(11) Número de Publicação: **PT 1907993 E**

(51) Classificação Internacional:
G06K 19/07 (2013.01) ***G06K 19/73*** (2013.01)
G06K 19/77 (2013.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2006.07.24**

(30) Prioridade(s): **2005.07.25 FR 0507887**

(43) Data de publicação do pedido: **2008.04.09**

(45) Data e BPI da concessão: **2013.12.04**
047/2014

(73) Titular(es):
OBERTHUR TECHNOLOGIES
420, RUE D'ESTIENNES D'ORVES 92700 COLOMBES **FR**

(72) Inventor(es):
CHRISTOPHE GOYET **FR**

(74) Mandatário:
NUNO MIGUEL OLIVEIRA LOURENÇO
RUA CASTILHO, Nº 50 - 9º 1269-163 LISBOA **PT**

(54) Epígrafe: **ENTIDADE ELETRÓNICA COM MEIOS DE COMUNICAÇÃO POR CONTACTO E À DISTÂNCIA**

(57) Resumo:
UMA ENTIDADE ELETRÓNICA QUE COMPREENDE MEIOS DE COMUNICAÇÃO POR CONTACTO (4) E MEIOS DE COMUNICAÇÃO À DISTÂNCIA (6). MEIOS (2, K) SÃO TAMBÉM FORNECIDOS PARA PERMITIR UMA TROCA DE ALGUNS DADOS PELO MENOS ATRAVÉS DOS MEIOS DE COMUNICAÇÃO À DISTÂNCIA EM FUNÇÃO DA RECEÇÃO PRÉVIA DE UMA INSTRUÇÃO ATRAVÉS DOS MEIOS DE COMUNICAÇÃO POR CONTACTO. UM TERMINAL PARA COMUNICAR COM TAL ENTIDADE ELETRÓNICA ASSIM COMO PROCESSOS DE COMANDO E DE PERSONALIZAÇÃO DE UMA TAL ENTIDADE ELETRÓNICA SÃO TAMBÉM DESCRITOS.

RESUMO

"ENTIDADE ELETRÓNICA COM MEIOS DE COMUNICAÇÃO POR CONTACTO E À DISTÂNCIA"

Uma entidade eletrónica que compreende meios de comunicação por contacto (4) e meios de comunicação à distância (6). Meios (2, K) são também fornecidos para permitir uma troca de alguns dados pelo menos através dos meios de comunicação à distância em função da receção prévia de uma instrução através dos meios de comunicação por contacto. Um terminal para comunicar com tal entidade eletrónica assim como processos de comando e de personalização de uma tal entidade eletrónica são também descritos.

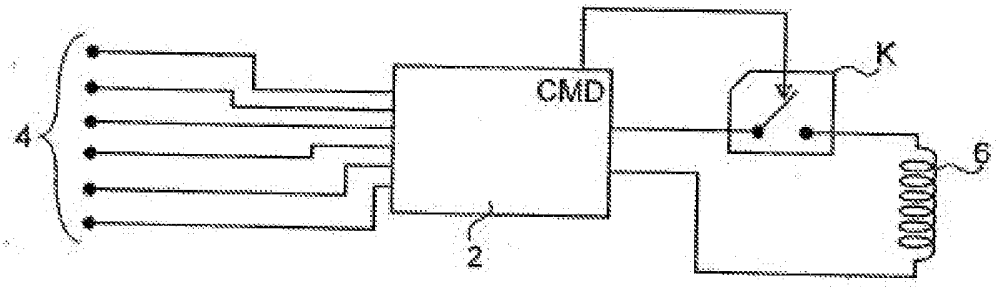

Fig. 1

DESCRIÇÃO

A invenção refere-se a uma entidade eletrónica com meios de comunicação por contacto e meios de comunicação à distância, um terminal de comunicação com uma tal entidade eletrónica assim como processos de comando e de personalização dessa entidade eletrónica.

Uma entidade eletrónica, como por exemplo um cartão microcircuito, que inclui em geral circuitos eletrónicos aptos para memorizarem informações, tem meios de comunicação com o exterior, especialmente para trocar informações detidas pela entidade eletrónica com dispositivos externos do tipo leitor ou terminal.

Entre os meios de comunicação correntemente utilizados, distinguem-se meios de comunicação por contacto, para os quais um contacto físico entre a entidade eletrónica e o terminal é uma condição necessária para o estabelecimento de uma comunicação, e os meios de comunicação à distância, graças aos quais uma comunicação entre a entidade eletrónica e um leitor é possível sem contacto físico entre esses dois elementos com um alcance da ordem de alguns centímetros em geral.

Algumas entidades de eletrónica reagrupam, por outro lado meios de comunicação dos dois tipos supracitados, caso em que os modos de funcionamento "*por contacto*" e "*sem contacto*" podem ser organizados de acordo com as funcionalidades exigidas pelo aparelho para cada um dos modos de comunicação, com está descrito nas patentes US 5 206 495 e US 5 999 713.

Se a utilização dos meios de comunicação sem contacto é conhecida para a sua conveniência (visto que nenhum posicionamento exato da entidade eletrónica é necessário para a troca de informações), tem no entanto o inconveniente de um risco de troca inoportuno de informações, por exemplo pelo estabelecimento de uma comunicação não desejada pelo utilizador no momento da sua passagem próximo de um leitor. Esse problema é particularmente sensível quando a entidade eletrónica guarda informações confidenciais, como por exemplo no caso de um passaporte eletrónico.

Portanto já se procurou no estado da técnica tomar medidas para evitar essa troca inoportuna de dados, por vezes referidos com o termo anglo-saxónico "*anti-skimming*".

Nesse sentido, foi proposto no pedido de patente WO 99/16019 dispor de um interruptor sobre a face superior de um cartão microcircuito para tornar possível a receção de dados por esse cartão somente depois da ativação do interruptor. A adição de um tal interruptor na entidade eletrónica põe no entanto problemas de realização e de fiabilidade (por exemplo no caso de flexão repetida da entidade eletrónica tal como definida pela norma ISO7816) e aumenta o seu custo de fabrico.

