



República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0914159-6 B1



(22) Data do Depósito: 21/06/2009

(45) Data de Concessão: 26/01/2021

(54) Título: CARTÃO SEM CONTATO COM LOGO DE SEGURANÇA

(51) Int.Cl.: G06K 19/077.

(30) Prioridade Unionista: 20/06/2008 FR 08/03472.

(73) Titular(es): SMART PACKAGING SOLUTIONS (SPS).

(72) Inventor(es): OLIVIER ARTIGUE; STÉPHANE SEMORI; DEBORAH TEBOUL; CÉCILE SICOT.

(86) Pedido PCT: PCT FR2009000747 de 21/06/2009

(87) Publicação PCT: WO 2009/153464 de 23/12/2009

(85) Data do Início da Fase Nacional: 20/12/2010

(57) Resumo: CARTÃO SEM CONTATO COM LOGO DE SEGURANÇA. A invenção se refere a cartão inteligente sem contato (1) que compreende um corpo de cartão (7) e um módulo eletrônico (3) fornecido com um chip eletrônico (9) ligado aos terminais de uma antena (11), o módulo eletrônico (3) sendo disposto em um recesso (5) formado no corpo de cartão, caracterizado pelo fato de que a superfície exposta (19) do módulo eletrônico (3) compreende pelo menos um elemento de segurança impresso (21) capaz de proteger o referido módulo eletrônico e o cartão sem contato contra tentativa de fraude.

Relatório Descritivo da Patente de Invenção para: **"CARTÃO SEM CONTATO COM LOGO DE SEGURANÇA"**.

[0001] A invenção refere-se a cartões inteligentes sem contato, mais particularmente, os cartões de identificação ou passaportes eletrônicos incluindo um logotipo de segurança.

[0002] A presente invenção não depende do tamanho do cartão de chip e pode ser aplicada a cartões de chip convencionais, bem como a outros documentos seguros fornecidos com um módulo eletrônico do cartão sem contato, de modo que, a fim de simplificar a descrição, a mesma palavra "cartão inteligente sem contato" irá referir-se a cartões de chip no formato convencional (de acordo com a norma ISO 7816-1), bem como aos documentos de segurança tendo um outro formato, mas também ser fornecido com um módulo eletrônico do mesmo tipo que aqueles normalmente usados em cartões inteligentes sem contato.

Estado da Técnica

[0003] Vários tipos de cartões ou documentos de segurança incluindo um chip eletrônico já são conhecidos no estado da técnica.

[0004] Em seguida, os cartões de identificação, no formato de um cartão com chip de contato são conhecidos, em que o módulo eletrônico está "incorporado", isto é, fixado

em um recesso do corpo do cartão, de modo que os contatos elétricos do módulo de permanecem acessíveis na superfície para permitir a conexão com um leitor de cartão de contato. Este tipo de cartão de identificação levanta o problema de um eventual acesso aos contatos, ou mesmo da pura e simples substituição do módulo eletrônico para fins de fraude de identidade.

[0005] É claro, seria aconselhável fornecer os cartões com chip de identificação de contato com um impresso de segurança que cubra a face superior do cartão e tornando possível detectar casos de fraude, mas tal impresso de segurança não pode ser facilmente fornecido na área do módulo eletrônico uma vez que a condutividade do contato pode ser afetada.

[0006] A fim de resolver parcialmente este problema, documento DE-196 25 466 C1 descreve um cartão com chip de contato, os contatos do qual também são fornecidos com um impresso, mais particularmente tendo uma cor específica diferente da cor dourada ou prateada habitual. Para este fim, os contatos são revestidos com uma camada de dispersão contendo partículas metálica coloridas à base de alumínio. No entanto, os contatos permanecem acessíveis eletronicamente, o que permite atos de fraude através do ataque do circuito de chip nos contatos do cartão com chip.

Além disso, os contatos e o módulo também permanecem fisicamente acessíveis, o que faz com que seja possível considerar a remoção ou mesmo substituição do módulo eletrônico.

[0007] Um cartão de chip de contato também é conhecido do documento de Pat dos EUA No. 6.259.035 B1, em que o módulo eletrônico e os contatos metálicos são feitos tão discretos quanto possível, conforme o seu aspecto, colorindo-se os contatos, e o impresso na superfície do módulo é uma extensão do impresso do corpo atual. Naturalmente, este método é reservado a cartões de contato e não pode ser aplicado a cartões sem contato, tais como os utilizados para a produção de cartões de identificação sem contato.

[0008] Uma abordagem inversa é descrita no documento de patente dos EUA No. 5.552.574, que descreve, pelo contrário, como a superfície dos contatos de um cartão com chip de contato pode ser fornecida com uma gravação de segurança executada com um feixe de laser.

[0009] Os resultados dos exemplos acima mencionados, é que o problema das gravações de segurança foi resolvido para cartões de contato, quer por guilhocês ou outros impressos executados no corpo do cartão ou pela alteração gráfica dos contatos metálicos do módulo, sob a forma de

cores ou gravação a laser executados diretamente nos contatos.

