



HU000029201T2

(19) **HU****MAGYARORSZÁG**
Szellemi Tulajdon Nemzeti Hivatala(11) Lajstromszám: **E 029 201**(13) **T2****EURÓPAI SZABADALOM**
SZÖVEGÉNEK FORDÍTÁSA(21) Magyar ügyszám: **E 09 766026**(22) A bejelentés napja: **2009. 06. 21.**

(96) Az európai bejelentés bejelentési száma:

EP 20090766026

(97) Az európai bejelentés közzétételi adatai:

EP 2294535 A1**2009. 12. 23.**

(97) Az európai szabadalom megadásának meghirdetési adatai:

EP 2294535 B1**2016. 03. 09.**(51) Int. Cl.: **G06K 190/77** (2006.01)

(86) A nemzetközi (PCT) bejelentési szám:

PCT/FR 09/000747

(87) A nemzetközi közzétételi szám:

WO 09153464

(30) Elsőbbségi adatok:

0803472**2008. 06. 20.****FR**

(72) Feltaláló(k):

ARTIGUE, Olivier, F-13530 Trets (FR)**SEMORI, Stéphane, F-83400 Hyères (FR)****TEBOUL, Deborah, F-13127 Vitrolles (FR)****SICOT, Cécile, F-13790 Rousset (FR)**

(73) Jogosult(ak):

Smart Packaging Solutions (SPS), 13106**Rousset Cedex (FR)**

(74) Képviselő:

Danubia Szabadalmi és Jogi Iroda Kft.,**Budapest**

(54)

Érintésmentes kártya biztonsági logóval

Az európai szabadalom ellen, megadásának az Európai Szabadalmi Közlönyben való meghirdetésétől számított kilenc hónapon belül, felszólalást lehet benyújtani az Európai Szabadalmi Hivatalnál. (Európai Szabadalmi Egyezmény 99. cikk(1))

A fordítást a szabadalmas az 1995. évi XXXIII. törvény 84/H. §-a szerint nyújtotta be. A fordítás tartalmi helyességét a Szellemi Tulajdon Nemzeti Hivatala nem vizsgálta.

Contactless card with security logo

The invention relates to contactless smart cards, in particular electronic identification cards or passports, comprising a security logo.

The invention is independent from the size of the smart card, and may be applied equally to conventional smart cards and to other secure documents provided with a contactless card electronic module so that, in order to simplify the presentation, the same term "contactless smart cards" will refer equally to smart cards in a conventional format (according to the ISO 7816-1 standard) and to security documents having a different format, but also being provided with an electronic module of the type normally used in contactless smart cards.

PRIOR ART:

A plurality of types of secure cards or documents comprising an electronic chip are already known in the prior art.

Identity cards in contact smart card format are thus known in which the electronic module is inserted, i.e. fastened in a cavity of the card body, so that the electrical contacts of the module remain accessible on the surface to allow the connection to a contact card reader. This type of identity card poses the problem of possible access to the contacts, or of pure and simple replacement of the electronic module, for identity fraud purposes.

Obviously, it would be desirable to provide contact identity smart cards with a security graphic covering the upper face of the card and allowing cases of fraud to be detected, but a security graphic of this type is not easy to produce in the zone of the electronic module since the conductivity of the contacts risks being compromised.

In order to partially solve this problem, document DE 196 25 466 C1 has described a contact chip card, the contacts of which are themselves provided with a graphic, in particular a specific colour different from the usual gold or silver colour. For this purpose, the contacts are coated with a metal dispersion layer containing aluminium-based colour particles. However, the contacts remain electrically accessible, thus allowing cases of fraud by attacking the circuit of the chip through the chip card contacts. Furthermore, the contacts and the module remain physically equally accessible, thus making it conceivable for the electronic module to be removed or replaced.

From US 6 259 035 B1, a contact chip card is also known in which it has been sought to make the electronic module and the metal contacts as discreet as possible in their appearance by colouring the contacts themselves and ensuring that the graphic of the surface of the module is an extension of the graphic of the card body. Obviously, this method is reserved for contact cards and cannot be suitable for contactless cards such as those used for the manufacture of contactless identity cards.