É provavelmente a razão pela qual foi proposto na patente US 6 424 029 usar um interruptor do tipo capacitivo mais bem adaptado, para a constituição geral das entidades eletrónicas portadoras de informações, em particular no caso dos cartões microcircuito. Se essa solução reduz as dificuldades que acabam de ser referidas, não consegue evitá-las totalmente.

Além disso, as soluções que acabam de ser lembradas perdem flexibilidade e especialmente não permitem considerar uma limitação do acesso ao modo de comunicação sem contacto, por exemplo por palavra-chave.

Conhece-se também do pedido de patente EP 1 258 831 um cartão microcircuito com uma interface de contacto e uma interface sem contacto em que a interface para utilizar é determinada em função do tipo de dados para trocar. O preâmbulo da reivindicação 1 é conhecido desse documento.

Neste contexto, a invenção propõe uma entidade eletrónica de acordo com a reivindicação 1. Essa entidade eletrónica que compreende meios de comunicação por contacto, meios de comunicação à distância, é caracterizada por meios para autorizarem uma troca de alguns dados pelo menos através dos meios de comunicação à distância em função da receção prévia de uma instrução através dos meios de comunicação por contacto.

A possibilidade de trocar os dados pelos meios de comunicação à distância pode assim ser gerida por meio da ligação por contacto, por exemplo mediante um terminal.

A troca de dados referida pela autorização é por exemplo a emissão de pelo menos alguns dados e/ou pelo menos a receção de alguns dados.

De acordo com uma primeira forma de realização possível, a entidade eletrónica compreende também meios de memorização de uma informação de ativação controlados pela referida instrução e meios para permitirem a troca (emissão e/ou receção) dos referidos dados através dos meios de comunicação à distância na presença da referida informação de ativação.

Pode assim separar-se a receção da instrução e a troca (por exemplo a emissão) dos dados, por exemplo no plano temporal.

A entidade eletrónica pode também compreender de modo complementar meios para inibir a troca dos referidos dados através dos meios de comunicação à distância na ausência da referida informação de ativação.

Quando os meios de comunicação à distância compreendem uma antena, os referidos meios para autorizarem uma troca compreendem, de acordo com uma segunda forma de realização possível, meios para comandar uma conexão da antena para um microcircuito sobre a base da referida instrução. A autorização e a inibição da troca (é por exemplo emissão e/ou receção) são então particularmente eficazes.

A entidade eletrónica é por exemplo um cartão microcircuito de acordo com a norma ISO14443 e/ou com a norma ISO7816.

A invenção propõe também um terminal que compreende meios de comunicação por contacto com uma entidade eletrónica que compreende meios de comunicação à distância, caracterizado por meios para emitir, através dos meios de comunicação por contacto, uma instrução destinada a condicionar uma troca de alguns dados pelo menos através dos meios de comunicação à distância.

Um tal terminal pode gerir a autorização de troca pelos meios de comunicação à distância da entidade eletrónica. A troca referida pela autorização pode ser uma emissão e/ou uma receção de dados.

Um tal terminal pode ser portátil: pode especialmente tratar-se de um terminal portátil ad hoc que permite gerir a autorização de troca pelos meios de comunicação à distância da entidade eletrónica.

A invenção propõe para além disso um processo de comando de uma entidade eletrónica de acordo com a reivindicação 4. Esse processo que compreende meios de comunicação por contacto e meios de comunicação sem contacto é caracterizado pelas etapas seguintes:

- receção de uma instrução de ativação através dos meios de comunicação por contacto;
-aplicação de uma autorização de troca de alguns dados pelo menos através dos meios de comunicação à distância para receção da referida instrução de ativação.

A possibilidade de trocar os dados através dos meios de comunicação à distância é deste modo controlada pela instrução de ativação, com as vantagens já mencionadas.

Neste processo, uma etapa de troca (emissão e/ou receção) dos referidos dados através dos meios de comunicação à distância é condicionada por exemplo pela referida autorização.

De acordo com uma forma possível de realização, a autorização é aplicada pela definição para um valor predeterminado de uma informação de ativação e a referida etapa de emissão condicionada compreende as seguintes etapas:

- verificação de que o valor da informação de ativação é igual ao valor predeterminado;

- troca (por exemplo emissão) dos referidos dados através dos meios de comunicação à distância somente no caso de verificação positiva.

Este processo é prático para aplicar e tem as vantagens já mencionadas em termos de separação da autorização e da troca.

O processo pode também compreender uma etapa de colocação da informação de ativação para um valor complementar do valor predeterminado num instante definido.

De acordo com uma outra forma possível de realização, o processo compreende uma etapa de inibição da troca num instante definido dos referidos dados.

O instante definido pode corresponder para a receção de um comando de fim de comunicação pelos meios de comunicação à distância, o que permite à instrução somente autorizar uma única comunicação.

O instante definido pode ser determinado por uma temporização, o que permite limitar a duração da autorização no tempo.

O instante definido pode ser alcançado depois da receção de um número predeterminado de comandos via os meios de comunicação à distância, o que permite limitar as possibilidades de utilização da autorização.

O instante definido pode corresponder à conclusão de uma etapa de inicialização da comunicação.

A invenção propõe finalmente um processo de personalização de uma entidade eletrónica que compreende

meios de comunicação sem contacto caracterizado por uma etapa de escrita de uma informação de ativação destinada a condicionar a troca de alguns dados pelo menos através dos meios de comunicação à distância.

Pode assim determinar-se no momento da personalização da entidade eletrónica se a utilização dos meios de comunicação sem contacto será autorizada por defeito.

A referida informação de ativação pode por outro lado ser modificada na receção de uma instrução através dos meios de comunicação por contacto da entidade eletrónica. Trata-se por exemplo de uma instrução segura.

Este processo pode compreender além disso uma etapa de escrita de uma informação de configuração representativa das condições de modificação da informação de ativação. Pode assim configurar-se a entidade eletrónica no que respeita as possibilidades de utilizar os meios de comunicação à distância no momento da personalização em função da sua utilização ulterior, sem que isso implique modificações dos circuitos utilizados.