[0010] A utilização de cartões inteligentes sem contato, em aplicações de segurança ou de identificação também são conhecidas e tais cartões tendem a se dissipar em tais aplicações, tendo em vista que pode ser usado mais facilmente.

[0011] Em cartões sem contato, a eletrônica incluindo um chip conectado a uma antena é fornecido mais frequentemente separadamente sob a forma de uma inserção que é então laminada entre camadas de proteção externas. Eletrônica é então protegida contra um acesso direto pelo contato, mas separando as várias camadas e substituição de forma fraudulenta da inserção ou mesmo recuperá-lo, a fim de produzir um cartão de identificação fraudulento sem contato, no entanto, continua sendo possível.

[0012] Outra desvantagem de cartões sem contato produzidos a partir de uma inserção interposta entre as camadas de proteção externa reside no método de produção dos mesmos. De fato, a inserção é a parte mais custosa do cartão e pode ser danificada durante a laminação com as camadas externas, o que faz com que o rendimento da produção deste tipo de cartões reduza e o preço unitário aumente.

[0013] Neste caso, seria mais aconselhável a utilização de métodos de produção mais confiáveis com um rendimento mais elevado, tais como o método convencional para a incorporação de cartões de contato, que consiste em posicionar um módulo de contato em um recesso da placa. Mas, como visto anteriormente, o método como tal, não é muito seguro, uma vez que os cartões assim produzidos estão particularmente expostos à fraude que consiste em arrancar o módulo de cartão, que particularmente não é recomendado para cartões ou documentos destinados a aplicações de verificação de identidade.

[0014] Além disso, alguns cartões são produzidos com uma tecnologia de interface de comunicação dupla, e incluem tanto a eletrônica sem contato embutida no corpo do cartão e ainda dotados de contatos para a comunicação com um leitor de cartão de contato. Este tipo de cartão potencialmente acumula as falhas de segurança de ambos os tipos de cartões descritos acima.

Objetivos da Invenção

[0015] Deste modo, um objetivo da presente invenção é fornecer uma estrutura de cartão sem contato capaz de resolver os inconvenientes acima mencionados dos cartões de identificação de chip ou documentos de identificação.

[0016] Mais particularmente, um objetivo da presente invenção é fornecer um cartão inteligente sem contato destinado a aplicações do tipo de verificação de identificação que podem ser facilmente produzidos com elevados rendimentos comparáveis com os rendimentos de produção de cartões de contato, ao serem compatíveis com os impressos de segurança tais como logotipos ou hologramas de segurança.

[0017] Outro objetivo da invenção é fornecer um cartão de chip com uma confiabilidade muito elevada e uma vida útil muito longa, da ordem de cinco a dez anos, permitindo simultaneamente um elevado rendimento de produção e um custo baixo, como cartões simples operados por contato.

[0018] Para este efeito, o objeto da presente invenção é um cartão inteligente sem contato que compreende um corpo de cartão e um módulo eletrônico operado sem contato fornecido com um chip eletrônico ligado aos terminais de uma antena, o módulo sendo disposto em um recesso formado no corpo do cartão, caracterizado pelo fato de que a parte exposta do módulo inclui um elemento de segurança impresso capaz de proteger o módulo eletrônico e o cartão sem contato contra as tentativas de fraude.

[0019] De acordo com uma concretização básica muito simples, o elemento de segurança impresso é simplesmente

constituído por um padrão impresso fornecido na superfície exposta do módulo eletrônico sem contato.

[0020] Este padrão impresso é composto de áreas com uma espessura extra e áreas em depressão com relação à superfície do módulo e/ ou áreas que têm uma cor diferente do resto da superfície do módulo eletrônico. Este padrão impresso pode ser obtido de maneira diferente, mais particularmente por meio de serigrafia ou gravação química, como para a produção de contatos metálicos fornecidos de uma maneira conhecida para os módulos para cartões de contato.

[0021] Numa concretização alternativa mais elaborada da invenção, tendo uma maior segurança e resistência em relação a ataques físicos contra o módulo, o elemento de segurança impresso é coberto por, pelo menos, uma camada de proteção transparente, mais particularmente, feita de policarbonato, colocada acima o corpo do cartão, de modo a revestir a face exposta do módulo eletrônico sem contato e o padrão de segurança impresso do mesmo.

[0022] A fim de ainda aumentar a segurança do produto e a resistência do mesmo à fraude e à violação, a camada de proteção transparente ou translúcida inclui, em uma das faces da mesma ou na espessura da mesma, um segundo elemento de segurança impresso que é complementar ao elemento de segurança impresso da superfície de módulo eletrônico, de

modo a formar com elas um elemento de segurança composto por meio da sobreposição de ambos os elementos de segurança separados.

[0023] Em seguida, a invenção prevê que ambos os elementos de segurança impressos podem ser duas partes distintas e complementares de uma imagem ou um logotipo, de modo que a sobreposição exata de ambos os elementos de segurança impressos só torna possível recriar a imagem ou logotipo completo.