An opposite approach has also been followed in US 5 552 574, which describes, on the contrary, the manner of providing the surface of the contacts of a contactless chip card with a security etching, produced using a laser beam.

It follows from the preceding examples that the problem of security markings has been tackled for contact cards, either by means of guilloches or other graphics produced on the card body, or by a graphical modification of the metal contacts of the module, in the form of colours or laser etching produced directly on the contacts.

The use of contactless chip cards in security or identity applications is furthermore known, and these cards tend to be widely used in these applications due to their greater ease of use.

In contactless cards, an electronic system, comprising a chip connected to an antenna, is most often produced separately in the form of an insert which is then laminated between external protective layers. The electronic system is then protected against direct access by contact, but it nevertheless remains possible to detach the different layers and fraudulently replace the insert, or even to retrieve it in order to produce a counterfeit contactless identity card.

Another disadvantage of contactless cards produced on the basis of an insert interposed between external protective layers relates to their production method. In fact, the insert is the most expensive part of the card, and it may be damaged during the lamination with the external layers, thus causing the production output of this type of card to fall and the unit cost to increase.

It would therefore be preferable to use more reliable and more efficient production methods, such as the conventional insertion method used for contact cards, consisting in placing a contact module in a cavity of the card. However, as seen previously, this method as such offers low security since the cards produced in this way are particularly exposed to fraud consisting in extracting the module from the card, this being particularly contra-indicated for cards or document intended for identity-checking applications.

Moreover, some cards are produced according to dual communication interface technology, comprising both a contactless electronic system inserted on the card body and furthermore provided with contacts for communication with a contact card reader. This type of card potentially combines the security vulnerabilities of the two types of card previously described.

From document D1 = WO 2001/008397 A1, a security document is known including a substrate on which a film provided with a unique visual element, such as a hologram, is deposited, and an integrated circuit disposed between the substrate and the film. Taking account of the fact that this involves a security document such as a banknote and not a chip card, it is essential that the thickness of the document is kept as small as possible. For this purpose, the integrated circuit is disposed in a cavity of the substrate and therefore the visual element can extend very little, or not at all, beyond the plane of the substrate. This document does not describe the manner in which the visual element produces a document-securing effect.

From document D2 = WO 2008/015363 A1, a security structure is known for a secure document, comprising a substrate, an electronic device carried by the substrate, and at least one security element and/or decorative element carried by the substrate. When a plurality of security elements coexist on the

same substrate, they are disposed in relation to one another without being superimposed on one another. There is therefore no possibility of the visual effects generated by the different security elements being superimposed on one another or interacting visually to strengthen the security of the document.

OBJECT OF THE INVENTION:

One object of the present invention is consequently to propose a contactless card structure capable of overcoming the aforementioned disadvantages of smart identity cards or identity documents.

In particular, one object of the present invention is to propose a contactless smart card intended for identity-checking applications, which is simple to produce with high outputs, comparable to the production outputs of contact cards, while being compatible with security graphics such as security logos or holograms.

Another object of the invention is to propose a smart card having a very high reliability and longevity during its utilisation, in the region of five to ten years, while enabling a high production output and low cost, along the lines of simple cards with contact operation.

For this purpose, the subject-matter of the invention is a contactless smart card as defined in the claims.

According to one very simple basic embodiment, a first graphical security element simply consists of a graphical pattern produced on the visible face of the contactless electronic module.

This graphical pattern consists of zones that protrude and zones that are recessed relative to the surface of the module and/or of zones of different colour from the rest of the surface of the electronic module. This graphical pattern can be obtained in various ways, in particular by screen printing or chemical etching, in the manner of the production of metal contacts produced in a known manner for contact card modules.

So as to offer increased security or resistance in respect of physical attacks on the module, this first graphical security element is surmounted by at least one transparent protective layer, particularly polycarbonate, disposed above the card body, so as to cover the visible face of the contactless electronic module and its graphical security pattern.

In order to further increase the security of the product and its resistance to fraud and counterfeit, the transparent or translucent protective layer comprises, on one of its faces or in its thickness, a second graphical security element that is complementary to the graphical security element of the surface of the electronic module so as to form therewith a composite security element through superposition of the two individual security elements.

The invention thus provides that the two graphical security elements can be two distinct and complementary parts of one image or logo, in such a way that only the exact superposition of the two graphical security elements allows the complete image or logo to be reconstructed.

