(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 540 519 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
02.01.2013 Bulletin 2013/01

(51) Int Cl.:
B42D 15/10 *(2006.01)* ***B41M 3/14*** *(2006.01)*

(21) Application number: **11305815.0**

(22) Date of filing: **27.06.2011**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **Oberthur Technologies**
92300 Levallois-Perret (FR)

(72) Inventor: **Delaplace, Gilles**
92000 Nanterre (FR)

(74) Representative: **Delumeau, François Guy et al**
Cabinet Beau de Loménie
158, rue de l'Université
75340 Paris Cedex 07 (FR)

(54) **A data carrier and a method of personalizing a data carrier**

(57) The invention is a data carrier (100) having first and second faces, a first face (101) of said carrier having an area (101') for printed information on the first face (101), with there being a window (105) extending between the first face (101) and the second face (102) of the carrier, characterized in that the area (101') for printed information covers at least a part of said window (105). A personalized security document based on such carrier is also disclosed.

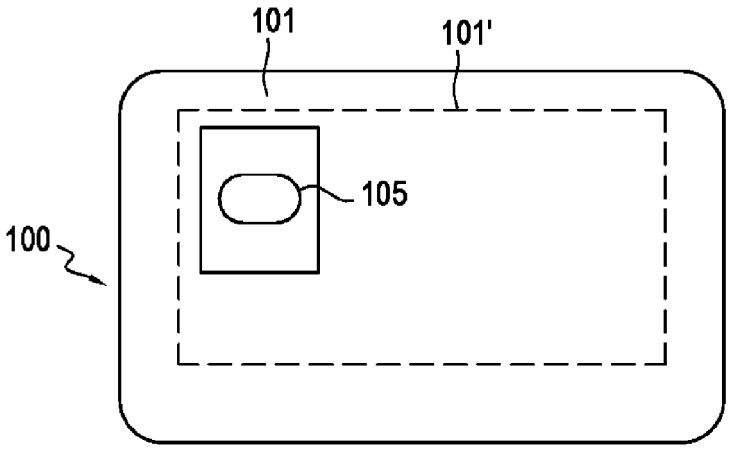

FIG.11

EP 2 540 519 A1

Description

Field of the invention

[0001] The invention relates to a data carrier and in particular but not exclusively to a data carrier in the form of an identity card or passport. In particular but not exclusively, the invention relates to documents with encrypted security features.

Background information

[0002] Data carriers such as security documents are usually carried by a bearer and used at control points such as airport check-ins. The security procedures used at the control points check the authenticity of the document and the fact that it has not been corrupted. These checks are usually made by a security agent.

[0003] The potential corruption of certain critical features of the document are checked, including the picture of the bearer, his or her name and social security number, the document number or the name of the authority that granted the identity card or the passport.

[0004] Some of these critical features are features introduced upon a personalization step when issuing the data carrier so the data carrier is linked just to the bearer. The critical features are typically the picture of the bearer but other features that are personal to the bearer can be used, for example finger prints or data on the data carrier that is linked to a separate carrier of data, such as a photograph that the bearer has with him or her. The data carriers that are intended to have a security feature are often manufactured and delivered to the granting authority in a semi-finished state, the granting authority being left with the personalization elements that are personal to the bearer on a case by case basis.

[0005] Known methods of corruption of a data carrier include modification or replacement of an isolated critical feature, such as the portrait photo of the bearer.

[0006] There is a growing need for enhancing the security level related to those documents and their critical features. In that regard, data carriers with encrypted graphics are known. In the context of the invention, encrypted graphics are graphic features that are invisible for the eyes of a human person, but that can be revealed for the eyes of the human person with an adequate optical system, known as revealing device.

[0007] Encrypted graphics can help a security agent to determine that the document was not corrupted, since those encrypted graphics are difficult to reproduce.

[0008] Moreover, if the encrypted graphics is co-printed or co-engraved, or more generally collocated (or intimately grouped together) with a critical feature (for example the portrait picture), i.e. if it lies in the same zone of material, the authenticity of the critical feature itself is guaranteed, since modification or replacement of the critical feature would have necessary impacted the encrypted graphics.

[0009] However, with encrypted graphics collocated with a critical feature of a data carrier, the critical feature must first be observed without the revealing device, in order to perceive all subtle details of its visual information with no distortion caused by the encrypted graphics. Subtle details may include, for example, details of the physical person's face presented in a photo, like the eyes of said person. In a second step, the document is observed with the revealing device to check the presence and integrity of the encrypted graphics.

[0010] With known systems, the security agent needs to have a revealing device with him or her enabling the decoding of the encrypted graphics, This is a major drawback, as various circumstances can require the data carrier to be checked unexpectedly, at a distance from the security office where the revealing device or system is likely kept. Furthermore, having to use a revealing device involves an extra step in the checking of documents as first the personalization features and then the encrypted features are checked which adds time to the checking process.

[0011] Known revealing devices include the use of a revealing component such as a revealing lens, network or filter in a foldable sheet or sheet fraction of the document that is being checked. This revealing component can be superimposed with the surface bearing encrypted graphics to reveal the encrypted graphics to the person having the document in their possession. Co-printed critical features and encrypted graphics of the document are placed on an opaque or opacified sheet surface. Such a solution is presented in the documents FR2918311 and EP1889727 related to passport booklets. In the latter document, it is in particular contemplated that the revealing component is attached or integrally formed with a regular page of the document.

