(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 November 2005 (10.11.2005)

PCT

(10) International Publication Number
WO 2005/106807 A1

(51) International Patent Classification[7]: G07D 7/00

(21) International Application Number:
PCT/GB2005/001627

(22) International Filing Date: 28 April 2005 (28.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0409429.8 28 April 2004 (28.04.2004) GB

(71) Applicant *(for all designated States except US)*: **ADVANCED ANALYSIS AND INTEGRATION LIMITED** [GB/GB].

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CORRY, John, Joseph** [GB/GB]; 24 Newlands Avenue, Cheadle Hulme, Cheshire SK8 6ND (GB). **MCNEIGHT, David, Leslie** [GB/GB]; Hill Dickinson, 50 Fountain Street, Manchester M2 2AS (GB).

(74) Agent: **MCNEIGHT, David, Leslie**; Hill Dickinson, 50 Fountain Street, Manchester M2 2AS (GB).

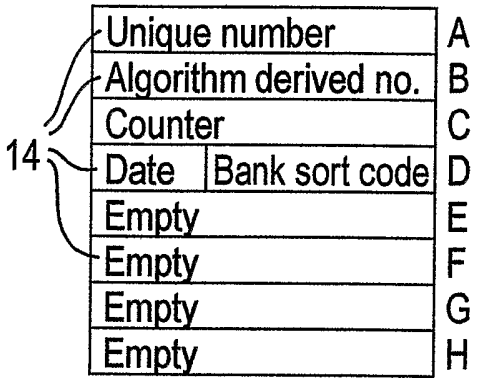
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: AUTHENTICATION OF RE-PRESENTABLE ITEMS




(57) Abstract: A system for authenticating re-presentable items, such as currency notes and passports, comprises applying to each item a unique code, reading the code on presentation, and checking the code against a database, characterised in that at each check, the code is altered.

WO 2005/106807 A1

# Authentication of Re-presentable Items

This invention relates to the authentication of re-presentable items, such as currency notes which are circulated, passports and identity cards, which are presented on multiple occasions on crossing borders or to obtain access to restricted places or benefits.

Security printing - expensive, fine detail printing, on special paper, with watermarks, metal stripes, holograms and other artefacts - has long been relied upon to deter forgery. Technology available to counterfeiters make it easier to produce passable, if not, indeed, indistinguishable copies of genuine articles.

In the case of currency notes, the greatest threat comes not from back street operators with colour printers, but from well-financed, highly skilled organisations, working on an altogether larger scale.

It has recently been proposed to use Radio Frequency Identification (RFID) tags on currency notes. These are microchips with a printed aerial mounted on a flexible film. Hitachi Europe Ltd, of Maidenhead, Berkshire, UK produces such a tag which is intended to be incorporated in currency notes. The microchips can be accessed by a read/write device which energises and controls the chip *via* the aerial. Such devices can be comprised in hand-held units or built into portals through which items are passed.

RFID tags are available with several data registers. Usually, one register has a manufacturer-assigned code, in the form of a binary number, which can be up to 64 bits long, each tag having a different code. There are more than $18 \times 10^{18}$ available numbers. The numbers are 'burnt in' to the register, which is to say, they cannot be altered or erased. It is understood that not all possible numbers are used, following, at least to some extent, the teaching of US4463250. The tag manufacturer will maintain a database of issued numbers, against which the number of any tag can be checked.

The ability to produce such tags is dependent on having, or having access to, a silicon foundry, which is an expensive plant. The idea behind protecting currency notes in this way appears to be that, even if the cost of setting up for the operation were not prohibitive, it would not be possible to generate the 64 bit numbers that would check out against the database.

If this is the reasoning, then it is flawed.

In the first place, the cost of setting up a silicon foundry would not be prohibitive to a counterfeiter intending to operate on a very large scale. A well-financed organisation could afford to do it, and would see the possibility of reaping rewards many times its investment. It is precisely such organisations, be they simply criminal, or be they intent on destabilising a currency for political ends, that are to be most feared.

Another flaw is the assumption that such an organisation could not produce tags with numbers that would check out against the genuine manufacturer's database.

It would be easy to produce tags with such numbers, simply by reading one number from a genuine note and producing all the spurious notes with that number.

US4463250 deals with that problem in this way, that each time a new number is read, it is checked against a database of already read numbers to check for repeats. There should not, of course, be any repeats. The production of millions of twenty dollar bills, all with the same number, would be rapidly detected. The smart counterfeiter will, having read US4463250, not produce all his notes bearing the same number. It is a simple matter to draw ten thousand, or a hundred thousand twenty dollar bills from a bank and copy the numbers into the chips - that would be facilitated by the ability to read the numbers by a read/write device, such being freely available, associated with a high speed note counting machine. The genuine notes can then be returned to the account from which they were withdrawn, the only cost being the loss of a day's bank interest.

Copies will be discovered, if the database check is set up to reveal repeats, of course, but only infrequently. And herein lies a major problem - with banknotes, which are in circulation, there would be no way to distinguish between a genuine note, presented twice, and a spurious note, presented after a genuine note had been presented.