In this way, it is evident that the elimination of the upper protective layer would cause the second graphical security element to disappear, which could be detected immediately, since the logo or equivalent would no longer be complete.

In one useful variant of this embodiment, the second graphical element comprises a hologram, having a pattern that is complementary to the security graphic of the surface of the electronic module, in such a way that the superposition of the security graphic and the hologram cause an unfalsifiable security logo to appear.

The surface of the hologram or more generally of at least one of the graphical elements is advantageously larger than the visible area of the module and is securely fastened to the surface of the module, so as to make it easier to detect fraudulent extraction of one of the graphical elements.

In order to further increase resistance or highlighting of physical attacks on the contactless smart card, the transparent protective layer is extended beyond the upper surface of the card and is produced in the form of a layer of encapsulating material surrounding the card body in its entirety over all its surface.

Obviously, the hologram technique is not reserved for the transparent protective layer or the encapsulating layer, but the graphical security element of the surface of the electronic module may also or independently comprise a hologram representing a security pattern and disposed above the visible face of the module so that access to the module requires the destruction of the hologram.

The variants above may be produced regardless of the contactless communication structure of the card, i.e., for example, the communication antenna may be directly located on the electronic module or in the card body, and it may also be complemented by a second antenna serving as an electromagnetic flux amplifier in relation to the first antenna.

Thus, in a first variant, the card body comprises a plurality of layers of material, of plastic material or even paper, and the antenna is produced between two adjacent layers of the card body and comprises contact pads disposed at the bottom of the cavity in the card body and connected to connection terminals of the electronic module.

According to a different variant, the antenna is produced on the electronic module itself and is connected to the electronic chip of the latter, so that the module coated with its graphical security element may simply be placed and fastened in the cavity of the card body.

However, the card may also comprise a second antenna produced in the card body and placed facing the antenna of the module, so as to amplify the electromagnetic flux collected by the antenna of the module.

Obviously, the invention extends to all smart cards comprising a card body and an innovative module as described above.

Other characteristics and advantages of the invention will become evident from a reading of the detailed description and from the attached drawings, in which:

- Figure 1 shows a perspective view and sectional view of a contactless smart card provided with an electronic module, the visible surface of which comprises a graphical security element according to the invention;
- Figure 2 shows a view similar to that shown in Figure 1, but in which the smart card comprises a large antenna integrated into the card body and connected to electrical contacts of the chip of the electronic module;
- Figure 3 shows a view similar to that shown in Figure 2, but in which the second antenna is not connected to the chip of the electronic module;
- Figure 4 shows a view similar to that shown in Figures 1 to 3, but in which the graphical security element of the surface of the electronic module is covered by a transparent protective layer;
- Figure 5 shows the elements of an electronic module capable of creating a security image by superposition of layers;
- Figure 6 shows a perspective view and sectional view of the superposition of layers according to Figure 5c, in which the transparent protective layer comprises a second graphical security element complementary to that of the surface of the electronic module;
- Figure 7 shows a view similar to those shown in Figures 1 to 3, in which a transparent encapsulating layer covers the entirety of the smart card;
- Figure 8 shows a view similar to that shown in Figure 6, in which a transparent encapsulating layer covers the entirety of the smart card.

Reference is made to Figure 1. This figure shows a perspective view and sectional view of a zone of a contactless smart card 1, in the vicinity of the electronic module 3 of the smart card, on the understanding that the zone shown may also correspond to a part of a secure document having a format different from that of a smart card, such as, for example, an electronic passport or identity card, and including an electronic module having contactless operation.

In a known manner, the electronic module 3 is mounted in a cavity 5 of the card body 7. A chip 9 fastened to the face of the module opposite its visible face is shown schematically. The chip 9 is electrically connected to the terminals of an antenna 11 produced on the module and intended to provide contactless communication with an external reader (not shown). The electronic module 3 is fastened in the cavity 5 by means of an adhesive 13. The electronic chip 9 is protected by a drop of encapsulating resin 15. During the assembly of the smart card, the module is placed facing the cavity 5 disposed in the card body. The module is placed in the cavity as shown in Figure 1, the turns of the antenna 11 coming into contact with the adhesive 13. A step of pressing on the upper face of the module then takes place to provide a good-quality adhesion of the module in the cavity.