[0012] A problem with such known systems for the authentication of the data carrier is that they require the manual operation of folding the document or its sheets and superimposing the revealing components and the encrypted graphics. Such operation, when performed a large number of times, like at an airport control desk, is cumbersome. Furthermore, such a solution also leaves open the issue of providing authentication to a non-foldable data carrier, such as a polycarbonate card serving as an identity card or included in a passport.

[0013] In FR2947211 there is discussion of a window in a card, extending in the thickness of the card in a manner allowing the light to go through the card, the window including a revealing lens or network. Such card also includes hidden information comprised in personal data specific to the in a way that it is not to reveal the hidden information with the window, because it would require folding the card to have the window and the hidden information coincide.

[0014] To proceed to the authentication of a first card (card to authenticate), a security agent needs to use another such card (revealing card), which can be his own personal security document or that of another individual,

and, superimpose the two cards in such a way that the position of the window of the revealing card matches with the position of the hidden information of the card to authenticate. This requires having the two cards aligned one with each but with the second card shifted from the first one parallel to their plane.

[0015] This solution first requires having a revealing card in one's possession to authenticate a card. It also requires a two-step authentication process, including first examining the critical feature without the revealing card, in order to perceive all subtle details of its visual information with no distortion, and then, in a second step, observing the card to authenticate with the revealing card positioned in a shifted position, to check the presence and integrity of the encrypted graphics. The step of positioning in a shifted manner is likely to be time-consuming, which is a drawback when performing a large number of controls is necessary, like at an airport control desk. It also requires the need to have two hands free and there is the risk that one step in the process may not be carried out as thoroughly as the other if the person checking the information is rushed.

[0016] The present invention seeks to overcome the problems of the prior art by providing a data carrier having security features which allows for easier and faster authentication and a system less likely to lead to inaccurate checking and which is particularly suitable at security control points where large numbers of people must he in a rapid manner with high reliability,

Summary of the invention

[0017] Accordingly, an aspect of the invention provides a data carrier having first and second faces, a first face of said carrier having an area for printed information on the first face, with there being a window extending between the first face and the second face of the carrier

[0018] The data carrier according to this aspect of the invention is remarkable in that said area for printed information covers at least in part the window.

[0019] The data carrier having said area for printed information covering at least in part the window allows its area for printed information to be examined through two different and separate angles, i.e. from front and from rear. This can be used in different ways, one of which is particularly disclosed herein.

[0020] This data carrier, when printed with the visual information collocated (intimately grouped together) with encrypted graphics constitutes a document that is easy to control and authenticate with an optical filter for revealing the encrypted graphics.

[0021] Indeed, the non-distorted visual information can be examined on the front face of the carrier, and a filter for revealing the encrypted graphics, if not already present as an incorporated element, can be placed on the rear face of the carrier, allowing the security agent to examine the revealed encrypted graphics on the rear face, through the window. Thus no folding is necessary, and handling of the document is very much facilitated compared to prior art solutions.

[0022] In particular, the data carrier can be hold to examine details of the visual information on the first side, and, after a simple gesture of turning the carrier back, the revealed encrypted graphics can be also examined. Complete cheking can thus be performed with a single hand.

[0023] In an the data carrier comprises an optical filter for revealing encrypted graphics, said filter art least a part of a face of the window within the second face of the carrier, said filter being opposite the area for printed information and integral on the carrier. Handling of the carrier is thus facilitated, since the filter is incorporated, and the authentication can be performed with no separate revealing device.

[0024] In another embodiment, the data carrier includes an optical filter for revealing encrypted graphics wherein the filter and the carrier can be stuck together to form a one piece structure with the filter covering at least a part of a face of the window within the second face of the carrier, said filter being stuck opposite the area for printed information in the first face of the carrier.

[0025] According to an embodiment, the area for printed information is a personalization area, for example a personalization area for a portrait photo covering at least in part the window. The term portrait photo is intended to designate a standard portrait photo. Outside the personalization area, labels or logos not personal to the bearer can be present.

[0026] Other features of the invention include the fact that said window is positioned in a region of the area for printed information that corresponds to the upper part of a portrait photograph of a face of a bearer of the carrier so the eyes of the bearer in said photograph are visible when viewing the carrier from the second face of the carrier. This is easy to recognize since on a standard portrait photo, the region of the eyes is always at the same place.

[0027] This feature is useful since it allows the security agent to check that the region of the eyes of the picture has not been corrupted, which is critical since matching the region of the eyes of the bearer with the region of the eyes of the portrait photo is an excellent way of checking that the picture is indeed or the bearer,

[0028] In interesting embodiments, the carrier includes a polycarbonate body, and can include, or be constituted essentially of, a rectangular card such as an identity card, or, as an alternative, a booklet such as a passport.

[0029] A second aspect of the invention is a data carrier as disclosed herein including visual information and encrypted graphics on the area for printed information. The visual information and encrypted graphics are collocated (intimately grouped together) on the window. The visual information is seen clear when viewed from the first face and the encrypted graphics is seen from the second face.

[0030] Also, the encryption mode used can be based on an encryption code, for example a scrambled indicia® encryption code or a GSSC code.

[0031] According to a third aspect of the invention, a method of personalizing for a particular individual a data carrier, for example for a security document, is disclosed, comprising collocating (intimately grouping together) visual information and encrypted graphics. At least some part of the collocating step is performed over a window traversing the carrier. The data carrier obtained is easy to control and authenticate with an optical filter for revealing the encrypted graphics, since the visual information and encrypted graphics can be seen through two different and separate angles.