Outras características e vantagens da invenção vão aparecer à luz da descrição seguinte, feitas em referência aos desenhos anexados nos quais:

- a figura 1 representa um primeiro exemplo de uma entidade eletrónica de acordo com os ensinamentos da invenção;
- a figura 2 é um fluxograma que ilustra o funcionamento geral da entidade eletrónica da figura 1;
- a figura 3 representa um segundo exemplo de uma entidade eletrónica de acordo com os ensinamentos da invenção;

- a figura 4 representa um exemplo possível de constituição física da entidade eletrónica da figura 3;

- a figura 5 é um fluxograma que descreve uma primeira parte do funcionamento da entidade eletrónica da figura 3;

- a figura 6 é um fluxograma que ilustra uma segunda parte do funcionamento da entidade eletrónica da figura 3.

O exemplo de entidade eletrónica representado na figura 1 compreende um microcircuito 2 (por exemplo um microcontrolador seguro como usado geralmente nos cartões inteligentes) apto para comunicar com outros dispositivos eletrónicos por um lado mediante contactos 4, estando cada contacto ligado a um terminal do microcircuito, e por outro lado, mediante uma antena magnética 6, formada por exemplo pelo enrolamento de uma pluralidade de espiras.

A antena magnética 6 está ligada a dois terminais do microcircuito com interposição de um interruptor K comandado por um terminal de comando CMD do microcircuito 2. Assim, sobre comando de um sinal gerado no terminal CMD, o microcircuito pode comandar a conexão da antena 6 para o microcircuito 2, e assim autorizar ou inibir a utilização de meios de comunicação à distância de que essa antena 6 faz parte.

Presentemente vai descrever-se em referência à figura 2 o funcionamento geral desse dispositivo.

Deverá notar-se primeiramente que, nesta forma de realização, a entidade eletrónica só é alimentada eletricamente quando está conectada pelos seus meios de comunicação por contacto (conjunto dos contactos 4) a um dispositivo exterior do tipo terminal, que garante uma conexão elétrica com cada um dos contactos 4 e assim

permite especialmente a fonte de alimentação da entidade eletrónica.

O interruptor elétrico K é então por exemplo tal que está aberto na ausência da fonte de alimentação (e especialmente por exemplo na ausência de sinal no terminal CMD),de modo que os meios de comunicação à distância que compreendem a antena 6 não podem ser usados enquanto a entidade eletrónica não estiver conectada (por meio dos contactos 4) ao terminal que garante a sua alimentação: na presente forma de realização, a entidade eletrónica não é fornecida para funcionar sobre uma só base de uma telealimentação fornecida pela antena 6.

O esquema geral de funcionamento da entidade eletrónica da figura 1 começa portanto no momento da conexão dessa entidade eletrónica para um terminal (via os contactos 4), o que provoca a inicialização da comunicação entre a entidade eletrónica (isto é o microcircuito 2) e o terminal (por exemplo meios de tipo microcircuito nesse terminal), como representado na etapa E2 na figura 2.

No momento da etapa de inicialização, efetua-se especialmente um comando do interruptor K de modo a que este esteja na posição aberta, o que permite inibir a comunicação sem contacto como explicado acima. O comando de abertura do interruptor K é efetuado pelo microcircuito 2 colocando o terminal CMD do potencial que provoca a abertura do interruptor K, por exemplo um potencial representando um nível lógico 0.

A entidade eletrónica pode então ter um funcionamento normal de modo “contactos”, durante o qual se procede por exemplo a uma troca de dados entre a entidade eletrónica e o terminal a que está conectada (etapa E4).

Durante essas trocas de dados, a entidade eletrónica pode receber especialmente uma instrução autorizando a comunicação de modo sem contacto, como representado na etapa E6.

Uma tal instrução é por exemplo um código de operação particular quando o microcircuito 2 da entidade eletrónica é dirigido no seu funcionamento por tais códigos recebidos do terminal. Em alternativa, poderá tratar-se de um dado (como por exemplo um código secreto introduzido pelo utilizador no terminal) cuja exatidão será interpretada pelo microcircuito 2 como uma instrução que autoriza a comunicação de modo "*sem contacto*".

Na receção desta instrução no momento da etapa E6, o micro circuito 2 comanda na etapa E8 o fechamento do interruptor K 8 por exemplo fazendo passar o terminal CMD para um potencial correspondente ao nível lógico 1); assim, a antena 6 é conectada nas suas duas extremidades ao microcircuito 2, o que torna possível uma comunicação da entidade eletrónica com um dispositivo externo através dessa antena 6, isto é através dos meios de comunicação sem contacto.

Na presente forma de realização, como descrito mais abaixo, o fechamento do interruptor K durará até ao fim de uma comunicação via os meios de comunicação sem contacto. Em alternativa, a comunicação sem contacto poderia só ser autorizada por um período predeterminado (temporização no fim da qual o potencial no terminal CMD volta a passar para o nível lógico 0). Outras variantes são também possíveis como explicado a propósito da segunda forma de realização.

Uma vez fechado o interruptor K, a entidade eletrónica está apta para estabelecer uma comunicação sem contacto com

um leitor destinado para esse fim (associado ou não ao terminal de comunicação por contacto), como está representado na etapa E10, o que permite uma troca de dados de modo "*sem contacto*" entre a entidade eletrónica e o leitor, como indicado na figura 2 pela etapa E12.

No fim do diálogo de modo sem contacto entre a entidade eletrónica e o leitor, isto é quando esses dois dispositivos procederam às trocas de dados fornecidos, a entidade eletrónica recebe uma instrução "*fim de transação*", como por exemplo a instrução "*DESELECT*" definida de acordo com a norma ISO1443-4, como representado na etapa E14.

Na receção de uma tal instrução, o microcircuito 2 comanda a abertura do interruptor K (pondo no exemplo aqui descrito num nível lógico 0 o terminal CMD), o que provoca a inibição da comunicação sem contacto visto que a antena 6 já não está conectada ao microcircuito 2, como representado na etapa E16.

Como já indicado, a inibição da comunicação sem contacto (aqui mediante a abertura do interruptor K) poderia como alternativa intervir sob outras condições, tal como uma certa duração a partir da autorização dessa comunicação, a saída da entidade eletrónica do campo do leitor, ou outra, como também mencionado mais abaixo.

O funcionamento retoma então a etapa E4 pela gestão do modo "*contacto*".

