

(51) International Patent Classification:
G07D 7/00 (2006.01)

(21) International Application Number: PCT/EP2010/062340

(22) **International Filing Date:** 24 August 2010 (24.08.2010)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
09305786.7 25 August 2009 (25.08.2009) EP

(71) **Applicant** (*for all designated States except US*):
GEMATLO SA [FR/FR]; Intellectual Property Dpt, 6
rue de la Verrerie, F-92190 Meudon (FR).

(72) Inventors; and

(75) **Inventors/Applicants (for US only): JOFFRAY, Olivier** [FR/FR]; c/o GEMALTO SA, Intellectual Property Dpt, 6 rue de la Verrerie, F-92197 Meudon Cedex (FR). **MALLET, Chrystele** [FR/FR]; c/o GEMALTO SA, Intellectual Property Dpt, 6 rue de la Verrerie, F-92197 Meudon Cedex (FR).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND DEVICE FOR VERIFYING SECURE DOCUMENTS

(57) Abstract: The present invention provides a method for verifying a secure document (2) of a bearer, said secure document (2) comprising identity information and an embedded electronic component comprising means for storing identity information of a bearer, said method comprising the following steps: a)selecting an area on the document, b)capturing an image of the selected area, c)processing the captured image to obtain identity information, d)extracting identity information stored in said embedded chip, e)comparing identity information extracted from said captured image and identity information stored in the electronic chip, f)signaling the counterfeiting of the secure document if step d) fails.

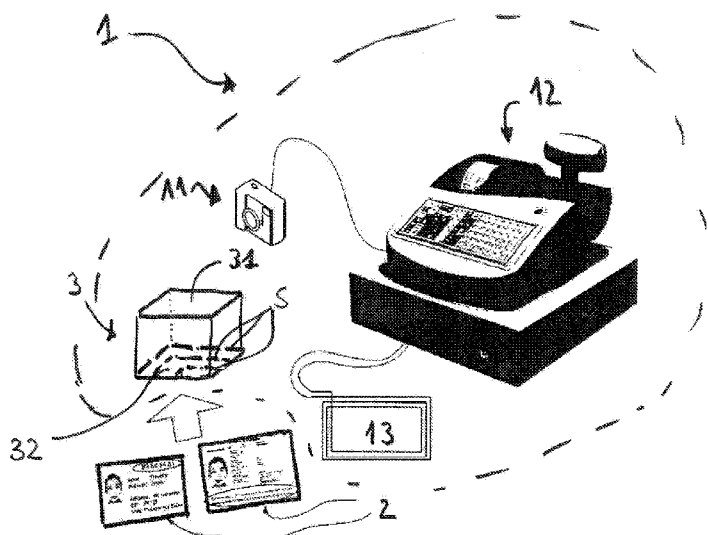


Fig 1

METHOD AND DEVICE FOR VERIFYING SECURE DOCUMENTS

5 The invention relates to the field of authentication of documents and in particular, relates to a method and a device for verifying the authenticity of secure documents.

10 Documents such as ID cards, passports, driving licenses, resident permits, and other types of identification documents are delivered to allow identification of the bearer. These documents contain information about the name, age, date of birth, address, photography, etc. of the bearer, and allow a controller his identification.

15 These identification documents have been secured in order to not to be easily reproduced or falsified. To avoid counterfeiting, these secure documents have been manufactured in specific ways and may comprise for example digital watermarks, specific layers or core layers with specific printing, such as a printed pattern in specific
20 areas of the document, etc. The verification of the integrity of the secure document is often made by a controller by screening the identification documents, using information located in the document identification.

25 Another way to verify the authentication is the use of an embedded electronic chip. Identification documents such as passports

2

are for example already equipped with such an electronic chip. The embedded electronic chip comprises stored information related to the bearer which can be the same information that can be seen on the document. Biometric information associated with the owner of the secure document such as fingerprint information, have been added to the secure element. For such identification document, a controller uses a specific electronic device. Current electronic devices are used at country frontiers and are dedicated to verify a single electronic document: the electronic passport. Future generation of electronic document will use different technologies that are not compatible with ePassport readers. Many type of identity electronic documents will be used in a near future such as national ID cards, health card,..., and the format of these documents will change depending on the issuer choices. Current electronic devices are not ready to accept these new documents' format.