The present invention solves that problem.

The invention comprises a system for authenticating re-presentable items, such as currency notes and passports, comprising applying to each item a unique code, reading the code on presentation, and checking the code against a database, characterised in that at each check, the code is altered.

This is capable of implementation using RFID tags. The unique codes can comprise the manufacturer-assigned, burnt-in 64 bit numbers plus another number in a writable register in the microchip. That other number would effectively constitute an incrementing counter. Suppose it starts at binary 00000 when a currency note, say, is issued; when it is first checked, it is changed to 00001, then 00010 and so on, the register size being chosen to comfortably cover the anticipated number of re-presentations during the life of the currency note or other item - indeed, filling up of this register can be used to signal the end of that useful life.

Even if this feature is known to the counterfeiter, so that he will be smart enough to realise that, on repayment into his (or some other) account of the twenty dollar bills from which he copied, their counters will be incremented, the counters on the genuine and the spurious bills will rapidly get out of synchronism, and it will be immediately apparent from the database checks that this is so, indicating a problem, which can be investigated.

As an aid to any such investigation, additional information can be written, at each check, to the tag. Such information may comprise the date and place of the check, the place being indicated, for example, by a bank sort code or a similar code for a currency exchange or a retail establishment. There may not, of course, be sufficient space on the

microchip to hold a complete history, but this information can be written over, being saved to the database.

Burnt in code can also, for example, hold information about the currency and denomination of a bank note, enabling note counting equipment also to count mixed currency and value notes, separating them into currency and denomination piles.

A further refinement involves the unique code itself, which can be backed up by an algorithm-generated check number, which will enable an on-the-spot check to be made, without reference to the database, to determine whether the unique code is an assigned number or not. Of course, if a counterfeiter has derived his code from a genuine item, the check number will also be copied. But, if not, passing the item through a checking device, which checks the algorithm-generated check number to see if it has been derived from the unique number by the proper algorithm, will give an instant indication, before the passer of the item has even left the bank, that a note is spurious.

Embodiments of system for authenticating re-presentable items according to the invention will now be described with reference to the accompanying drawings, in which:

Figure 1 shows an RFID tag;

Figure 2 is a diagrammatic illustration of the data registers on an RFID tag;

Figure 3 is a diagrammatic illustration of a possible hierarchical structure for a database connection to check stations;

Figure 4 is a diagrammatic illustration of a currency note reading, counting and sorting machine; and

Figure 5 is a diagrammatic illustration of a passport/identity card authenticating system.

The drawings illustrate a system for authenticating re-presentable items, such as currency notes, passports and credit and debit cards, comprising applying to each item a unique code, reading the code on presentation, and checking the code against a database, characterised in that at each check, the code is altered.

In the embodiments, the system is realised through the use of read/write RFID tags. One such is illustrated in Figure 1, and comprises a piece of flexible film 11 with a printed aerial 12 and a microchip 13. Typically, a tag suitable for use in the applications herein specifically described will have an area of 20mm x 20mm. The chip 13 will scarcely be thicker than the film, and will have a sub-millimetre dimension.

The chips 13 typically have eight data registers 14, of which at least one, Register A, in Figure 2, will be 64 bits long. The number of different numbers that can be stored in such a register is in excess of $18 \times 10^{18}$, or eighteen million million million. This register

usually contains a unique code number, which is also contained in a database maintained by the chip manufacturer. The other registers, B – H, are empty, but writable.

Register B, in the example, is written to with a number derived from the Register A number by an algorithm. This is to give an instant check that the Register A number is a genuine number, without having to access the database. The algorithm will, of course, be a closely guarded secret, that cannot be deduced even by examining a lot of tags - a public/private key encryption technique can give such security, and provide other benefits, as will be explained below.

Register C is used as an incremental counter. Suppose a banknote, say, were to have an expected life involving no more than 1000 transactions, this would need to be a nine but register. It would initially contain the number 00000000000; each time the note passed through a checkpoint, this counter would be incremented by 1. So the unique code would be contained in Registers A, B and C, and would change by virtue of the number in Register C changing.

Register D can contain an indication of the date and place of the last check, represented here as a bank sort code or a code for a currency exchange or retail establishment, and a date - here, the representations are in decimal notation for ease of understanding, though, in practice, they would be in binary.

Register E can contain information about the currency and denomination of the banknote, which can be used to count a stack of mixed currency and denomination notes into separate stacks. Figure 4 shows diagrammatically an arrangement in which a stack of notes 41 is placed in a high speed counting machine 42 which picks them off individually and reads the tags, directing the notes into bins 43 according to their currency and denomination. The machine 42 is connected to the bank's computer which uses the data from the machine and adds up the various amounts of each currency, without any need for manual sorting and counting, directs credit to an appropriate account or accounts, and passes on the data to an area hub and eventually to the host computer.

There is still further space on the chip for other information, should that be required for any reason.