The chip 9 and the turns of the antenna 11 are fastened onto a carrier layer 17 of dielectric material, which is in turn surmounted by the visible face 19 of the electronic module 3 when the latter is placed in the cavity 5 of the card body.

According to the invention, this visible layer 19, the surface of which is flush with the surface of the card body, comprises one or more graphical security elements 21, capable of protecting the electronic module and the contactless card against fraud attempts. For this purpose, this visible layer 19, which is, in particular, produced from metal in the same way as the well-known contacts of contactless smart cards, comprises graphical patterns, produced by various techniques known per se, such as etching or printing, and capable of identifying the smart identity card or its bearer, or in any event making a fraudulent copy of the identity card more difficult.

Thus, whereas in the case of contact cards, the surface of the module comprises electrical contacts of more or less uniform and standardised shape and size, the contactless card according to the invention comprises graphical elements produced with similar technologies known per se, but with a different shape and function, i.e. the security marking of the modules of the contactless cards. It must be noted that a marking of this type is not in itself required to perform the communication function of the smart card with an external reader, but, due to its difficulty of being copied, it performs a new security function in its application to a contactless card.

Obviously, the size and shape of the graphical security elements 21 may be of any type, as well as their manner of implementation, insofar as they achieve the desired security objective.

Insofar as the graphical security elements 21 do not interfere with the contactless communication function of the smart card, this communication structure may be produced in a variety of forms.

Figure 2 thus shows a variant in which, in order to increase the communication range of the contactless smart card, an antenna 23 larger than the antenna 11 shown in Figure 1 has been disposed between layers of the card body 7, instead of the antenna 11 of the module, and this antenna 23 is connected to appropriate terminals of the electronic chip 9 via connection pads 25.

A different implementation variant is shown in Figure 3, in which the second antenna 27 is electrically insulated from the antenna 23 by an insulating layer 27. The antenna 23 is thus likely to resonate with the antenna 11 of the module, and then serves as an electromagnetic amplifier with regard to signals that must be exchanged between the electronic chip 9 and an external contactless reader.

According to an even more useful variant of the invention, shown schematically in Figure 4, the visible layer 19 of the electronic module comprises first graphical security elements 21, and this visible layer 19 is surmounted by at least one transparent or at least translucent protective layer 29, disposed above the card body, so as to cover the visible face 19 of the electronic module and its first graphical security elements 21. A material that is sufficiently resistant to prevent its separation from the rest of the card, and sufficiently durable to ensure the longevity required by identity card applications, typically from 5

to 10 years, will be chosen for the protective layer 29. One possible choice will be to produce the protective layer from polycarbonate or equivalent.

As shown schematically in Figure 5b, the protective layer 29 itself preferably comprises second graphical security elements 31, ideally complementary to the first graphical security elements 21 disposed on the visible face 19 of the module, so that their superposition forms a composite image or a complete security logo (21, 31) obtained by superposition of the images of the first and second graphical security elements (21, 31).

The two graphical security elements (21, 31) are thus ideally two distinct parts of the same composite image or of a logo, so that only the superposition of the two graphical security elements allows the complete image or logo or to be reconstructed. Conversely, the removal of or damage to the upper protective layer 29 would immediately result in the detection of the fact that the contactless smart card has been modified and can no longer be accepted by the card application management authorities.

Obviously, in order to avoid accidental damage to the second graphical security elements 31, it is preferable for these elements to be produced either on the face of the layer 29 which is in close contact with the external face of the layer 19, or in the thickness of the layer 29, as shown in perspective in Figure 6.

In one advantageous variant of the invention, said first and/or second graphical elements 21, 31 comprises holograms. The hologram 31 thus has a pattern that is complementary to the security graphic or to the hologram 21 of the surface of the electronic module, so that the superposition of the security graphic and the hologram, or of the two holograms, causes an unfalsifiable security logo to appear.

The surface of at least one of the graphical elements (21, 31) is preferably larger than the visible surface 19 of the module and is securely fastened to the surface of the module, so as to make it easier to detect a fraudulent extraction of one of the graphical elements (21, 31).