Next generation of ID cards, resident permits, driving licenses will embed an electronic component such as a chip as some current passports. Then there is a real need to provide a electronic device and a method suitable for securely authenticate any secure documents which comprise identity information and which are simpler and cheaper, and which are not easily hacked or corrupted as falsification is growing up.

It is an object of the invention to provide a method adapted to enhance the security for every type of identification document.

3

In this purpose, the invention provides a method for verifying a secure document of a bearer, said secure document comprising identity information and an embedded electronic component comprising means for storing identity information of a bearer, said method

5 comprising the following steps:

- a) selecting an area on the document,
- b) capturing an image of the selected area,
- c) processing the captured image to obtain identity information,
- 10 d) extracting identity information stored in said embedded chip,
- e) comparing identity information extracted from said captured image and identity information stored in the electronic chip,
- 15 f) signaling the counterfeiting of the secure document if step d) fails.

According to one aspect of the invention,

- the method may comprise using an image capturing device;
- 20 - the step a) may consist in zooming on said area with the image capturing device;
- it may comprise using a machine readable zone (MRZ) as selected area;
- it may comprise using a processing device, adapted to
- 25 process the captured image;

4

- the processing device may treat the captured image using optical character recognition process, and using cryptographic application;
- it may comprise a step of establishing a communication with a remote server suitable to manage partially or totally the communication with the secure document;
- the remote server may provide feedback regarding the verification of the secure document.

5

10

It is a further object of the invention to provide an electronic device that operate the method and which is adapted to enhance the security for every type of identification document as well.

15

In this purpose, the invention provides an electronic device for verifying a secure document, said secure document comprising identity information and an embedded electronic component comprising means for storing identity information of a bearer, said electronic device comprising an image capturing device suitable for capturing an image of an area from said secure document, a processing device for processing the captured image, means for establishing a contactless communication (13) with the secure document.

20

According to one aspect of the invention,

- the image capturing device may be a camera;

5

- the image capture device may be integrated to the processing device;

- the electronic device may be a mobile phone;

- the processing device may be a cash register;

5

- the electronic device may comprise a receiving device adapted to receive said secure document so as to position the area of the secure document to be captured;

- the receiving device may be a box with an upper face and a below face under the upper face, the below face comprising

10

- different stops so as to position the secure document.

This method and this electronic device are advantageously applicable for all government document verification applications.

15

The invention is now described, by way of example, with reference to the accompanying drawings. The specific nature of the following description should not be construed as limiting in any way the broad nature of this summary.

20

In order that the manner in which the above recited and other advantages and features of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference.

6

Notwithstanding any other forms that may fall within the scope of the present invention, preferred forms of the invention will now be described, by way of example only, with reference to the accompanying drawing in which:

5 **FIG.1** schematically shows an embodiment of an electronic device for verifying a secure document device according to the invention.

The present invention may be understood according to the detailed description provided herein.

10 Shown in Fig.1 is an electronic device 1 for verifying that a secure document 2 is not counterfeited, and more precisely when the secure document 2 is a secure electronic identity document.

In the present invention, a secure identity document is a secure document which comprises identity information. It may be an
15 electronic identity document such as an electronic passport, or an electronic identity card, etc.

This electronic identity document is made of a standard paper passport and comprises text data about the bearer such as his name, his date of birth, and other type of data such as his photography, or
20 his signature.

The electronic identity document also comprises an embedded electronic component not represented in figure 1. This electronic component, such as a chip, stores identity information of the bearer

7

and can not be removed from the electronic identity document 2 without damaging it.

The chip may be addressed through a contact or a contactless interface (ISO 7816-x or ISO 14443-x standard respectively, but not
5 exclusively).

The electronic identity document 2 also comprises a machine readable bearer data in an area usually called machine readable zone or MRZ which can be read with a dedicated device as it will be
10 described further. The MRZ comprises identification information of the bearer.