[0024] Assim, a eliminação da camada de proteção superior iria suprimir claramente o segundo elemento de segurança impresso, que seria imediatamente visível, uma vez que o logotipo ou o equivalente já não estaria completo.

[0025] Numa solução alternativa interessante de uma tal concretização, o segundo elemento impresso é composto de um holograma com um padrão complementar ao impresso de segurança sobre a superfície do módulo eletrônico, de modo que a sobreposição do impresso de segurança e do holograma mostra um logotipo de segurança à prova de falsificação.

[0026] Vantajosamente, a superfície do holograma, ou de forma mais geral, pelo menos, um dos elementos impressos, é maior do que a superfície exposta do módulo e é unido à superfície do módulo, de modo que uma recuperação fraudulenta de um dos elementos impressos é mais facilmente visível.

[0027] A fim de ainda aumentar a resistência ou o realce de ataques físicos contra o cartão inteligente sem contato, a camada de proteção transparente é estendida além da superfície superior da placa e é fornecida como uma camada de material de encapsulamento que envolve o conjunto de corpo de cartão sobre toda a superfície da mesma.

[0028] É claro que, a técnica de holograma não está reservada para a camada de proteção transparente ou a camada de encapsulamento, mas o elemento de segurança impresso da superfície do módulo eletrônico pode também ou, independentemente, ser composto por um holograma que mostra um padrão de segurança e posicionado acima da face exposta do módulo, de modo que o acesso aos módulos requer a destruição do holograma.

[0029] As soluções alternativas acima mencionadas podem ser fornecidas independentemente da estrutura comunicação sem contato do cartão, isto é, por exemplo, a antena de comunicação pode ser posicionada diretamente sobre o módulo eletrônico ou no corpo do cartão e também pode ser complementada por uma segunda antena utilizada como um amplificador de fluxo eletromagnético com relação à primeira antena.

[0030] Em seguida, em uma primeira solução alternativa, o corpo do cartão inclui várias camadas de

material, material plástico ou mesmo de papel, e a antena é fornecida entre duas camadas adjacentes do corpo do cartão e inclui almofadas de contato dispostas na parte inferior do recesso do corpo do cartão e ligadas a terminais de ligação do módulo eletrônico.

[0031] De acordo com uma outra solução alternativa, a antena é fornecida no próprio módulo eletrônico e está ligada ao chip eletrônico do mesmo, de modo que o módulo revestido com o elemento de segurança impresso do mesmo pode simplesmente ser reportado e fixo dentro do recesso da placa de corpo.

[0032] Mas, o cartão pode ainda incluir uma segunda antena fornecida no corpo do cartão e posicionada no lado oposto do módulo de antena, de modo a amplificar o fluxo eletromagnético detectado pela antena do módulo.

[0033] Outro objetivo da invenção é também proporcionar um módulo eletrônico operado sem contato adaptado para ser montado em um cartão inteligente sem contato e fornecido com meio de segurança impresso disposto na superfície exposta do mesmo, de modo a permanecer visível após a incorporação do módulo no corpo do cartão, tal meio de segurança impresso sendo, mais particularmente, obtido por diferenças no nível, as diferenças nas cores da face exposta e/ ou da inserção de um holograma.

[0034] Naturalmente, a invenção estende-se a cada cartão com chip, incluindo um corpo do cartão e um módulo inovador tal como descrito acima.

[0035] Outras características e vantagens da invenção aparecerão com a leitura da descrição detalhada e os desenhos em anexo em que:

[0036] A figura 1 mostra uma vista em perspectiva em corte transversal de um cartão inteligente sem contato fornecido com um módulo eletrônico, a superfície exposta dos quais inclui um elemento de segurança de acordo com a ilustração da invenção;

[0037] A figura 2 mostra uma vista semelhante à da figura 1, mas em que o cartão com chip inclui uma grande antena integrada no corpo do cartão e conectado aos contatos elétricos do módulo eletrônico;

[0038] A figura 3 mostra uma vista semelhante à da figura 2, em que a segunda antena não está ligada ao chip do módulo eletrônico;

[0039] A figura 4 mostra uma vista semelhante às das figuras 1 a 3, em que o elemento de segurança impresso do módulo eletrônico superfície é revestido com uma camada de proteção transparente;

[0040] A figura 5 ilustra os elementos de um módulo eletrônico capaz de criar uma imagem de segurança por meio da sobreposição de camadas;

[0041] A figura 6 mostra uma perspectiva e em corte transversal de uma sobreposição de camadas de acordo com a figura 5c, em que a camada de proteção transparente inclui um segundo elemento de segurança impresso complementar àquele da superfície do módulo eletrônico;

[0042] A figura 7 mostra uma vista semelhante às das figuras 1 a 3, em que uma camada de encapsulamento transparente cobre todo o cartão com chip;

[0043] A figura 8 mostra uma vista semelhante à da figura 6, em que a camada de encapsulamento transparente cobre todo o cartão de chip.