As shown in Figure 7, the transparent protective layer 19 provided with graphical security elements 21 can protrude beyond the surface of the smart card and can be produced in the form of a layer of encapsulating material 33 that surrounds the card body in its entirety over all its surface, thus rendering any separation of the layers of the smart card impossible without visible damage.

An encapsulating layer 33 of this type may obviously also be envisaged in the case where the card comprises an additional protective layer 29 provided with second graphical security means 31, as shown in Figure 8.

ADVANTAGES:

The invention achieves the defined objects and proposes a smart card using a contactless electronic module, comprising graphical security elements allowing resistance to physical attacks on the contactless cards to be substantially increased, particularly, but not exclusively, for bearer identity-checking applications, such as contactless identity cards and contactless passports.

In reality, the graphical security elements 21 being produced on the surface of the electronic module, this module becomes particularly simple to use by manufacturers not specialising in contactless cards. In fact, it suffices to place the already secured contactless module in the cavity of a card body, by using very conventional insertion methods already well-known in the field of contact cards, resulting in a significant gain in the rate of production, a significant increase in production outputs and reliability and correlatively a reduction in the unit cost.

It thus becomes possible to apply this technology for the production of modules with a security logo to obtain smart cards intended for field applications that are very demanding or have a very long utilisation period, such as, for example, application to electronic passports or identity cards for which the government offices generally require a guarantee of good performance and effective operation for ten years.

Érintésmentes kártya biztonsági logóval

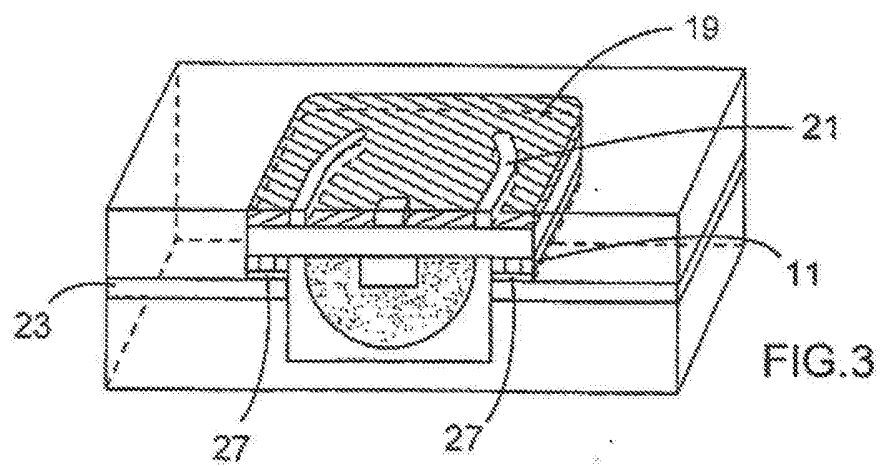
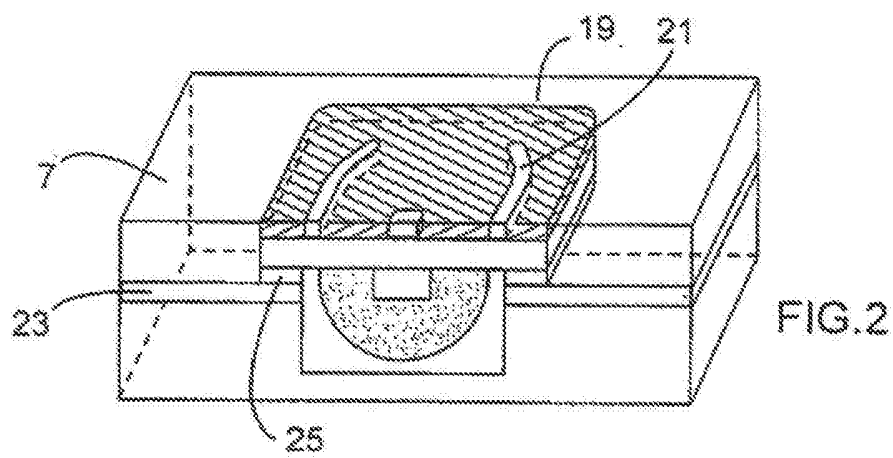
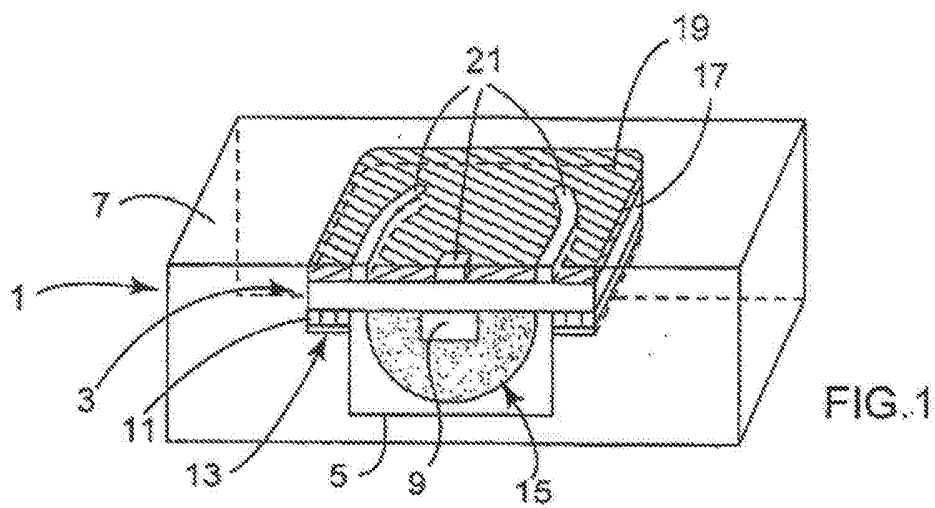
Szabadalmi igénypontok