Deverá notar-se que a forma de realização que acaba de ser descrita é particularmente vantajosa quando um leitor que funciona à distância deve comunicar com a entidade

eletrónica mesmo se esta também está conectada a um terminal que funciona por contacto. Pode tratar-se por exemplo de um cartão microcircuito inserido num terminal adaptado para um veículo no momento da passagem deste sob um pórtico equipado com um leitor que funciona à distância. A troca de dados entre a entidade eletrónica e o leitor à distância (por exemplo para a abertura de uma barreira e/ou o pagamento de uma portagem) pode assim estar sujeita a condições particulares geridas pelo terminal de contactos colocados no veículo, como por exemplo a introdução de um código secreto pelo utilizador nesse terminal ou um interruptor de comando no volante.

Uma segunda forma de realização da invenção será presentemente descrita em referência às figuras de 3 a 6.

A figura 3 representa os elementos principais de uma entidade eletrónica de acordo com essa segunda forma de realização: essa entidade eletrónica compreende um microcircuito 12 (por exemplo um microprocessador) que pode ser conectado a um dispositivo exterior do tipo terminal mediante contactos 14 para estabelecer uma comunicação do tipo "*por contacto*" entre a entidade eletrónica e esse terminal.

A entidade eletrónica compreende também uma antena 16 conectada em cada uma das suas extremidades a um terminal correspondente do microcircuito 12 (sem que esteja previsto interromper as ligações entre a antena 16 e o microcircuito 12 contrariamente à primeira forma de realização descrita precedentemente).

A antena 16 faz parte de meios de comunicação à distância da entidade eletrónica.

Uma memória regravável 18 (por exemplo uma memória não volátil do tipo memória apagável e programável eletronicamente, em geral denominada pelo acrónimo anglo-saxónico EEPROM) está também conectada ao microcircuito 12.

Deverá notar-se que, nesta forma de realização, o microcircuito 12 pode ser alimentado através da ligação por contactos (via pelo menos um dos contactos 14) ou, independentemente dessa primeira possibilidade de alimentação, por uma telealimentação de utilização da antena magnética 16 (e isso contrariamente à primeira forma de realização). A utilização do modo de comunicação "sem contacto" não será portanto aqui condicionada pela utilização simultânea da ligação por contacto (através dos contactos 14).

A entidade eletrónica poderá pois ser alimentada quer por ligação por contacto, quer por telealimentação, o que dá lugar a dois modos principais de funcionamento descritos respetivamente nas figuras 5 e 6; uma alimentação simultânea pela alimentação por contacto e a telealimentação é naturalmente possível sem pôr em causa os princípios de funcionamento das duas formas descritas acima.

No momento de uma comunicação da entidade eletrónica com um terminal através dos contactos 14, o processo ilustrado na figura 5 é aplicado sob o comando do microcircuito 12 (por exemplo programado mediante instruções armazenadas na memória).

Anteriormente, por exemplo no momento de uma etapa de inicialização dos dados armazenados na entidade eletrónica (como por exemplo a etapa de personalização convencionalmente usada na fabricação dos cartões

microcircuito antes da sua colocação no mercado), põe-se a 0 um bit de ativação armazenado por exemplo na memória regravável 18, o que permite indicar que, por defeito, uma comunicação à distância é inibida (como será descrito em detalhe mais abaixo).

No momento da etapa de personalização, pode também fornecer-se a escrita de uma informação de configuração que indica (por exemplo na forma de direitos de acesso ao arquivo onde está memorizado o bit de ativação) até que ponto a utilização dos meios de comunicação à distância da entidade eletrónica poderá ser autorizada via a ligação por contacto, ou seja por exemplo:

- sempre, por exemplo deixando livre acesso ao arquivo que contém o bit de ativação (o programa de comando da entidade eletrónica que no entanto pode neste caso condicionar a emissão de introdução de um código secreto como descrito mais abaixo);
- depois uma autentificação do leitor (ou do titular do cartão que introduz eventualmente um código no leitor), o que constitui uma variante na forma de realização descrita mais adiante para somente autorizar a utilização dos meios de comunicação à distância aos utilizadores autentificados;
- nunca, por exemplo proibindo o acesso ao arquivo que contém o bit de ativação, o que torna impossível a modificação deste para autorizar eventualmente a utilização dos meios de comunicação sem contacto.

Coloca-se depois se o acesso ao bit de ativação está livre vis a vis do programa de controlo da entidade eletrónica.

A um certo ponto de funcionamento de modo "*contactos*" (em que o microcircuito 12 é alimentado pelo terminal e troca dados com este mediante contactos 14), o microcircuito pode receber do terminal uma instrução de ativação da comunicação sem contacto, isto é um dado (ou de modo mais geral uma informação) que visa comandar a autorização de um funcionamento de modo "*sem contacto*" através da antena 16, como explicado em referência à figura 6 (etapa E20).

No exemplo descrito aqui, um código fornecido pelo utilizador (por exemplo mediante um teclado) para o terminal é transmitido em associação com a instrução de ativação de modo que a autorização do funcionamento de modo "*sem contacto*" só seja efetiva na presença do bom código fornecido pelo utilizador, quer dizer um código predeterminado e armazenado (eventualmente de forma protegida) na memória regravável 18 associada ao microcircuito 12 (ou numa outra memória, do tipo memória morta, associada a esse microcircuito 12).

Depois de ter recebido a instrução de ativação acompanhada do código fornecido pelo utilizador, o microcircuito 12 procede a uma etapa E22 para verificação da exatidão do código fornecido, isto é na prática comparação do código fornecido com o código memorizado na entidade eletrónica como já mencionado.

Se o código fornecido corresponde de maneira correta ao código secreto memorizado na entidade eletrónica, a autorização de uma comunicação sem contacto torna-se efetiva pela colocação a 1 na etapa E24 do bit de ativação precedentemente mencionado, o que significa que a entidade eletrónica recebeu efetivamente uma informação de ativação da comunicação correta sem contacto.

Pelo contrário, se o código fornecido pelo utilizador é transmitido à entidade eletrónica com a instrução de ativação na etapa E20 não é o código memorizado por esta, procede-se na etapa E 26 à colocação a 0 do bit de ativação na memória regravável 18, o que significa que se considera então que nenhuma informação de ativação correta tenha sido recebida.