[0044] Faz-se referência à figura 1. Uma área do cartão inteligente sem contato 1 é mostrada em perspectiva e em corte transversal, próxima do módulo eletrônico 3 do cartão de chip, sendo entendido que a área mostrada também pode corresponder a uma parte de um documento seguro com um formato diferente de um cartão com chip, tal como por exemplo um cartão de identificação ou um passaporte eletrônico e incluindo um módulo eletrônico operando sem contato.

[0045] O módulo eletrônico 3 está conscientemente montado num recesso 5 do corpo de cartão 7. Um chip 9 fixado

na face do módulo oposta à face visível do mesmo é mostrado esquematicamente. O chip 9 está eletricamente ligado aos terminais de uma antena 11 fornecida no módulo e destina-se a proporcionar uma comunicação sem contato com um leitor externo, não mostrado. O módulo eletrônico 3 está fixo no recesso 5, usando um adesivo 13. O cartão eletrônico 9 é protegido por uma gota de resina de encapsulamento 15. Durante a montagem do cartão com chip, o módulo é relatado em frente ao recesso 5 disposto no corpo do cartão. O módulo é fixo no recesso, como mostrado na figura 1, com os enrolamentos da antena 11 contatando o adesivo 13. Em seguida, uma etapa de pressionamento sobre a face superior do módulo seguinte para proporcionar uma colagem de alta qualidade do módulo no recesso.

[0046] O chip 9 e os enrolamentos da antena 11 são fixados numa camada de suporte 17 feita de material dielétrico, que é por sua vez coberta pela face visível 19 do módulo eletrônico 3, quando este último é posicionado no recesso 5 do corpo do cartão.

[0047] De acordo com a invenção, tal camada exposta 19, a superfície de que é nivelada com a superfície do corpo do cartão, inclui um elemento ou vários dos elementos de segurança impresso 21 capaz de proteger o módulo eletrônico e o cartão sem contato contra tentativas de fraude. Para

este efeito, esta camada exposta 19, a qual é, mais particularmente, feita de metal, como os contatos bem conhecidas dos cartões inteligentes sem contato inclui padrões impressos fornecidos através de várias técnicas conhecidas per se, tais como gravação ou impressão, e capaz de identificar o cartão de chip de identificação ou o suporte do mesmo, e em qualquer caso em fazer uma cópia fraudulenta do cartão de identificação mais difícil.

[0048] Em seguida, ao passo que no caso de cartões de contato da superfície do módulo inclui contatos elétricos tendo forma e tamanho mais ou menos uniforme e normalizada, a placa de contato de acordo com a invenção inclui elementos impressos fornecidos com tecnologias semelhantes conhecidas per se, mas com forma e função diferente, ou seja, a marcação de módulos de cartão sem contato de segurança. Deve-se notar que uma tal marcação não é necessária para proporcionar a função de comunicação do cartão com chip com um leitor externo, mas proporciona, graças à cópia difícil do mesmo, uma nova função de segurança na sua aplicação a um cartão sem contato.

[0049] Naturalmente, o tamanho e a forma dos elementos de segurança impresso 21 podem ser de qualquer tipo, bem como a concretização da mesma, na medida em que cumpram a finalidade de segurança requerida.

[0050] Na medida em que os elementos de segurança impressos 21 não interferem na função de comunicação sem contato do cartão de chip, tal estrutura de comunicação pode ter várias concretizações.

[0051] Em seguida, uma concretização alternativa é mostrada na figura 2, em que, a fim de aumentar o alcance de comunicação do cartão inteligente sem contato, uma antena 23 maior do que a antena 11 na figura 1 foi fornecida entre as camadas do corpo do cartão 7 em vez da antena 11 do módulo, e uma tal antena 23 que é ligada aos terminais apropriados do chip eletrônico através de almofadas de ligação 25.

[0052] Uma outra concretização alternativa é mostrada na figura 3, em que a segunda antena 27 é eletricamente isolada a partir da antena 11 do módulo por meio de uma camada isolante 27. Em seguida, a antena 23 é susceptível de entrar em ressonância com a antena 11 do módulo e é então utilizada como um amplificador com relação eletromagnético aos sinais que devem ser trocados entre o chip eletrônico 9 e um leitor externo sem contato.

[0053] De acordo com uma alternativa muito mais interessante da invenção, esquematicamente mostrada na figura 4, a camada exposta 19 do módulo eletrônico inclui os primeiros elementos de segurança impressos 21, e tal camada exposta 19 é coberta por pelo menos uma camada de proteção

transparente ou translúcida 29, disposta por cima do corpo do cartão, de modo a revestir a face exposta 19 do módulo eletrônico e os primeiros elementos de segurança impressos 21 da mesma. Um material suficientemente resistente para evitar a sua separação do resto do cartão e tendo uma vida suficientemente longa para proporcionar a vida de serviço solicitado pelas aplicações do cartão de identificação, tipicamente de 5 a 10 anos, será escolhido para a camada de proteção 29. Uma possível escolha será a de proporcionar uma camada de proteção feita de policarbonato ou equivalente.