1. Érintésmentes chipkártya (1), amely egy kártyatestet (7) és egy elektronikus modult (3) tartalmaz, amely egy elektronikus chippel (9) van ellátva, amely egy antenna (11) csatlakozóival van összekötve, ahol az elektronikus modul (3) egy üregben (5) van elrendezve, amely üreg a kártyatestben van kiképezve, emellett az elektronikus modul (3) látszódó oldala (19) legalább egy első grafikai biztonsági elemmel (21) rendelkezik, amely fölé legalább egy átlátszó védőréteg (29) van elhelyezve, amely a kártyatest fölött van elrendezve, oly módon, hogy átfedje és védje az elektronikus modul látszódó oldalát (19), ahol az első grafikai biztonsági elemet (21) olyan grafikai motívum képezi, amely többletvastagságú zónákat és az elektronikus modul felületéhez képest besüllyesztett zónákat tartalmaz és/vagy olyan zónák képezik, amelyek színe különböző az elektronikus modul felületének többi részétől, ahol a többletvastagságú zónák és a besüllyesztett zónák és/vagy az eltérő színű zónák az elektronikus modul olyan biztonsági megjelölését képezik, amely alkalmas arra, hogy megvédje az elektronikus modult és az érintésmentes kártyát a grafikai biztonsági elem (21) kizsákmányolása általi csalási kísérletektől, *azzal jellemezve*, hogy az átlátszó védőréteg (29) legalább egy második grafikai biztonsági elemet (31) tartalmaz, amely az első grafikai biztonsági elemet (21) oly módon egészíti ki, hogy azzal egy, a két biztonsági elem (21; 31) egymásra helyezése révén egy összetett biztonsági elemet (21, 31) képez.

2. Az 1. igénypont szerinti chipkártya, *azzal jellemezve*, hogy a két grafikai biztonsági elem (21, 31) egy kép vagy egy logó két különálló részét képezi oly módon, hogy a két grafikai biztonsági elem (21, 31) egymásra helyezése teszi lehetővé a teljes kép vagy logó helyreállítását.

3. A 2. igénypont szerinti chipkártya, *azzal jellemezve*, hogy a grafikai biztonsági elemek (21, 31) legalább egyikének felülete nagyobb, mint az elektronikus modul látszódó felülete, és szilárdan össze van kötve a modul felületével, oly módon, hogy a grafikai biztonsági elemek (21, 31) egyikének csalo szándékú kihúzása jobban láthatóvá váljon.