[0032] The visual information and encrypted graphics may be deposited in simultaneous or distinct steps. Deposition can include printing, engraving or other methods, provided that the visual information and encrypted graphics are finally collocated.

[0033] In an embodiment, the method comprises collocating the region of the eyes of a portrait photo and encrypted graphics on said window.

[0034] A fourth aspect of the invention is a method of control of the identity of an individual bearing a data carrier, comprising observing information personal to the own a first face of the and checking the presence of an encrypted graphics by observing the second face of the document.

[0035] Advantages of the invention will become apparent from the following description taken in conjunction with the accompanying drawings wherein certain embodiments of the invention are set forth.

Brief description of the drawings

[0036]

Figure 1 illustrates a data carrier according to an embodiment of the invention.

Figure 2 is a side view of a data carrier conforming to the invention.

Figure 3 is a schematic drawing showing a trajectory of visible light inside the data carrier.

Figure 4 shows the resulting image seen by a user.

Figure 5 is a schematic drawing showing another trajectory of light inside the data carrier.

Figure 6 shows the resulting image seen by the user.

Figure 7 shows a data carrier according to a second embodiment of the invention.

Figure 8 shows an accessory for the use and authentication of the data carrier of the second embodiment.

Figure 9 shows a rear view of the document of the second embodiment used with the accessory of figure 8.

Figure 10 shows a third embodiment of a data carrier according to the invention.

Figure 11 shows a carrier for a data carrier before a step of personalization for a particular carrier.

Figure 12 shows a method of preparing a data carrier according to an embodiment of the invention.

Detailed description of an embodiment of the invention and alternatives

[0037] The invention will be described in terms of a specific embodiment, to which various modifications, rearrangements and substitutions can be made.

[0038] Referring to figure 1, an example of a security document (as an example of a data carrier) to which the invention applies is illustrated. The document is a level one security identity card essentially made of a rectangular card 100 approximately of the size of a credit card. This card 100 constitutes a carrier for an identity card.

[0039] Its front face 101 has a predefined area for printed information that is a personalization area 101'. In the disclosed embodiment it is rectangular and has been personalized to show a standard portrait photo 110 of the bearer and if required, further information 150 such as name, address, gender or age of the bearer or user. This information 150 and the photo 110 are personal to the bearer of the card 100. By personal, it is meant that the information is connected with the bearer in some way but it needs not be limited to a picture. It could be another piece of information such as a picture of an object that the bearer has. This way, the bearer presents the card 100 in conjunction with the object so a comparison can be made, by example by a security agent, between the two pieces of information that are connected with the bearer.

[0040] The lateral dimensions of the card 100 (and its front face 101) are around 86 x 54 mm, for example. In the described embodiment, both dimensions of the personalization area 101' (length and height) are shorter than the respective dimensions of the front face, but one of these dimensions or both of them could be equal to the respective dimension of the front face. In alternative embodiments, the personalization area 101' could have a non-rectangular shape, or there could be several separate personalization areas.

[0041] The portrait photo 110 is collocated with encrypted graphics 111, which is not visible to the eyes of an individual with no specific equipment. This encrypted graphics, in a specific embodiment, might be encrypted with GSSC technology or with the Hidden **Indicia** ™ technology, which allows invisible data to be integrated into a photo. The encrypted graphics 111 is approximated to the location that corresponds with the region of the eyes of the standard portrait photo 110, such region being always at the same place because of the standard of the photo. The encrypted graphics can include letters, symbols, a logo or another visual pattern or a combination of these graphics.

[0042] Referring to figure 2, which is a side view of the security document of figure 1, the card is made of a material and has a thickness that allows it to be essentially rigid. The card 100 is thus easily inserted in a wallet or in a card case or card folder, since it is mostly unfoldable. In an embodiment, the material is essentially a polycarbonate polymer, and the thickness is 0.8 mm. Other ma-

terials can be used, such as PVC (polyvinyl chloride) or PET (polyethylene terephthalate) or paper. The rear face 102 is parallel to the front face 101.

[0043] The portrait photo 110 and the encrypted graphics 111 are positioned on the personalization surface 101'. Various methods can be used. The portrait photo 110 and the encrypted graphics 111 can be printed directly on the polycarbonate surface by an offset process, a laser engraving process, a punching or an embossing process. Alternatively, the portrait photo 110 and the encrypted graphics 111 can be printed on or in an additional transparent plastic sheet that is laminated on the personalization surface 101'.

[0044] A material window 105 is present in the thickness of the card 100. It is covered by a portion of the portrait photo 110, which is the region of the eyes. The window 105 extends from the front face 101 to the rear face 102 of the card 100, having a generally cylindrical shape, with any kind of section geometry (rectangular, oval or oblong, for example). Its rear surface is labeled 102' on figure 2. Outside the window 105, the card 100 is opaque, but the window 105 is transparent. In the context of the invention, transparent is meant to characterize a material body causing little or no distortion, and little or no absorption to regular visible light.

[0045] The window 105 is made of a transparent material body that is inserted in a cavity of the card 100. As an alternative, the material of the card 100 is transparent, and its front and rear surfaces have been opacified outside the perimeter of the window.

[0046] The window allows visibility through the window with excellent resolution, inducing no distortion nor absorption on regular visible light patterns, in a way that all subtle details of a portrait photo can be potentially examined through the window 105.