[0054] Tal como mostrado esquematicamente na figura 5b, a camada de proteção 29 inclui de preferência dois segundos elementos de segurança impressos 31, idealmente complementares aos primeiros elementos de segurança impresso 21 dispostos na face exposta 19 do módulo, de modo que a sobreposição dos mesmos forma uma imagem composta ou um logotipo de segurança completo 21, 31 obtido por meio da sobreposição das imagens do primeiro e segundo elementos de segurança impressos 21, 31.

[0055] Deste modo, ambos os elementos de segurança impressos 21, 31 são idealmente duas partes distintas da mesma imagem composta ou de um logotipo, de modo a que a sobreposição dos dois elementos de segurança impressos somente torna possível recriar a imagem completa ou logotipo.

Pelo contrário, a remoção ou a danificação da camada de proteção superior iria revelar imediatamente o fato de que o cartão inteligente sem contato foi modificado e não pode mais ser aceito pelas autoridades de gerenciamento de pedido de cartão.

[0056] É claro que, a fim de evitar danos acidentais dos segundos elementos de segurança impressos 31, estes últimos são preferencialmente fornecidos quer na face da camada 29 que está em contato estreito com a face externa da camada 19, ou na espessura da camada 29, como mostrado em perspectiva na figura 6.

[0057] Numa concretização alternativa vantajosa da invenção, os referidos primeiro e/ ou segundo elementos impressos 21, 31 são compostos de hologramas. Em seguida, o holograma mostra um padrão complementar para o impresso de segurança ou o holograma 21 da superfície do módulo eletrônico, de modo que a sobreposição do impresso de segurança e do holograma ou ambos os hologramas mostram um logotipo de segurança à prova de violação.

[0058] A superfície de pelo menos um dos elementos impressos 21, 31 é de preferência maior do que a superfície exposta 19 do módulo e é unida à superfície do módulo, de modo que uma recuperação fraudulenta de um dos elementos impressos 21, 31 é mais facilmente visível.

[0059] Como mostrado na figura 7, a camada de proteção transparente 19 fornecida com os elementos de segurança impressos 21 pode ir além da superfície do cartão com chip e pode ser fornecida como uma camada de um material de encapsulamento 33 em torno do conjunto do corpo da placa sobre a totalidade da superfície da mesma que faz com que qualquer separação das camadas do cartão com chip impossível, sem causar danos visíveis.

[0060] Naturalmente, uma tal camada de encapsulamento 33 pode também ser considerada no caso em que o cartão inclui uma camada de proteção adicional 29, provida com segundo meio de segurança impresso 31, como mostrado na figura 8.

Vantagens

[0061] A invenção alcança os objetivos pretendidos e fornece um módulo eletrônico sem contato e um cartão de chip, utilizando tal módulo, incluindo elementos de segurança impresso, tornando-se possível aumentar substancialmente a resistência aos ataques físicos de cartões sem contato e, mais particularmente, mas não exclusivamente, para aplicações de verificação de identidade do titular, como os cartões de identificação sem contato e os passaportes sem contato.

[0062] De fato, os elementos de segurança impressos 21 são proporcionados na superfície do módulo eletrônico e tal módulo torna-se particularmente simples de usar aos industriais que não são especializados em cartões sem contato. De fato, é suficiente informar o módulo sem contato já seguro no recesso de um corpo de cartão, utilizando métodos de incorporação extremamente convencionais e já conhecidos no campo dos cartões de contato, o que resulta num ganho significativo de taxas de produção, um significativo aumento do rendimento de produção e confiabilidade e, conseqüentemente uma redução no custo unitário.

[0063] Então, torna-se possível aplicar uma tal tecnologia de produção de módulos com um logotipo de segurança para obter cartões de chip destinados a aplicações extremamente rigorosas ou aplicações que têm uma vida útil muito longa, tais como, por exemplo, a aplicação para cartões de identificação ou passaportes eletrônicos para os quais organizações governamentais geralmente exigem comportamento e funcionamento corretos garantidos por dez anos.

REIVINDICAÇÕES

1. Cartão inteligente (1) sem contato, compreendendo um corpo de cartão (7) e um módulo eletrônico (3) com um microchip (9) ligado aos terminais de uma antena (11), o módulo eletrônico (3) sendo colocado em uma cavidade (5) disposta no corpo do cartão, sendo que a superfície aparente (19) do módulo eletrônico (3) inclui pelo menos um primeiro elemento gráfico de segurança (21) coberto por pelo menos uma camada protetora transparente (29) disposta acima do cartão, de modo a abranger e proteger a superfície exposta do módulo eletrônico, o referido elemento gráfico de segurança (21) consistindo em um padrão gráfico compreendendo zonas que são ressaltadas e zonas que são rebaixadas em relação à superfície do módulo eletrônico e/ou zonas de cor diferente do resto da superfície do módulo eletrônico, as ditas zonas ressaltadas e rebaixadas e/ou as zonas de cor diferente formando uma marca de segurança, do módulo eletrônico, capaz de proteger o referido módulo eletrônico e o cartão sem contato de tentativas de fraude por meio da extração do elemento gráfico de segurança (21), **caracterizado pelo** fato de que a dita camada protetora transparente (29) compreende pelo menos um segundo elemento gráfico de segurança (31), complementar ao dito primeiro elemento gráfico de segurança (21), de modo a formar um elemento de segurança composto (21,31) por meio da sobreposição dos dois elementos de segurança.