A method according to the invention for verifying that the secure document is not counterfeited, is to compare the information data stored in the electronic document with the identity information
15 printed on the document. For this, the method comprises a step which consists in an extraction of the identification information printed on the document and a step which consists in an extraction of the identification information stored in the chip. To access the information available in the chip, the MRZ has to be captured, and
20 the data extracted from it are used to establish a link between the electronic device 1 and the document 2.

For processing the step which consists in the extraction of the information included in the MRZ, the electronic device 1 comprises an
25 image capture device 11, means for processing 12 the captured image, also called a processing device 12 and means for establishing 13 a

8

communication with the secure identity document 2. In the following description, the secure identity document is a secure identity card 2.

5 The image capture device 11 comprises means for selecting an area 10 from the secure identity document 2, means for capturing and storing a selected image stemming from said selected area 10, which is the MRZ. These different means are not represented in Fig.1 and are suitable for capturing the MRZ in high resolution in order for the selected area to be well readable and well exploitable by the 10 means for processing 12, such as a zoom lens, etc.

According to the invention, in a first embodiment, the image capturing device 11 is a camera, which is suitable for taking the picture of the secure identity document 2 in a whole or by directly 15 selecting the MRZ, for example by zooming onto the MRZ.

It will be well understood that this image capturing device is not a limited example, and every device suitable for capturing an image is available. Then the image capturing device may be for 20 example a bar code electronic device 1 if the capturing image includes bar-code information.

Once the image is selected and captured by the controller, it is stored by the image capture device 11, for example in a memory 25 card. The stored image is then sent to the processing device 12.

Optionally, the selected and captured image is directly stored in the processing device 12.

5 The processing device 12 comprises means for treating the captured image, for example a computer unit which embeds a software for the extraction of information data from the MRZ.

For doing so, an optical character recognition (OCR) algorithm is for example used for the extraction of the identification information of the bearer. This algorithm permits the extraction of
10 text and symbols from an image using computer means. Classically, a printed or handwritten text, or a digital picture is scanned from the secure identity document 2.

The algorithm depends on the nature of the selected image. Then if the MRZ includes bar-code information, the extraction of the
15 identity information is made with an appropriate algorithm.

The means for processing the captured image may further includes stemming imaging application in order to facilitate the extraction of identity information from the MRZ.

The extraction may be automatically launched by the processing
20 device 12 as soon as it detects that an image has been stored or may be launched by the controller.

At this stage, the controller has captured the MRZ from the secure identity card 2 with the image capture device 11 and the
25 identification information has been extracted from the MRZ by the processing device 12.

10

For the step which consists in the extraction of the identification information stored in the chip, the electronic device 1 has to establish a communication with the chip embedded in the secure identity card 2.

5 As represented in Fig.1, the communication between the electronic device 1 and the secure identity document 2 is a contactless communication and the means for establishing the communication 13 comprise an antenna. The electronic device 1 embeds a so called CLF (Contactless Front End) which is constituted by an RF
10 proximity antenna and a Near Field Contactless controller.

The reading of the electronic component is then made in contactless mode such as define in ISO standard 14443.

In order to avoid the secure identity document 2 being read without the bearer agreement, a secure messaging is used. The secure
15 messaging protects electronic data exchange from disclosure or modification. It comprises the calculation of cryptographic keys on both the processing device 12 and the chip embedded in the secure identity card 2, said keys being based on information known by both. The calculation of the encrypted keys is for example made in a
20 microcontroller of the processing device 12. These cryptographic keys are loaded in the chip during the personalization and can be recalculated from the MRZ.

In fact, until very recently, the electronic device 1 had to embed a secret (such as a master key) to open a secure channel between the
25 electronic device 1 and the identity card 2, thus becoming a very sensitive device. In order to avoid this drawback, the use of

11

algorithm requiring the electronic device 1 to hold a secret is replaced by a mechanism called PBM (Password Based Mechanism) that does not require any secret in the electronic device 1 to open a secure channel between the identity card 2 and the electronic device

5 1. After the MRZ is captured and treated by the processing device, both the electronic device 1 and the chip share the same information. Other algorithms such as the BAC or equivalent algorithm may also be used instead of a PBM. The session keys are the output of the PBM and are shared by both the identity card 2 and the electronic device 1.