Nos dois casos, o bit de ativação é por exemplo modificado por uma instrução do tipo "*UPDATE BINARY*" (definida pela norma ISO7816-4) depois da seleção do arquivo que contém esse bit de ativação por um comando do tipo "*SELECT*".

Pode notar-se que, no caso precedentemente mencionado onde o bit de ativação é posto a 0 no momento de uma etapa de inicialização, a etapa E26 não é necessária visto que não muda *a priori* o valor do bit de ativação. Pode desejar-se no entanto utilizá-la, por exemplo para garantir que qualquer utilização de um código incorreto conduza à colocação a 0 do bit de ativação mesmo se o código correto foi sujeito a uma fase precedente. Por outro lado, na presença ou não da etapa E26, a receção de um código incorreto poderia levar a outras consequências, como por exemplo a emissão de uma mensagem de erro do cartão para destino do terminal via os contactos 14.

Além disso, embora numa finalidade de concisão se tenha descrito uma única etapa de verificação da exatidão do código sem determinar se era possível repetir ou não essa etapa, pode evidentemente considerar-se a possibilidade de deixar ao utilizador um número limitado de tentativas de introdução do código secreto, com a consequência por exemplo do bloqueio da entidade eletrónica

quando o número limitado de tentativas é esgotado e o código sempre errado.

O modo de funcionamento "*sem contacto*" será presentemente descrito em referência à figura 6. Como indicado depois, esse modo de funcionamento é desencadeado pela entrada da entidade eletrónica no alcance de um leitor à distância, que tenha sido realizado ou não anteriormente nas etapas da figura 5 visando ativar a ligação sem contacto.

No momento da entrada da entidade eletrónica no campo do leitor (etapa E30), a entidade eletrónica é telealimentada (o que pode ser visto como uma deteção do leitor pela entidade eletrónica) e o microcircuito 12 inicia o seu funcionamento de modo "*sem contacto*".

No início deste funcionamento (de preferência no momento das primeiras etapas do programa executado pelo microcircuito 13, por exemplo durante a aplicação dos programas de inicialização e de anticolisão como definidos na norma ISO14443-3), o microcircuito 12 procede à leitura na memória regravável 18 do bit de ativação (etapa E32).

Pode então proceder-se na etapa E34 a uma verificação do valor do bit (que, como já mencionado, é indicativo de uma informação de ativação da comunicação sem contacto).

Se o bit de ativação está a 0 (ou porque esse valor foi registado no momento da inicialização da entidade eletrónica e não foi modificado pela receção de uma instrução de ativação correta, ou porque esse bit foi reposto a 0 depois da introdução de um código errado ou na realização prévia de uma troca de dados autorizada sem que uma nova autorização tenha sido fornecida), termina a etapa

E36 para a comunicação sem contacto, cujas únicas primeiras etapas terão assim sido realizadas sem que isso implique uma troca de dados.

Pelo contrário, se se verificou pelo micro circuito 12 que o bit de ativação armazenado na memória regravável 18 é de valor 1 (isto é que se está na presença de uma informação de ativação), procede-se à procura da aplicação da comunicação sem contacto ou seja em primeiro lugar a uma inicialização do protocolo de ligação para a etapa E38 (por exemplo de acordo com a norma ISO14443-4 para chegar ao nível da execução do protocolo "*Half-Duplex Block Transmission Protocol*".

Uma vez estabelecida a comunicação sem contacto (por exemplo depois da etapa E38), procede-se à colocação a 0 do bit de ativação na memória regravável 18, como representado pela etapa E40 na figura 6. A aplicação da etapa E40 depois da inicialização do protocolo permite garantir que a entidade eletrónica não será autorizada a estabelecer uma nova comunicação sem contacto depois de ter saído do campo do leitor (exceto para receber uma nova instrução de ativação mediante a ligação por contacto.

No entanto, como já evocado, a colocação a 0 do bit de ativação (isto é a inibição do estabelecimento de uma nova comunicação sem contacto) poderia intervir noutras condições, tais como por exemplo uma temporização em relação ao momento da receção da instrução de ativação (ou eventualmente em relação ao estabelecimento da ligação sem contacto), a execução de um número predeterminado de instruções pelo microcircuito 12 (ou de comandos APDU "*Application Protocol Data Unit*") ou a receção de uma mensagem de fim de transação (como era o caso na primeira forma de realização)

De acordo com uma outra variante, pode considerar-se que o bit de ativação não seja reposto a 0 no momento do funcionamento de modo sem contacto, mas antes na receção de uma instrução de desativação de modo "contactos". Uma tal instrução de desativação poderia por outro lado ser fornecida mesmo se o bit de ativação fosse reposto a 0 no momento do funcionamento sem contacto (como por exemplo descrito na figura 6).

No exemplo descrito, uma vez o protocolo inicializado na etapa E38 e embora o bit de ativação seja reposto a 0 na etapa E40, procede-se em seguida a uma troca de dados de acordo com o protocolo sem contacto com uma etapa E42. Deverá notar-se todavia que, quando a troca de dados da etapa E42 terminar, por exemplo pela saída da entidade eletrónica do campo do leitor, ou em alternativa à receção deste de um comando que põe fim à comunicação tendo o bit de ativação sido reposto a 0 pela etapa E40, uma nova iteração das etapas de E30 a E40 pelo retorno da entidade eletrónica no campo do leitor conduzirá a uma falha da comunicação sem contacto pela passagem para a etapa E36.

Na forma de realização que acaba de ser descrita, o bit de ativação (usado como indicador da receção prévia de uma instrução de ativação correta) condiciona o conjunto das trocas de dados de modo sem contacto. Em alternativa, poderia prever-se que esse bit de ativação só condiciona a troca de alguns dados particulares da entidade eletrónica, enquanto outros dados poderiam livremente ser comunicados pela entidade eletrónica durante a sua passagem perto de um leitor à distância, mesmo se nenhuma instrução específica foi recebida primeiramente pela ligação por contacto.