2. Cartão inteligente, de acordo com a reivindicação 1, **caracterizado pelo** fato de que os dois elementos gráficos de segurança (21,31) são duas partes distintas de uma imagem ou logotipo, de modo que a superposição dos dois elementos

gráficos de segurança (21,31) permite restaurar toda a imagem ou logotipo.

3. Cartão inteligente, de acordo com a reivindicação 2, **caracterizado pelo** fato de que a área da superfície de pelo menos um dos elementos gráficos (21,31) é maior do que a superfície aparente do módulo e é parte integrante da superfície do módulo, de modo a detectar mais facilmente uma extração fraudulenta de um dos elementos gráficos (21,31).

4. Cartão inteligente, de acordo com a reivindicação 3, **caracterizado pelo** fato de que os ditos segundos elementos gráficos (31) consistem em hologramas e compreendem padrões complementares, de modo que a sobreposição dos gráficos de segurança e do holograma, ou a sobreposição dos dois hologramas permite a aparição de um logotipo de segurança não falsificável.

5. Cartão inteligente, de acordo com a reivindicação 1, **caracterizado pelo** fato de que a camada protetora transparente (29) é formada como uma camada de material de encapsulamento (33) que envolve o corpo completo do cartão em toda a sua superfície.

6. Cartão inteligente, de acordo com qualquer uma das reivindicações anteriores, **caracterizado pelo** fato de que o corpo de cartão (7) tem várias camadas de material, e em que a antena de comunicação (11) está entre duas camadas adjacentes do corpo de cartão e inclui almofadas de contato dispostas no fundo da cavidade do corpo de cartão, as ditas almofadas sendo ligadas a terminais de conexão do módulo eletrônico.

7. Cartão inteligente, de acordo com qualquer uma das reivindicações 1 a 6, **caracterizado pelo** fato de que a antena

de comunicação (11) é realizada no módulo eletrônico (3) propriamente dito e é conectada ao microchip (9), de modo que o módulo (3), revestido com o seu elemento gráfico de segurança (21), pode simplesmente ser transportado e colocado na cavidade (5) do corpo de cartão.

8. Cartão inteligente, de acordo com a reivindicação 7, **caracterizado pelo** fato de que inclui uma segunda antena (23) realizada no corpo de cartão e posicionada em frente à antena (11) do módulo, a fim de ampliar o fluxo eletromagnético recebido pela antena do módulo.