[0047] An optical filter 120 is present on the rear surface 102 of the card 100. In a particular embodiment, the filter 120 has been laminated on the rear surface 102, but it could also be printed on the rear surface 102 using an offset process, or a laser engraving process, a punching or an embossing process. The filter 120 covers the rear surface 102' of the window 105. The filter is integral with the card and cannot be displaced from the rear surface 102' of the window 105.

[0048] Referring to figure 3, when a user stares at the front surface 101 of the card, the portrait photo 110 is visible for him, as it is apparent on the front surface 101. The user also sees objects behind the window 105 and the filter 120. But since no encrypted graphics is present in the space behind the filter 120, nothing is revealed for the user by the filter 120 in this configuration. Finally, the window 105 and the filter 120 being both transparent for the regular visible light, the user does not see anything particular except the portrait photo.

[0049] Referring to figure 4, the configuration of figure 3 with the card 100 being placed in of a light source, the user can see the portrait photo 110 with all details and no distortion nor loss of visual information, since no encrypted graphics appears on the photo.

[0050] The two portrait photos show the effect with different skin tones. A brighter central area delimited by the perimeter of the window 105 is visible, since some light is allowed to go through the window 105, whereas the periphery of the portrait photo 110 is slightly darker. The window 105 has an oblong section, resulting in a brighter central area with an oblong perimeter. Should the card be placed against a non-illuminated surface, the brighter central area would hardly be visible.

[0051] In the configuration of figure 5, a user stares at the rear surface 102 of the card. A fraction of the portrait picture 110 is visible for him in a reversed manner. The fact that the picture is reversed is due to the fact that the portrait photo has been printed for a viewer positioned in front of the front surface 101. The fact that only a fraction of the picture is visible is due to the fact that, in the presented embodiment, the window 105 has a perimeter smaller than the portrait photo 110.

[0052] Importantly, the filter 120, being interposed between the portrait photo 110 and the human viewer, allows the user to see the portrait photo, but also the encrypted graphics 111 co-printed with it. Referring to figure 6, illustrating the configuration of figure 5, only a fraction of the portrait photo 110 inside the perimeter of the window 105 is visible. It has the same size and shape as the brighter area visible on the other side of the card (figure 4), and includes the encrypted graphics 111 co-printed with the portrait picture 110, that is decoded and thus visible for the human user.

[0053] Importantly, the fraction of the photo inside the perimeter of the window 105 includes the region of the eyes of the portrait picture 110, together with the encrypted graphic 111. This the human user to check that no tampering has been performed on the region of the eyes, which is the most information-conveying region of portrait pictures.

[0054] In a further embodiment, the optical filter is present in a second carrier, displaceable relative to the card that constitutes a first carrier, permanently linked to it or not. The filter can thus be placed on the rear face of the transparent window of the card on demand. In particular it can stick to the card at the point of identification to form a one piece structure.

[0055] This is illustrated shown on figures 7 to 9, where the card 200 has a portrait picture 210 with collocated encrypted graphics 211 on its front face 201 but does not have a filter on its rear face 202. The card 200 includes a transparent window 205 matching with the region of the eyes.

[0056] However, the card 200 is provided with a card case (or card holder) 300, the open face of which is shown on figure 8 and consisting essentially in a rear surface 302 in which a filter 320 is incorporated in a transparent window 305 of the rear surface 302. The place of the window and filter is adapted to, when the card 200 is placed inside the card holder, reveal the encrypted graphics 211 of the card for a user staring at the rear

surface 302 of the card case 300.

[0057] In another embodiment illustrated on figure 10, the card 400 has a portrait picture 410 with collocated encrypted graphics 411 on its front face 401 but does not have a filter on its rear surface 402. The card 400 includes a transparent window 405 matching with the region of the eyes, traversing the carrier 400 and including an incorporated optical filter 420 adapted to reveal the encrypted graphics 411.

[0058] The invention also relates to a method of personalizing a non-personalized carrier. Referring to figure 12, in a non-limiting embodiment, the front surface 101 of a card 100 constituting a carrier for an identity card is, in a preliminary manufacturing step S1, designed or prepared to be ready to be personalized with a portrait photo of an individual. The design can include frames, lines and labels defining a personalization area 101' for the information personal to the bearer, The care 100 with its personalization area 101' is a semi-finished carrier that is illustrated on figure 11, having a front surface 101 and a personalization surface 101'. Figure 11 shows the frame for the portrait photo, prepared on the personalization area 101', and covering the window 105. No portrait photo is present at that stage. The card is delivered to the granting authority, upon a step S2 of delivery.

[0059] Thanks to the prepared personalization surface 101', it is easy for an operator of the granting authority performing a step S3 of personalizing the document for a given bearer to know at least the orientation he has to give to the card 100 when printing the portrait photo 110, and the distance from the edges of the card at which such photo 110 must be printed. This enables the region of the eyes of the photo to match with the transparent window 105 or 405, or with the transparent windows 205 and 305.

[0060] The encrypted graphics 111 and the portrait photo 110 are deposited simultaneously, but depending on the coding and printing methods used, the encrypted graphics could be present before the printing of the photo or be deposited later.

[0061] The invention has been described with the Hidden Indicia encryption algorithm, but the person of the art can readily reproduce the invention with alternative encryption modes, such as any Scrambled Indicia® algorithm, or polarizing filters, color filters, interference filters, line/dots grids, holograms or diffraction gratings.