10 By using the session keys, a secure channel between the card and the electronic device 1 is established allowing the exchanges to be protected.

It will be understood that the identification information included in the identity card 2 used as input to PBM may

15 alternatively be a bar-code, a printed digital code, or a PIN, entered by the bearer on the electronic device 1 for example thanks to a keyboard. In this case, the electronic device 1 comprises a keyboard in order to enter the card bearer PIN or password, said PIN or password being used as the input to the PBM.

20

Once a secure session is established with the chip, the processing device 12 extracts identification information stored in the chip.

The next step is then the comparison of the data inside the

25 chip with the data captured from the secure identity card 2.

12

The electronic device 1 sends a signal to the controller at the end of the verification. If these data are matching, a signal for example a green light, or a special sound, informs the controller that the identity card is not counterfeited.

5 It will be understood that the nature of the signal is not a limited example.

10 In accordance with another embodiment, the processing device 12 is a handset such as a mobile phone, which comprises an antenna for the NFC contactless communication and a smart card.

 In this case, the calculation of the encrypted keys can be made optionally by the smart card (e.g. SIM or UICC) in order to fasten the process.

15 In accordance with another embodiment, in the electronic device 1, the image capture device 1 is integrated to the processing device 12.

20 It will be understood that all these embodiments can be combined and are not limited examples. Then according to an embodiment of the invention, the electronic device is a mobile phone comprising an image capturing device 12, a smart card, a microcontroller, etc. The image capturing device 11 is able to take picture, or to dynamically capture pictures if a video mode is used,
25 to parse said picture(s) in order to extract the information to be

13

used as the input of the PBM, or other information such as the name of the document bearer.

The handset may embed software applications which are able to complete cryptographic calculations in order to establish a secure
5 channel with the electronic document.

Optionally, the handset allows the controller to identify on a picture an area to parse by zooming and/or surrounding information on said picture by an external action, for example with a finger on the screen.

10

The calculation of session keys can be made for example by the microcontroller of the mobile phone or by the smart card. The mobile phone can then embed a digital camera.

Such a mobile phone embeds a microcontroller running a software
15 addressing the services provided by the device such as phone call, taking picture, sending SMS or MMS, etc. Many mobile phones' manufacturers also provide a SDK (Software Development Kit) that permits to develop applications such as games, unit convertor, etc. These SDK also allow to address the camera and / or to work on
20 picture taken by the camera.

According to another embodiment, the electronic device 1 for verifying the secure identity document comprises a receiving device 3
suitable for receiving the secure identity document. The receiving
25 device 3 is suitable for receiving secure documents with different

14

formats in order to facilitate the caption of MRZ or of other information on the printed card. Each stop may be related to the.

In an embodiment, the receiving device 3 is a box with an upper face 31 and a below face 32, under the upper face 31. The below face
5 32 comprises different stops S such as abutments, designed in an interior face and which are able to position secure documents 2.

The upper face 31 may also comprises a positioning element that can be placed such that the relative position of the image capture device 11 and of the secure document 2 facilitate capturing an image
10 of the secure document 2.

This device 3 allows maintaining the identity card 2 in order to facilitate the caption of the MRZ.

In another embodiment, the electronic device 1 establishes a
15 communication with a remoter server. The electronic device has a data connection to the remote server (not represented) which can manage partially or totally the communication with the secure identity document 2.

The remote server uses the electronic device's characteristics
20 as an extension to its own system (e.g. piloting the camera, sending APDU ...) and provides feedback regarding the verification of the secure identity document 2.

The remote server is able to update the software of the processing device 12 and/or data for the secure identity document
25 verification, for example, when a picture parsing software does not know how the electronic document is organized (e.g. foreign country

15

electronic document). In this case, the controller may indicate the country from which the secure document is issued to the electronic device 1. If the country is unknown to the electronic device 1, it connects to the remote server to get instructions or a software
5 update for verifying the secure document 2.

This method can be advantageously being used by a storekeeper who uses a cash register as a processing device and a bar code electronic device or an image capture device connected to the register cash in order to verify that a secure document presented by
10 a buyer is not counterfeited. The cash register may also integrate the image capturing device 11.

