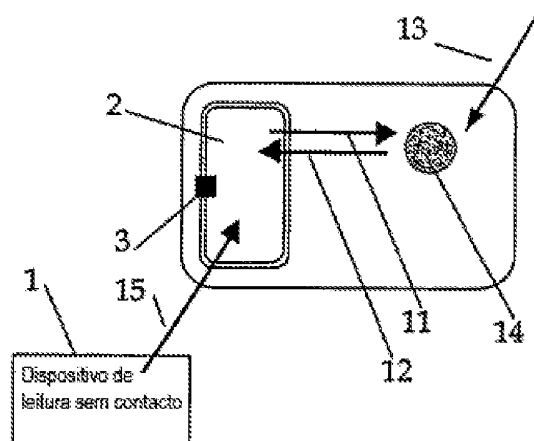


Fig. 4

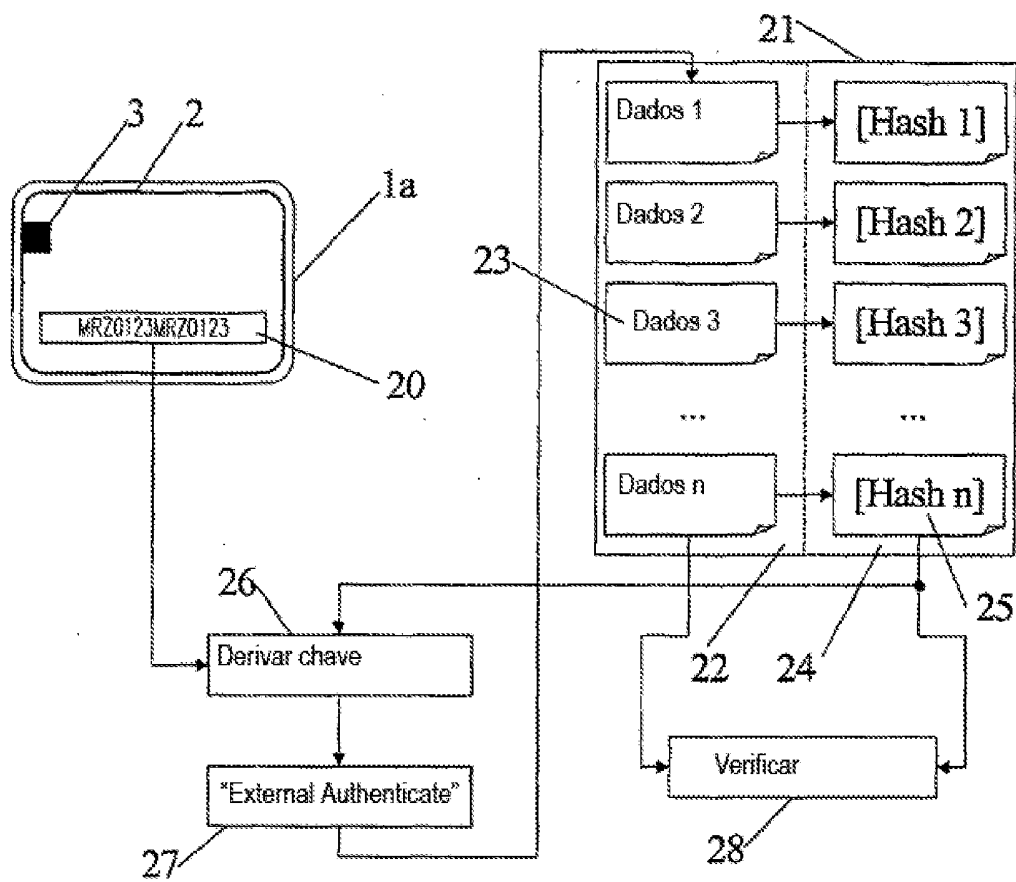


Fig. 5

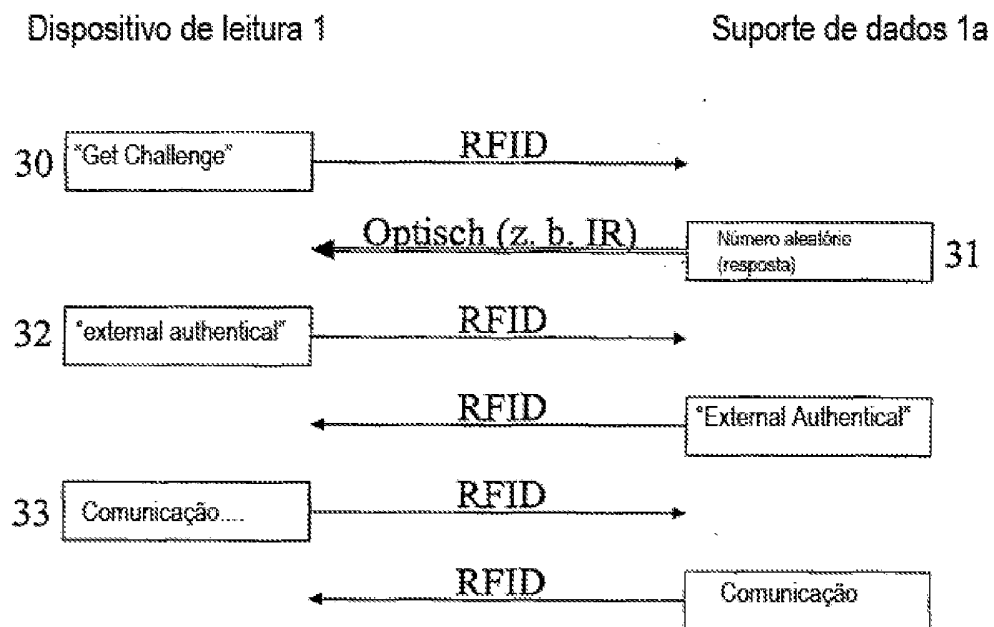


Fig. 6

PE1616291

DOCUMENTOS CITADOS NA DESCRIÇÃO

Esta lista de documentos citados pelo requerente foi estabelecida exclusivamente para informação do leitor e não é parte integrante do documento de patente europeia. Foi organizada com o maior cuidado; o EPA não assume contudo qualquer responsabilidade por eventuais erros ou omissões.

Documentos de patente citados na descrição

- FR 2770316 A
- US 20030057276 A1