[0062] Also, instead of a portrait picture, the critical visual element that is protected against tampering by the present invention can be a fingerprint.

[0063] The data carrier could be, in an alternative embodiment, a security document such as a paper passport with a carrier comprising transparent or translucent paper forming a window traversing the carrier or a passport having a polycarbonate page insert as a page of the passport,

[0064] It can be appreciated that various modifications and alterations may be made to the embodiments of the invention without departing from its spirit. Although individual embodiments are described it is to be understood that the invention can include combinations of the embodiments discussed.

Claims

1. A data carrier (100; 200; 400) having first and second faces, a first face (101) of said data carrier having an area (101') for printed information on the first face (101), with there being a window (105; 205; 405) extending between the first face (101) and the second face (102) of the carrier, **characterized in that** the area (101') for printed information covers at least a part of said window (105; 205; 405).

2. A data carrier (100) according to claim 1, further including an optical filter (120) for revealing encrypted graphics, said filter (120) covering at least a part of a face (102') of the window (105) within the second face (102) of the data carrier, said filter being opposite the area (101') for printed information in the first face (101) of the data carrier and integral on the carrier (100).

3. A data carrier according to any of claims 1 to 3, further including an optical filter (120) for revealing encrypted graphics wherein the filter (120) and the carrier can be stuck together to form a one piece structure with the filter covering at least a part of a face (102') of the window (105) within the second face (102) of the carrier, said filter being stuck opposite the area (101') for printed information in the first face (101) of the carrier.

4. A data carrier (100; 200; 400) according to any of claims 1 to 3, wherein the area (101') for printed information is a personalization area.

5. A data carrier (100; 200; 400) according to any of claims 1 to 3, the personalization area (101') is a personalization area (101') for a portrait photograph covering at least a part of the window (105; 205; 405).

6. A data carrier (100; 200; 400) according to claim 5, wherein said window (105; 205; 405) is positioned in a region of the personalization area (101') that corresponds to the upper part of a portrait photograph of a face of a bearer of the carrier so the eyes of the bearer in said photograph are visible when viewing the carrier from the second face (102; 202; 402) of the carrier.

7. A data carrier (100; 200; 400) according to any of claims 1 to 6, wherein the carrier is a carrier for an identity card.

8. A data carrier according to any of claims 1 to 6,

wherein the carrier includes a passport booklet.

9. A data carrier (100; 200; 400) according to any of claims 1 to 8, including visual information (110; 210; 410) and encrypted graphics (111; 211; 411) collocated on said area (101') for printed information on the window (105; 205; 405).

10. A data carrier according to claim 9, wherein the encrypted graphics (111; 211; 411) is encrypted with a scrambled indicia encryption code.

11. A data carrier according claim 9 or 10, wherein the visual information is seen clear when viewed from the first face (101) and the encrypted graphics (111; 211; 411) is seen from the second face (102).

12. A of personalizing (S3) for a particular individual a data carrier, comprising collocating visual information (110; 210; and encrypted graphics (111; 211; 411) on a carrier (100; 200; 400), **characterized in that** at least some part of the collocating is performed over a window (105; 205; 405) traversing the carrier.

13. A method of personalizing according to claim 12, comprising collocating the region of the eyes of a portrait photo (110; 210; 410) and encrypted graphics (111; 211; 411) on said window (105; 205; 405).

14. A data carrier including security features obtained by the method of claim 12 or claim 13.

15. A method of control of the identity of an individual bearing a data carrier according to any of claims 9 to 11 or claim 14, comprising observing information personal to the bearer on a first face (101) of the document and checking the presence of an encrypted graphics (111) by observing the second face of the document.

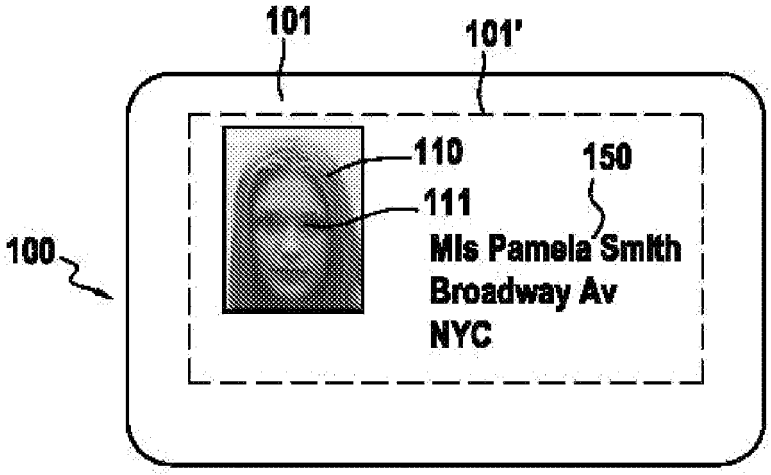
101
101'
110
111
150
100
Mls Pamela Smith
Broadway Av
NYC