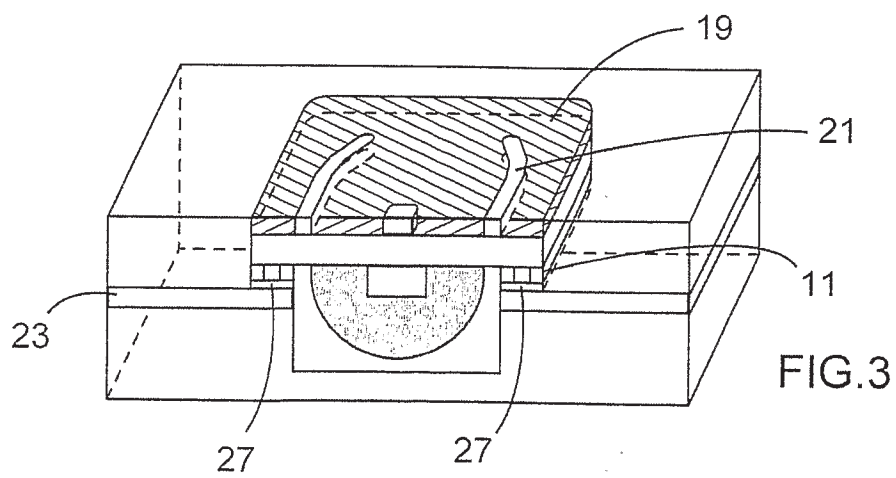
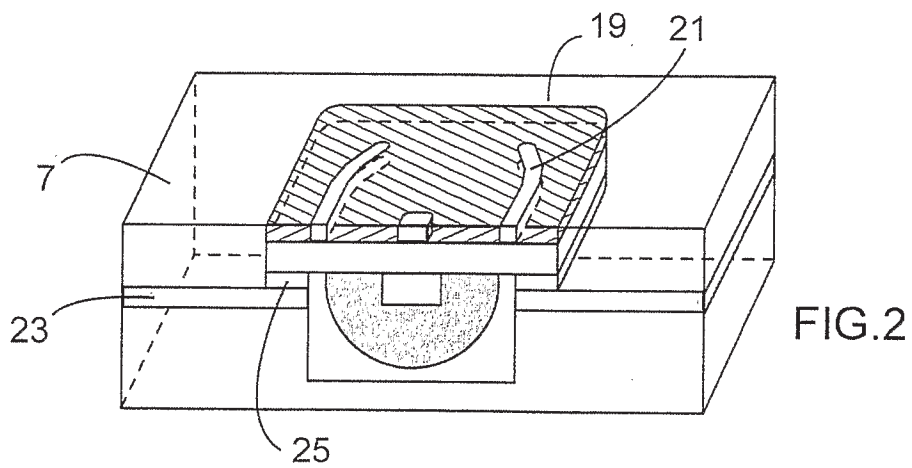
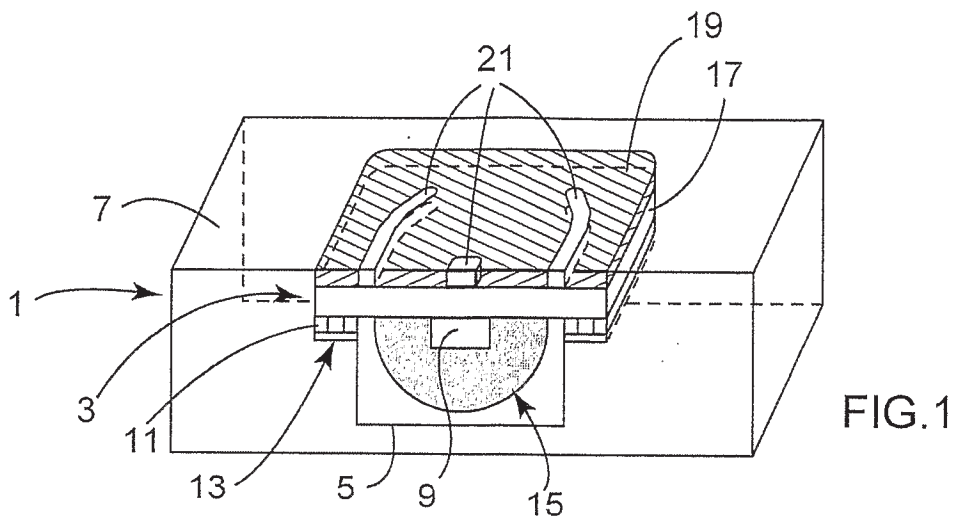