4. A 3. igénypont szerinti chipkártya, *azzal jellemezve*, hogy a második grafikai biztonsági elemek (31) hologramokból állnak és egymást kiegészítő motívumokkal rendelkeznek, oly módon, hogy a grafikai biztonsági kialakítás és a hologram egymás fölé helyezése vagy a két hologram egymás fölé helyezése egy hamisíthatatlan biztonsági logót eredményez.
5. Az 1. igénypont szerinti chipkártya, *azzal jellemezve*, hogy az átlátszó védőréteg (29) egy kapszulázó anyagból levő réteg (33) formájában van kialakítva, amely körbeveszi a kártya egész testét annak teljes felületén.
6. Az előző igénypontok bármelyike szerinti chipkártya, *azzal jellemezve*, hogy a kártyatest (7) több anyagréteggel rendelkezik, és *azzal jellemezve*, hogy a kommunikációs antenna (11) a kártyatest két szomszédos rétege között van kialakítva és olyan érintkezőelemekkel rendelkezik, amelyek a kártyatest üregének aljában vannak elrendezve és az elektronikus modul összekötő csatlakozóival vannak összekötve.
7. Az 1-6. igénypontok bármelyike szerinti chipkártya, *azzal jellemezve*, hogy a kommunikációs antenna (11) magán az elektronikus modulon (3) van kialakítva és annak elektronikus chipjével (9) van összekötve, oly módon, hogy a grafikai biztonsági elemével (21) lefedett elektronikus modul (3) könnyen áthelyezhető és a kártyatest üregében (5) rögzíthető legyen.
8. A 7. igénypont szerinti chipkártya, *azzal jellemezve*, hogy a chipkártya egy második antennával (23) rendelkezik, amely a kártyatestben van kialakítva és az elektronikus modul antennájával (11) szemben van elrendezve, oly módon, hogy felerősítse az elektronikus modul antennája által befogott elektromágneses fluxust.