Assim, quando a entidade eletrónica é um documento de identificação eletrónica, pode prever-se que alguns dados

presentes no documento (como o nome da pessoa em causa) sejam comunicados sem primeiro necessitarem da ativação de uma autorização particular, enquanto a emissão de outros dados (por exemplo as informações confidenciais de tipos de dados biométricos - impressões digitais, íris ou imagem facial) só poderão ser emitidas pela entidade eletrónica via a ligação sem contacto desde que a entidade eletrónica tenha recebido primeiramente uma instrução válida de ativação nesse sentido mediante a ligação por contacto.

Nesse caso, a presença de uma informação de ativação (isto é o valor 1 do bit de ativação) não condicionará o estabelecimento da ligação sem contacto estritamente falando, mas algumas etapas de emissão dos dados confidenciais.

Pode então prever-se por exemplo que a instrução de ativação apenas corresponde à autorização para emitir uma única vez esses dados, quer dizer que o bit de ativação será então reposto a 0 imediatamente depois da emissão dos dados confidenciais.

De acordo com uma variante, pode prever-se que a informação de ativação condiciona a receção de dados via a ligação sem contacto. Pode assim evitar-se por exemplo que um código de identificação seja apresentado na entidade eletrónica via a ligação sem contacto por um terceiro mal-intencionado, sem o conhecimento do titular autorizado da entidade eletrónica, com risco por exemplo de bloquear a entidade eletrónica após a apresentação de vários códigos falsos por esse terceiro.

Por outro lado, os dados conferidos pela autorização de troca não estão necessariamente limitados aos dados aplicativos da entidade eletrónica (isto é especialmente os

dados levados pela entidade eletrónica na sua função de suporte de informação), mas podem também incluir dados de outros tipos, como dados que permitem o estabelecimento de um protocolo de comunicação.

As formas de realização que acabam de ser dadas, com as variantes consideradas, só constituem exemplos possíveis de aplicação da invenção sem limitação.

Lisboa, 28 de Fevereiro de 2014

REIVINDICAÇÕES

1. Entidade eletrónica que compreende:

   - meios de comunicação por contacto (4; 14);
   - meios de comunicação sem contacto (6; 16);
   - uma memória não volátil regravável apta para memorizar uma informação;

   caracterizada por:

   - meios de definição para um valor predeterminado da informação de ativação na receção de uma instrução através dos meios de comunicação por contacto;
   - meios (12) para autorizarem uma troca de alguns dados pelo menos através dos meios de comunicação sem contacto somente na presença do valor predeterminado da referida informação de ativação:

2. Entidade eletrónica de acordo com a reivindicação 1, **caracterizada por** meios para inibirem a troca dos referidos dados através dos meios de comunicação sem contacto na ausência do valor predeterminado da referida informação de ativação.

3. Entidade eletrónica de acordo com a reivindicação 1 ou 2, **caracterizada por** ser um cartão microcircuito.

4. Processo de comando de uma entidade eletrónica que compreende meios de comunicação por contacto e meios de comunicação sem contacto, **caracterizado por** uma memória não volátil regravável apta para memorizar uma informação de ativação e pelas etapas seguintes:

- receção de uma instrução de ativação (E20) através dos meios de comunicação por contacto;
- aplicação de uma autorização de troca (E24) de alguns dados pelo menos através dos meios de comunicação sem contacto, pela definição de um valor predeterminado (E24) da referida informação de ativação, na receção da referida instrução de ativação;
- verificação (E34) de que o valor da informação de ativação é igual ao valor predeterminado;
- troca dos referidos dados (E38, E42) através dos meios de comunicação sem contacto somente no caso de verificação da igualdade.

5. Processo de a acordo com a reivindicação 4, **caracterizado por** uma etapa de colocação da informação de ativação para um valor complementar (E40) do valor predeterminado num instante definido.

6. Processo de acordo com a reivindicação 5, **caracterizado por** o instante definido corresponder à receção de um comando de fim de comunicação (E14) pelos meios de comunicação sem contacto.

7. Processo de acordo com a reivindicação 5, **caracterizado por** o instante definido ser determinado por uma temporização.

8. Processo de acordo com a reivindicação 5, **caracterizado por** o instante definido ser alcançado após receção de um número predeterminado de comandos via os meios de comunicação sem contacto.

9. Processo de acordo com a reivindicação 5, **caracterizado por** o instante definido corresponder à conclusão de uma etapa de inicialização (E38) da comunicação.

10. Processo de acordo com uma das reivindicações de 4 a 9, caracterizada por um código ser transmitido através dos meios de comunicação por contacto e por a referida autorização de troca ser efetiva se o código transmitido corresponde a um código memorizado na entidade eletrónica.

11. Processo de acordo com a reivindicação 10, caracterizado por a instrução de ativação ser recebida juntamente com o código transmitido.