This method and this electronic are able to enhance the security for every type of identification document and can be used by each person who want to verify that a secure document is not
15 counterfeited.

16
CLAIMS

1) A method for verifying a secure document (2) of a bearer, said
secure document (2) comprising identity information and an
5 embedded electronic component comprising means for storing
identity information of a bearer, said method comprising the
following steps:

- a) selecting an area on the document,
- b) capturing an image of the selected area,
- 10 c) processing the captured image to obtain identity
information,
- d) extracting identity information stored in said
embedded chip,
- e) comparing identity information extracted from said
15 captured image and identity information stored in
the electronic chip,
- f) signaling the counterfeiting of the secure document
if step d) fails.

20 2) A method according to claim 1, characterized in that it comprises
using an image capturing device (11).

3) A method according to claim 2, characterized in that step a)
consists in zooming on said area with the image capturing device
25 (11).

17

4) A method according to claim 3, characterized in that it comprises using a machine readable zone (MRZ) as selected area.

5) A method according to one of the preceding claims, characterized in that it comprises using a processing device (12), adapted to process the captured image.

5

10

6) A method according to claim 6, characterized in that the processing device (12) treats the captured image using optical character recognition process, and using cryptographic application.

15

7) A method according to one of the preceding claims, characterized in that it comprises a step of establishing a communication with a remote server suitable to manage partially or totally the communication with the secure document (2).

20

8) A method according to claim 7, characterized in that the remote server provides feedback regarding the verification of the secure document (2).

25

9) An electronic device (1) for verifying a secure document (2), said secure document (2) comprising identity information and an embedded electronic component comprising means for storing identity information of a bearer, said electronic device (1) comprising:

18

a. an image capturing device (11) suitable for capturing an image of an area from said secure document (2),

b. a processing device (12) for processing the captured image,

5 c. means for establishing a contactless communication (13) with the secure document (2).

10) An electronic device (1) according to claim 11, characterized in that the image capturing device (11) is a camera.

10

11) An electronic device (1) according to claim 10 to 11, characterized in that the image capture device (11) is integrated to the processing device (12).

15 12) An electronic device (1) according to claim 9 to 11, characterized in that the electronic device (1) is a mobile phone.

13) An electronic device (1) according to claim 9 to 11, characterized in that the processing device (12) is a cash
20 register.

14) An electronic device (1) according to claim 9 to 13, characterized in that it comprises a receiving device (3) adapted to receive said secure document (2) so as to position the area of
25 the secure document (2) to be captured.

19

15) An electronic device (1) according to claim 14, characterized
in that the receiving device (3) is a box with an upper face (31)
and a below face (32) under the upper face (31), the below face
(32) comprising different stops (S) so as to position the secure
5 document (2).