FIG.1

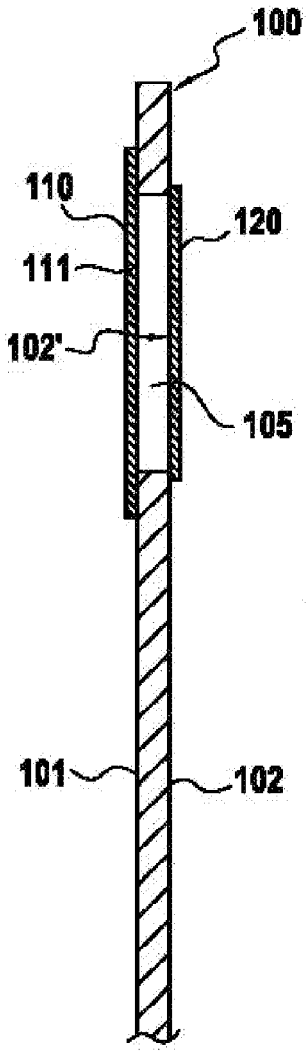
100
110
120
111
102'
105
101
102

FIG.2

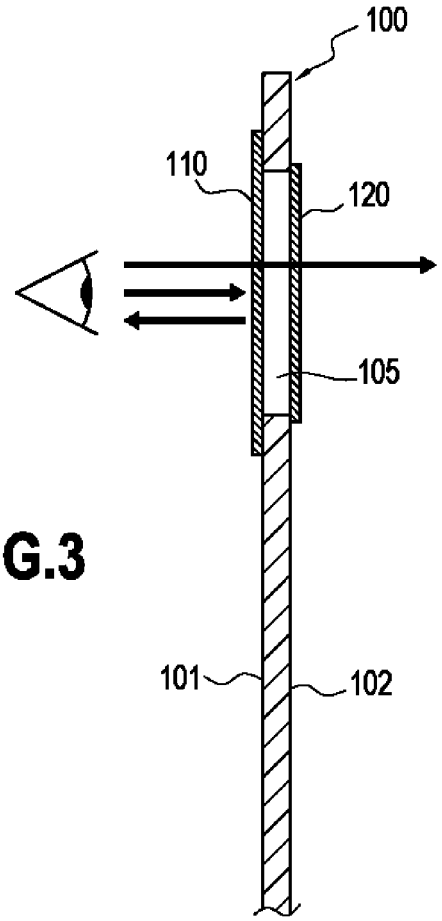

FIG.3

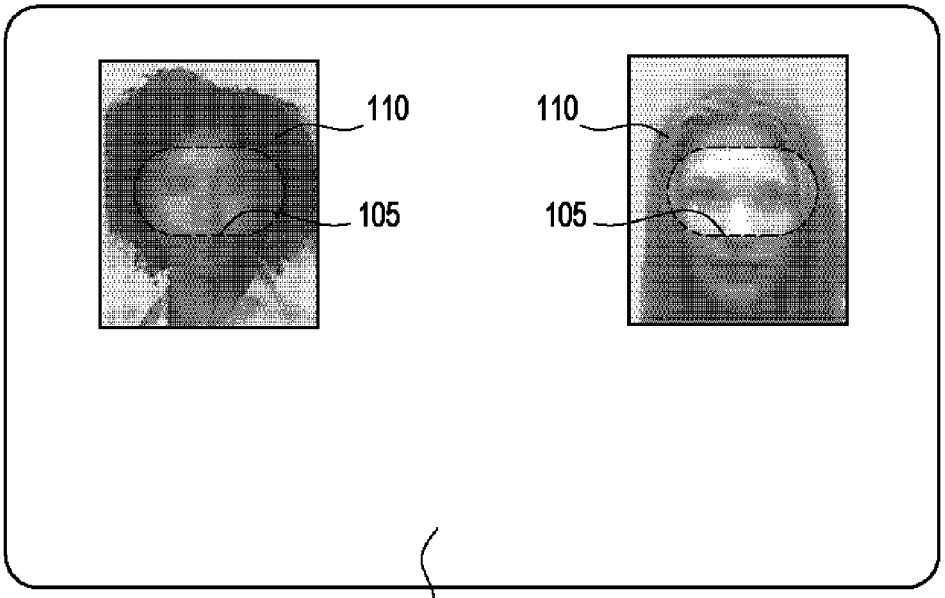

FIG.4

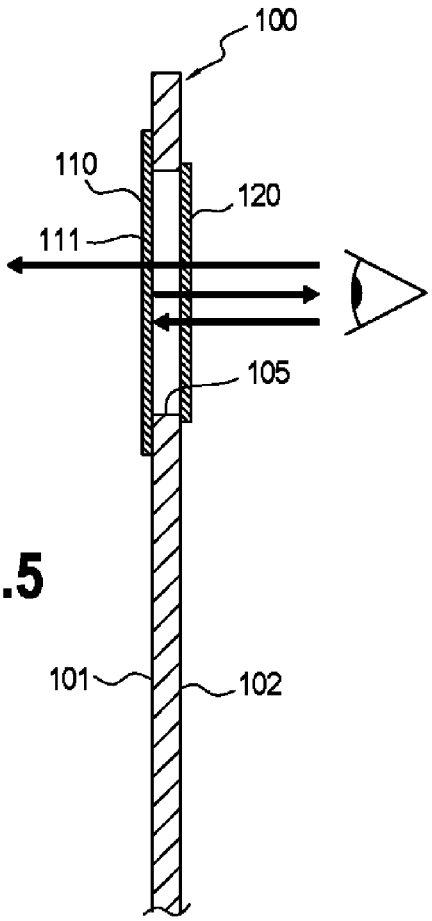

FIG.5

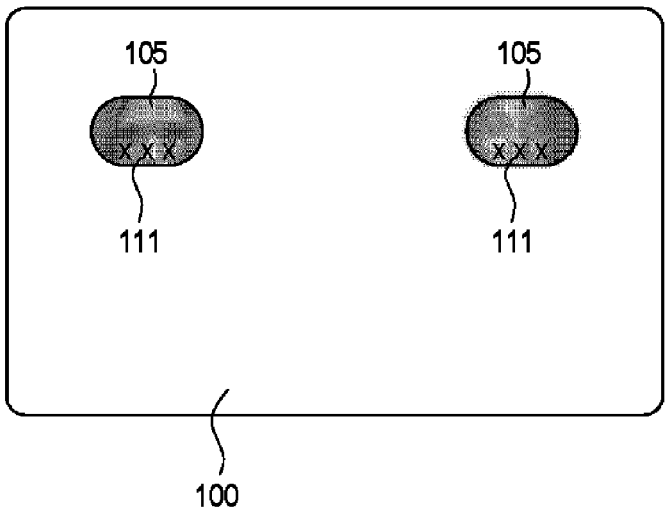

FIG.6

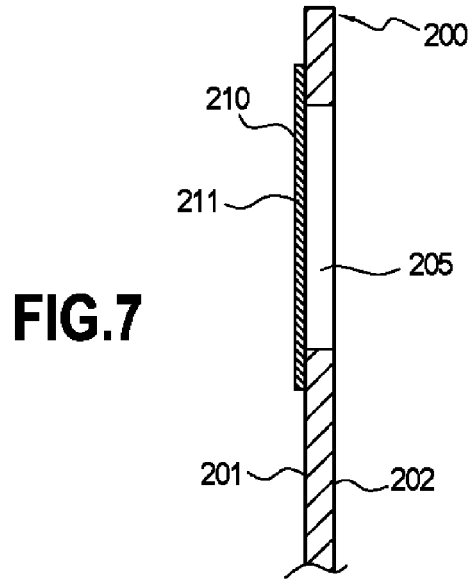

FIG.7

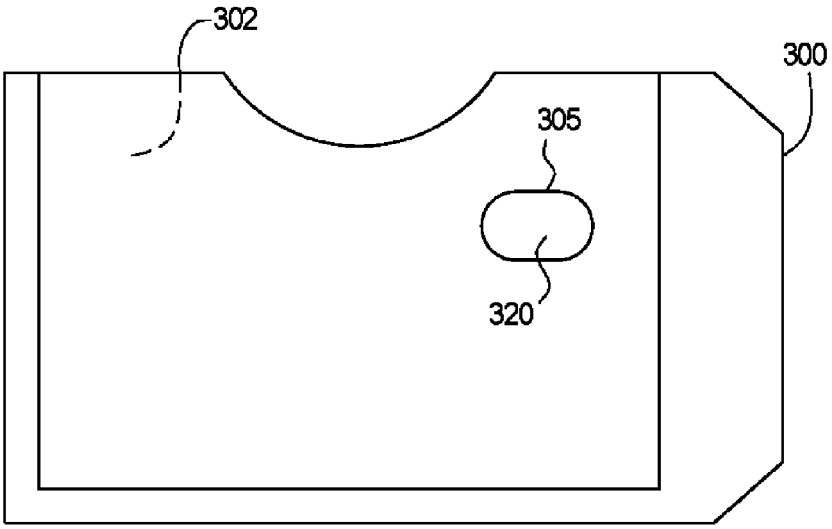

FIG.8

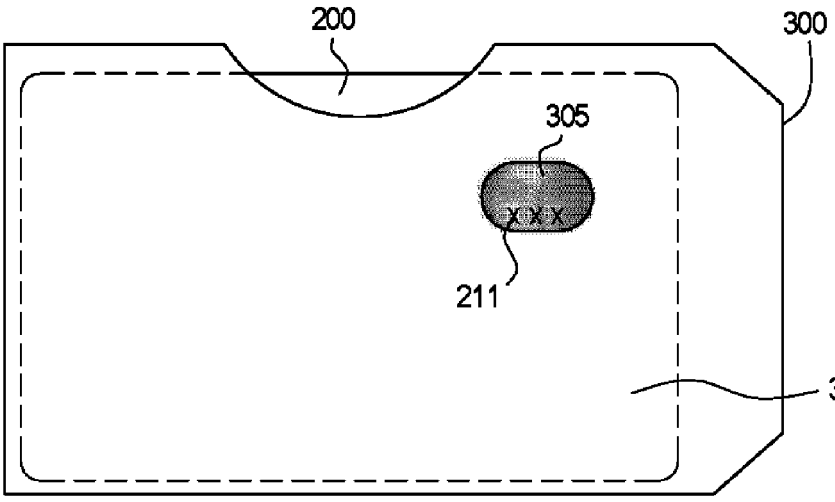

FIG.9

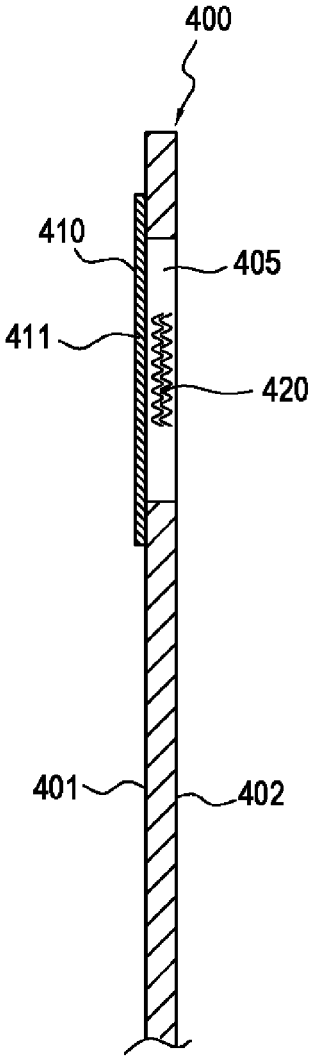

FIG.10

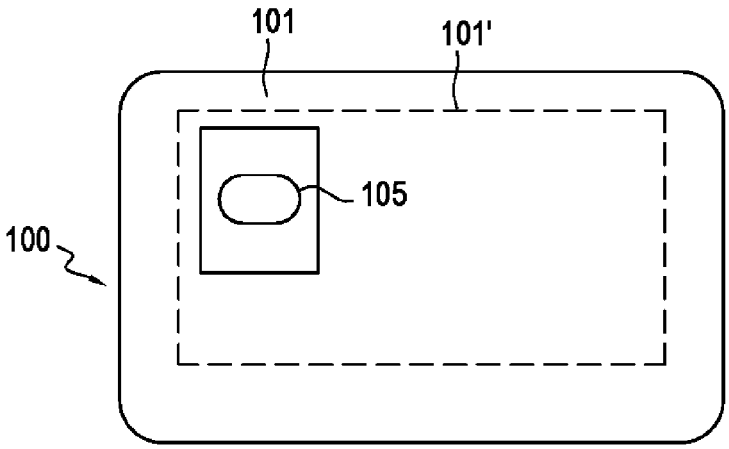

FIG.11

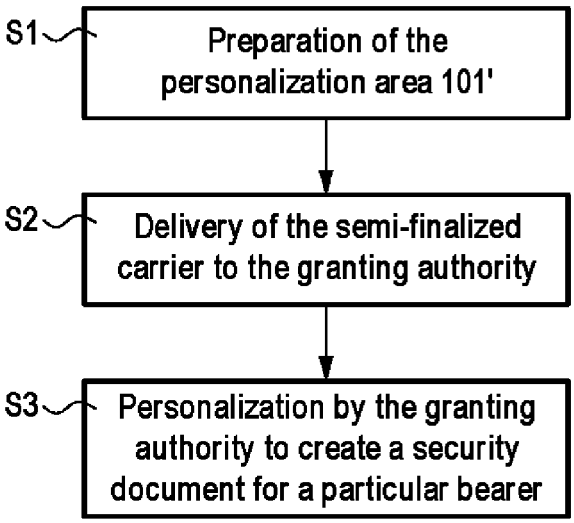

FIG.12

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 11 30 5815

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 2 199 099 A1 (GEMALTO OY [FI]) 23 June 2010 (2010-06-23) * EPO & WPI Abstracts; paragraphs [0008] - [0010], [0015], [0016], [0021] - [0028]; claim 10; figures 1-2 *	1-15	INV. B42D15/10 B41M3/14