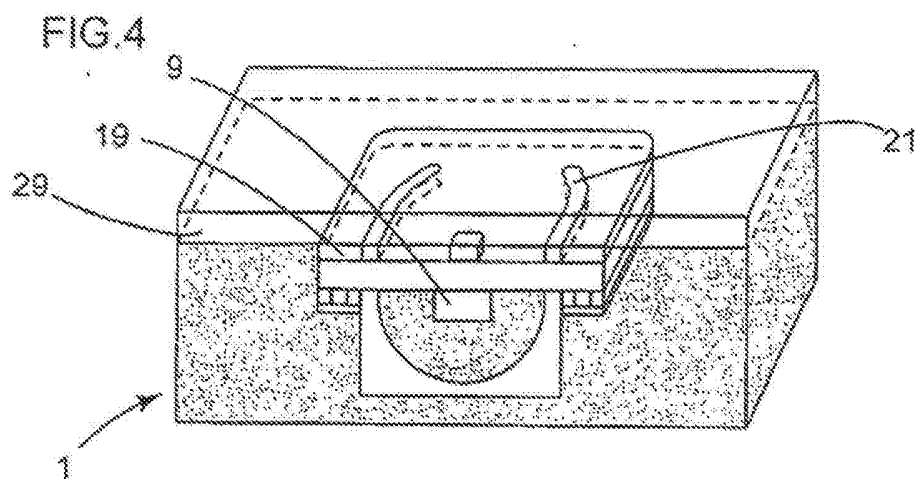


FIG.5

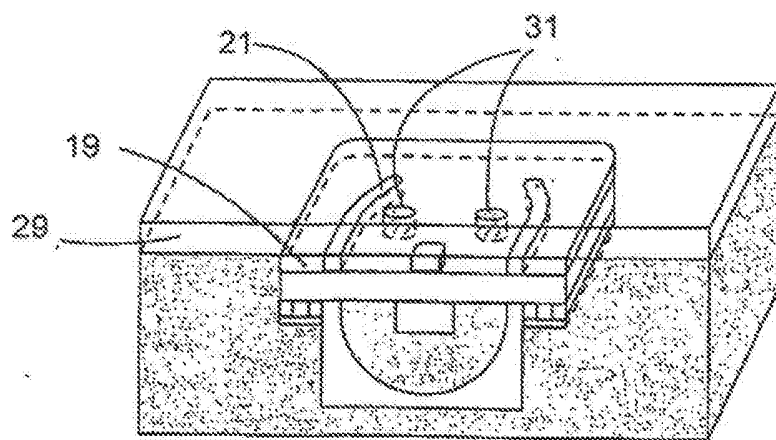
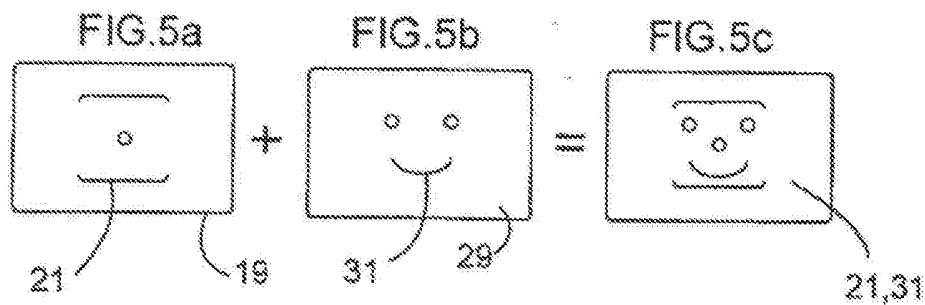


FIG.6

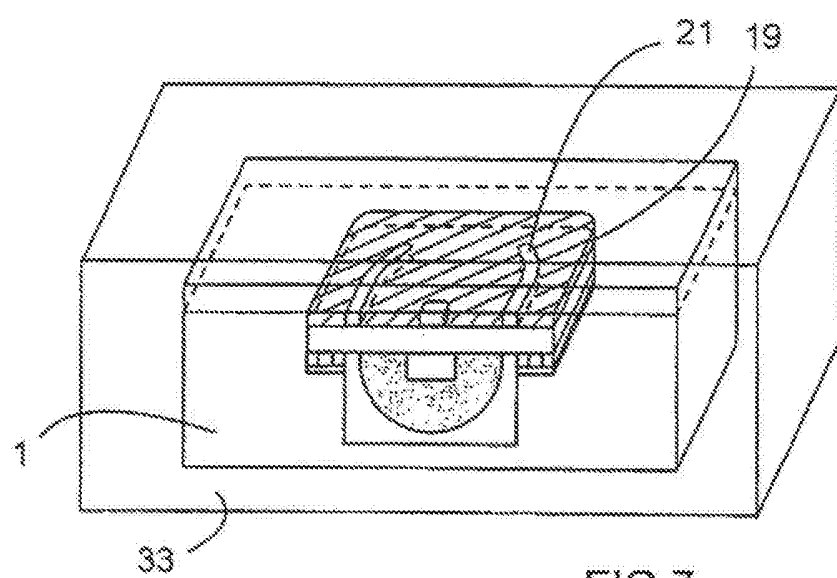


FIG. 7

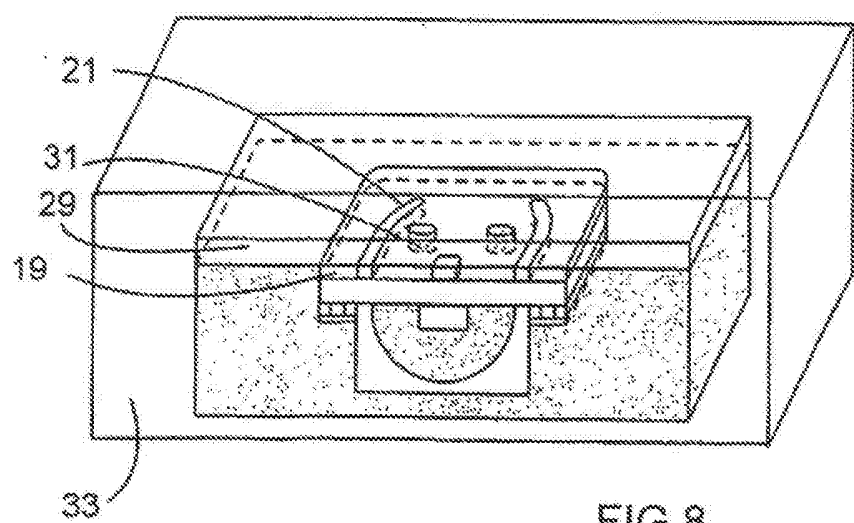


FIG. 8