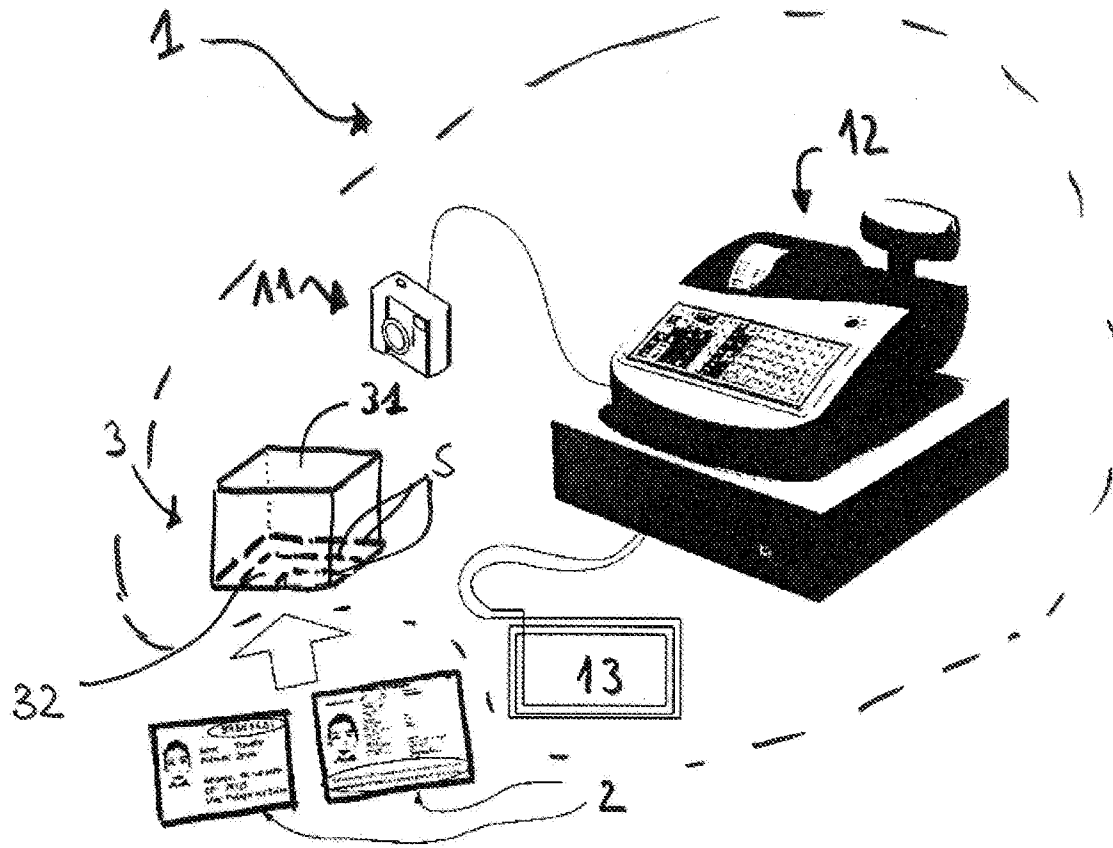


Fig 1

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/062340

A. CLASSIFICATION OF SUBJECT MATTER

INV. G07D7/00

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/108412 A1 (OKAMOTO ET AL.) 25 May 2006 (2006-05-25) paragraphs [0043] - [0045], [0050] - [0060], [0067], [0070]; figures 1-6 -----	1-15
X	EP 2 003 622 A (SIEMENS AG ÖSTERREICH) 17 December 2008 (2008-12-17) paragraphs [0004], [0017], [0022], [0023]; figures -----	1-15
X	DE 197 34 507 A1 (SIEMENS AG) 11 February 1999 (1999-02-11) column 2, line 44 - column 3, line 51; figure ----- -/--	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

16 November 2010

Date of mailing of the international search report

30/11/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Neville, David

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/062340

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/192850 A1 (COWBURN) 16 August 2007 (2007-08-16) paragraphs [0098] - [0101], [0120], [0121], [0127] - [0136], [0151]; figures 4,7-13 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2010/062340

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006108412 A1	25-05-2006	NONE	
EP 2003622 A	17-12-2008	DE 102007023063 A1	20-11-2008
DE 19734507 A1	11-02-1999	AT 225542 T	15-10-2002
		BR 9811871 A	15-08-2000
		CN 1266521 A	13-09-2000
		WO 9908230 A2	18-02-1999
		EP 1010136 A2	21-06-2000
		ES 2185217 T3	16-04-2003
		JP 2001512873 T	28-08-2001
		RU 2222049 C2	20-01-2004
		US 6615351 B1	02-09-2003
US 2007192850 A1	16-08-2007	AR 048090 A1	29-03-2006
		AU 2005220385 A1	22-09-2005
		BR PI0508631 A	07-08-2007
		CA 2559283 A1	22-09-2005
		CN 1969289 A	23-05-2007
		EP 1730675 A1	13-12-2006
		EP 2128790 A2	02-12-2009
		EP 2131315 A2	09-12-2009
		EP 2131309 A2	09-12-2009
		EP 2131310 A2	09-12-2009
		WO 2005088533 A1	22-09-2005
		HK 1077113 A1	20-10-2006
		JP 2007529068 T	18-10-2007
		JP 2010079917 A	08-04-2010
		KR 20070024511 A	02-03-2007
		RU 2385492 C2	27-03-2010
		SG 151277 A1	30-04-2009