X	EP 1 935 663 A1 (SETEC OY [FI]) 25 June 2008 (2008-06-25) * Abs &WPI Abs; paragraph [0012] *	1-15	
X	EP 1 698 485 A2 (CANADIAN BANK NOTE CO LTD [CA]) 6 September 2006 (2006-09-06) * EPO & WPI Abstracts; paragraphs [0008], [0009], [0021]; figures 1-6 *	1,12	
X	EP 2 275 279 A1 (OBERTHUR TECHNOLOGIES [FR]) 19 January 2011 (2011-01-19) * abstract; figure 3 *	1,12	TECHNICAL FIELDS SEARCHED (IPC)
A	US 2006/290136 A1 (ALASIA ALFRED V [US] ET AL) 28 December 2006 (2006-12-28)	1-15	B42D B41M

1 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 November 2011	Callan, Feargel

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 11 30 5815

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-11-2011

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2199099 A1	23-06-2010	EP 2199099 A1	23-06-2010
		EP 2373493 A1	12-10-2011
		WO 2010070084 A1	24-06-2010
EP 1935663 A1	25-06-2008	CA 2672847 A1	26-06-2008
		EP 1935663 A1	25-06-2008
		EP 2114690 A2	11-11-2009
		JP 2010514084 A	30-04-2010
		KR 20090125238 A	04-12-2009
		US 2010047488 A1	25-02-2010
		WO 2008075164 A2	26-06-2008
EP 1698485 A2	06-09-2006	AU 2006200935 A1	21-09-2006
		CA 2538444 A1	04-09-2006
		EP 1698485 A2	06-09-2006
		NZ 545680 A	27-07-2007
		US 2006197337 A1	07-09-2006
EP 2275279 A1	19-01-2011	BR PI1001936 A2	05-07-2011
		EP 2275279 A1	19-01-2011
		FR 2947211 A1	31-12-2010
US 2006290136 A1	28-12-2006	AU 2007284106 A1	21-02-2008
		CA 2661185 A1	21-02-2008
		EP 1889727 A2	20-02-2008
		IL 185364 A	30-06-2011
		US 2006290136 A1	28-12-2006
		WO 2008021825 A2	21-02-2008

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- FR 2918311 **[0011]**
- EP 1889727 A **[0011]**
- FR 2947211 **[0013]**