Lisboa, 27 de Fevereiro de 2014

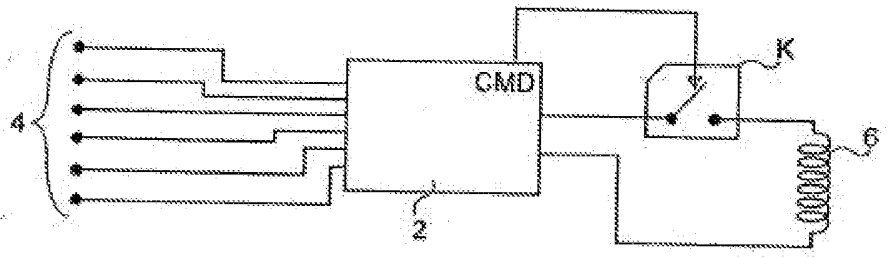

Fig. 1

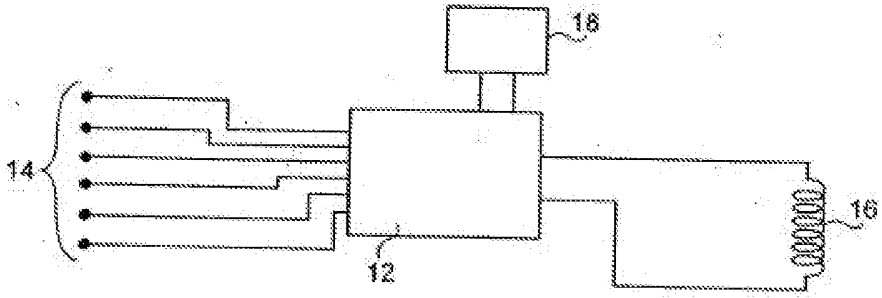

Fig. 3

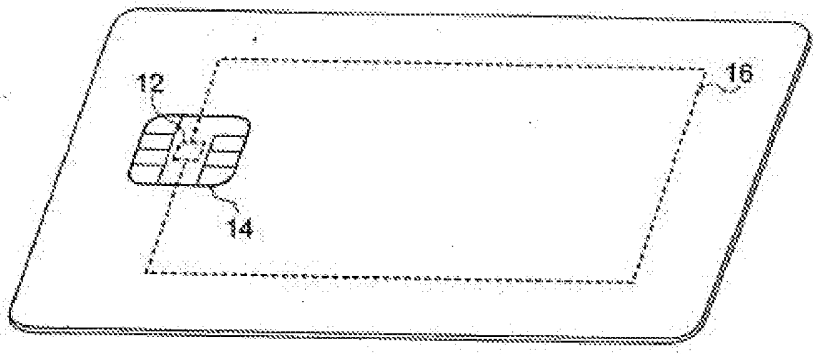

Fig. 4

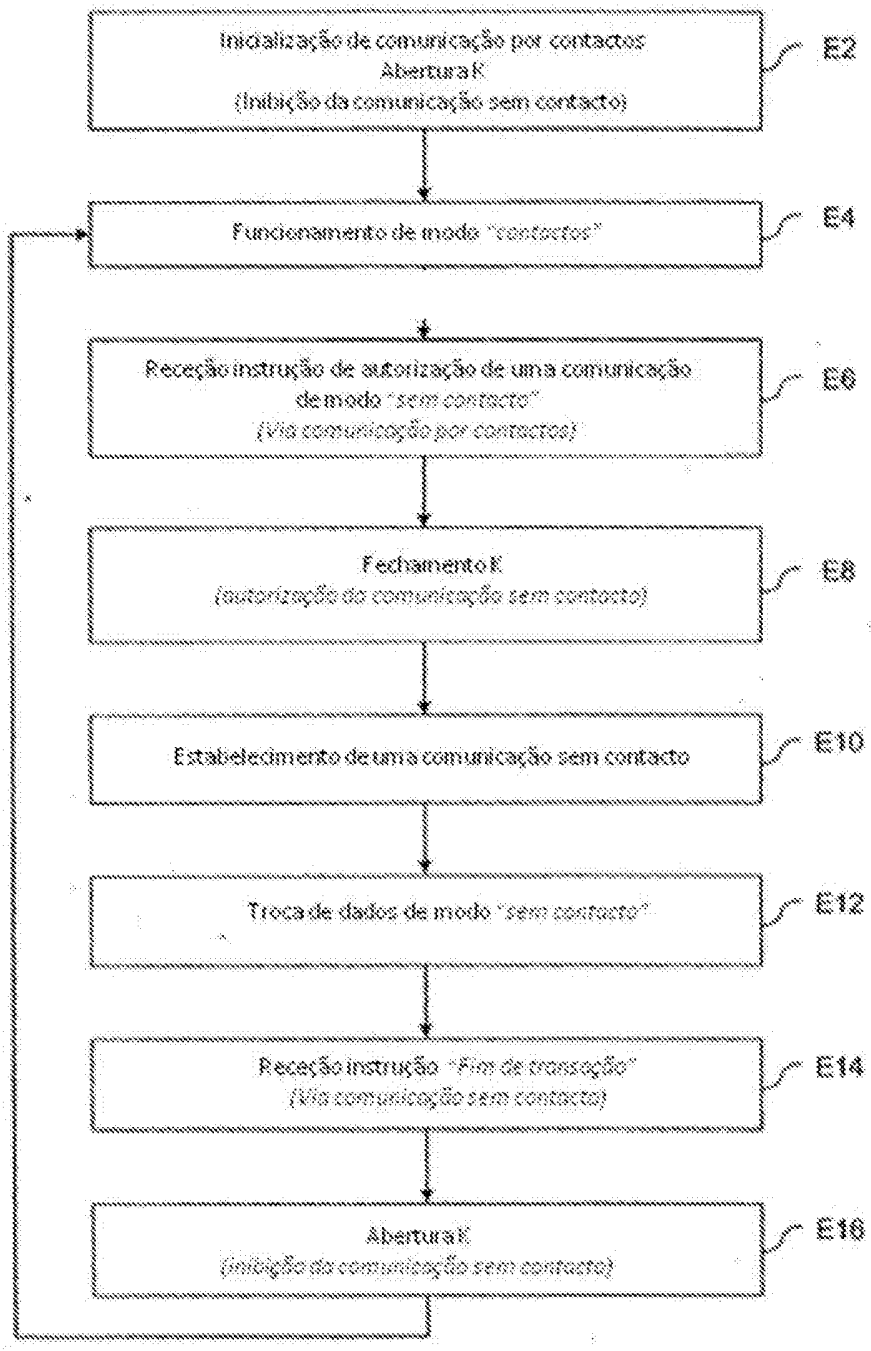
Inicialização de comunicação por contactos
Abertura IC
(Inibição da comunicação sem contacto)
E2
Funcionamento de modo "contactos"
E4
Receção instrução de autorização de uma comunicação de modo "sem contacto"
(Via comunicação por contactos)
E6
Fechamento IC
(autorização da comunicação sem contacto)
E8
Estabelecimento de uma comunicação sem contacto
E10
Troca de dados de modo "sem contacto"
E12
Receção instrução "Fim de transação"
(Via comunicação sem contacto)
E14
Abertura IC
(inibição da comunicação sem contacto)
E16