FIG.4

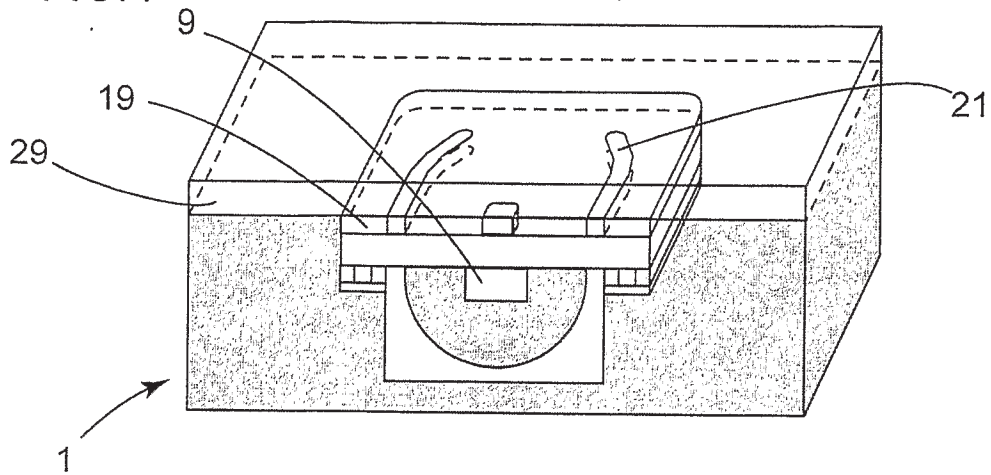


FIG.5

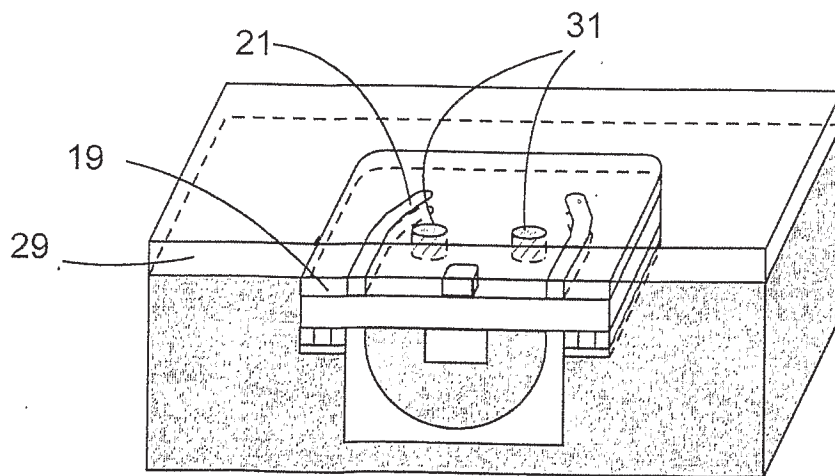
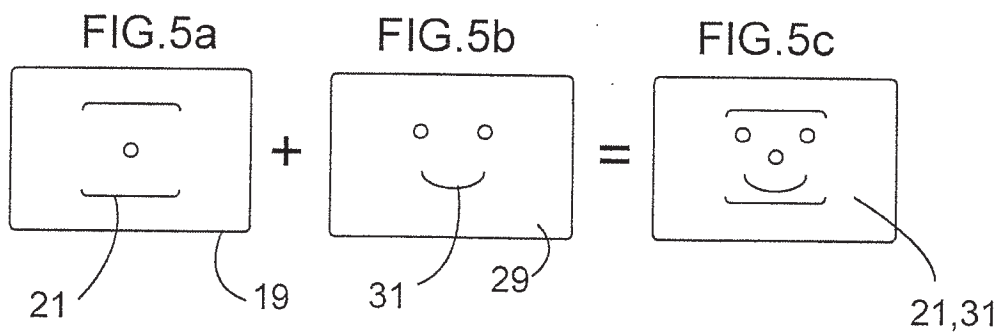


FIG.6

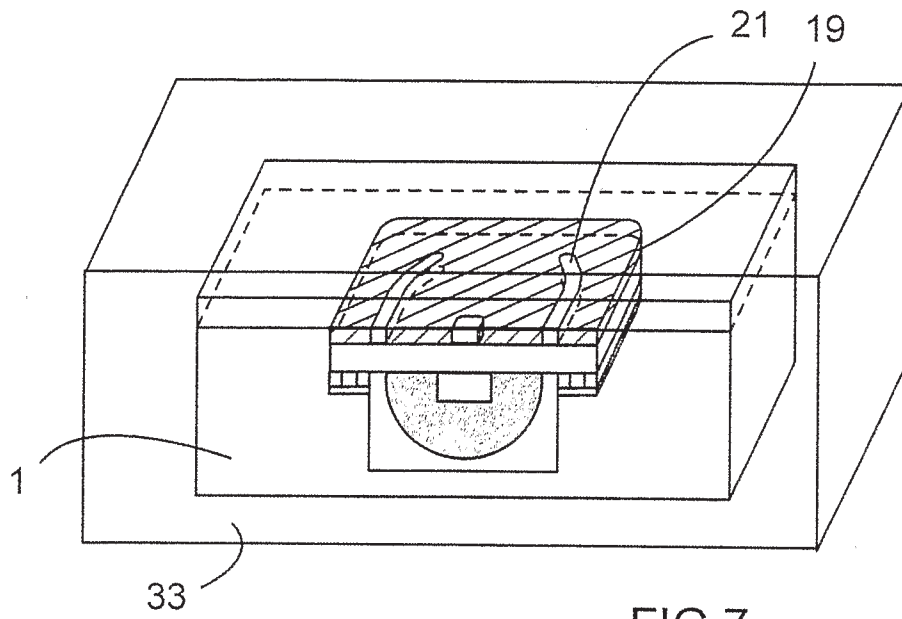


FIG. 7

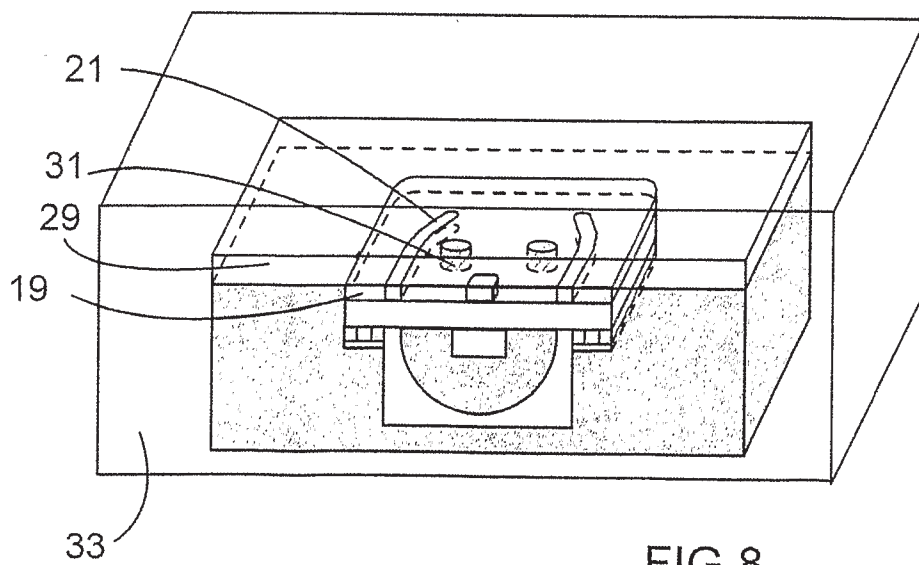


FIG. 8