Fig.2

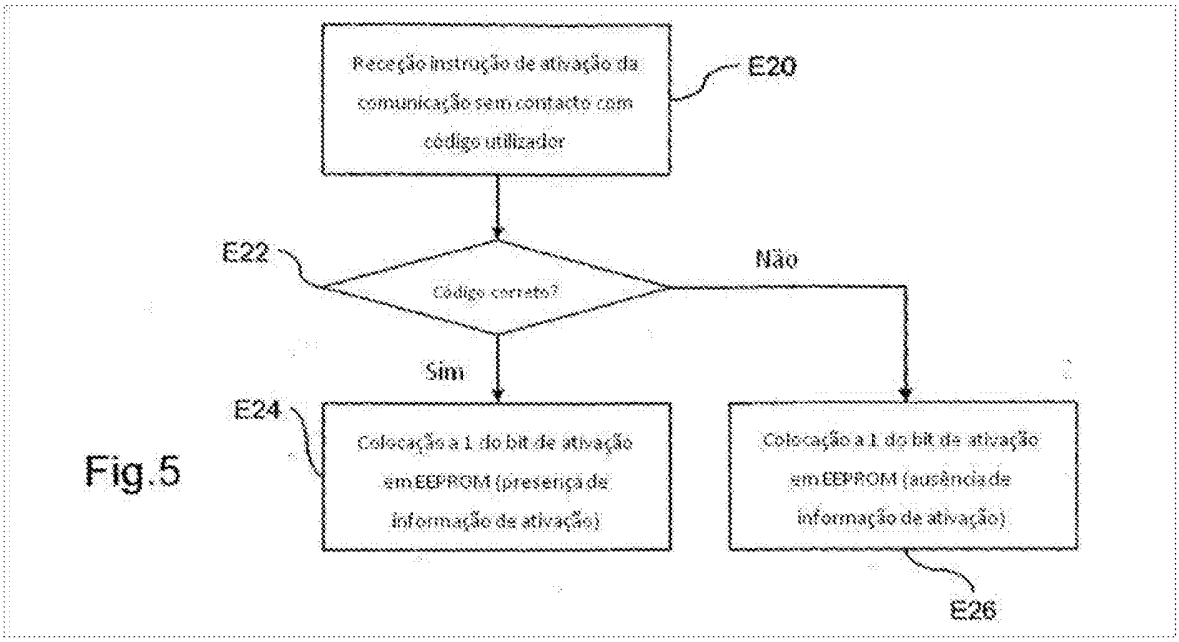
Receção instrução de ativação da comunicação sem contacto com código utilizador
E20
E22
Código correto?
Não
Sim
E24
Colocação a 1 do bit de ativação em EEPROM (presença de informação de ativação)
Colocação a 1 do bit de ativação em EEPROM (ausência de informação de ativação)
E26

Fig.5

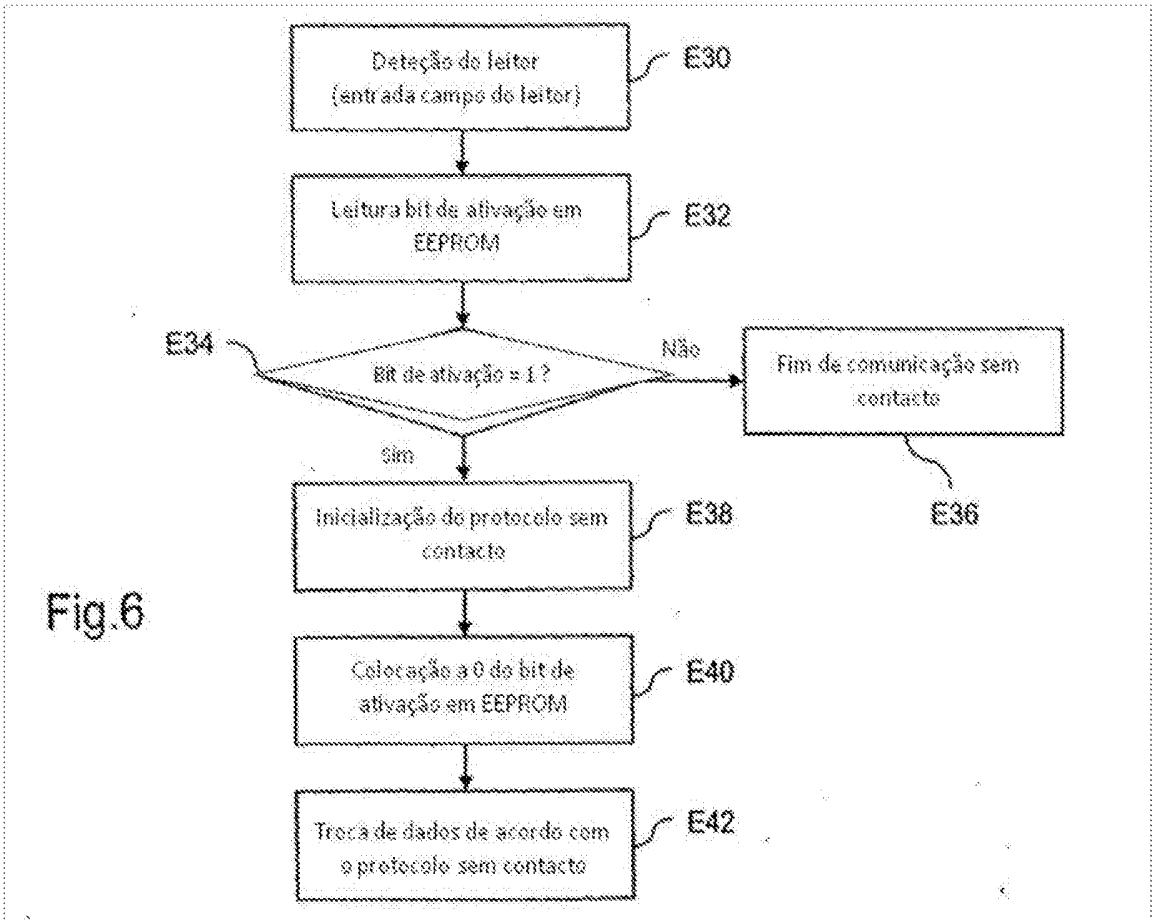
Deteção do leitor (entrada campo do leitor)
E30
Leitura bit de ativação em EEPROM
E32
E34
Bit de ativação = 1 ?
Não
Fim de comunicação sem contacto
E36
Sim
Inicialização do protocolo sem contacto
E38
Colocação a 0 do bit de ativação em EEPROM
E40
Troca de dados de acordo com o protocolo sem contacto
E42

Fig.6