Figure 3 shows a possible structure for a database connection for a banknote authenticating system. Bank based reader/writer units 31 would be connected to the bank's internal computer 32, which would, in turn, be connected to an area hub 33 along with other banks (and currency exchanges and other places where banknotes are passed). Area hubs 33 would in turn connect to a host computer 34.

Each time a tag is read in one of the reader/writer units 31, its counter is incremented and a record of the date and time, and the place of the transaction entered. The information read from the tag, together with the new information entered thereon, is transmitted through the network up to the host computer 34, where it is checked against the database held thereon, and the new information entered. Checks can also be made in the bank's

computer 32 and in the hubs 33, for repeated codes, these computers, together, of course, with the host computer 34, being programmed to detect repeats and clear them as acceptable, because of the changed information, or not acceptable, if the check shows that there are two or more instances of the incremental counter data being the same. That can happen, of course, only if there are two banknotes in circulation, one of which has been copied from the other. The information about the time and date, and the location of recent checks gives a good audit trail on which to launch an investigation.

Because the worst case scenario is that a counterfeiter would withdraw from a bank account, or from several accounts, banknotes that he could copy, information about the time and place of that or those transactions would be on the host computer, and this would probably be sufficient to pin down the counterfeiter. Moreover, having then figured out which notes are genuine and which are not, the last-known location of the counterfeit notes would be instantly known, and their reappearance from circulation could be awaited, so they could be withdrawn from circulation.

Another, incidental, advantage of the system is that, when currency is stolen, it can be readily identified, because of the audit trail, and rendered worthless by the host computer issuing instructions through the network to the bank computers.

The network can, of course, be international.

In Figure 5, a system for passports is illustrated. A passport 51 will have a unique identifying code in Register A of an RFID tag 11, which can be supplemented by an algorithm-derived code in Register B. Examining the passport at a frontier control will involve reading the contents of Registers A and B, and reading and incrementing a counter in Register C. Time and place data can be entered, as before into Register D.

Here, the problem is somewhat simpler than for currency notes, inasmuch as a counterfeiter is unlikely to be able to secure large numbers of passports to copy genuine codes, and the algorithm-derived code in register B will almost certainly be wrong, permitting instant detection at the frontier post, without resort to the database in a host computer. What is more likely to happen is that a genuine passport will be obtained by theft, and a new photograph substituted which is a likeness of the new bearer. Registers E - H, however, can contain anthropometric data, such as locations of salient points on a fingerprint, or in iris patterns, or distance between pupil centres, the coding for these data being impenetratingly difficult. In case, however, the counterfeiter is expert enough to be able to change the register data to correspond to the anthropometric data appropriate to the new bearer, that data can be rendered inaccessible by storing it on the host computer rather than on the passport. Or one register might have information about, say, fingerprint salients, the others being blank, but, at the frontier post, the fingerprint salient data is uploaded into the host computer, where it is compared to the original data stored for that particular microchip, other data being downloaded into the chip, about, say, iris patterns, which the counterfeiter would not have been able to alter. There are thus two ways, now, of identifying a forged passport based on a genuine original, one being that changed anthropometric data does not correspond to the original held on the host

computer, the other being that new, original information will be downloaded which will not check out at the next frontier post. Or, on detection of a failure to correlate old and new data, the passport can simply be cancelled, if not at the start of a journey, because of time taken to upload and download, at least before the journey's end, and the carrier arrested on arrival. To facilitate this, at the start of each journey, when a passport is presented at check-in at an airport, for example, the flight number and destination can be entered into one of the registers.

Of course, a passport reported lost or stolen could be cancelled in any event, rendering it useless and of no value.

The considerations will apply, also, to identity cards. Indeed, an identity card and a passport could very well be the same thing, in due course. The fact that information can be written to the chip could eliminate the need to have visa stamps, so the passport booklet form will be redundant. Register space could also be allocated to driving licence details.

Claims

1 A system for authenticating re-presentable items, such as currency notes and passports, comprising applying to each item a unique code, reading the code on presentation, and checking the code against a database, characterised in that at each check, the code is altered.

2 A system according to claim 1, in which the code is comprised in an RFID tag.

3 A system according to claim 2, in which the tag has writable register means.

4 A system according to claim 1 or claim 2, in which at least part of the code is burnt in so that it cannot be erased or altered.

5 A system according to any one of claims 1 to 3, in which a part of the code is the tag manufacturer's burnt in unique number.

6 A system according to any one of claims 1 to 5, in which the code is altered by incrementing a counter at each check.

7 A system according to any one of claims 1 to 6, in which a code derived by an algorithm from a burnt-in code is also part of the unique code.

8 A system according to claim 7, in which the code is altered to contain time and place information about the check.

9 A system according to claim 8, in which historic time and date information is written over.

10 A system according to any one of claims 1 to 9, in which deleted or written over information is stored on the database.

11 A system according to any one of claims 1 to 10, in which the items are currency notes.

12 A system according to any one of claims 1 to 10, in which the items are passports or other identity cards.

13 A re-presentable item authenticated by a system according to any one of claims 1 to 12.

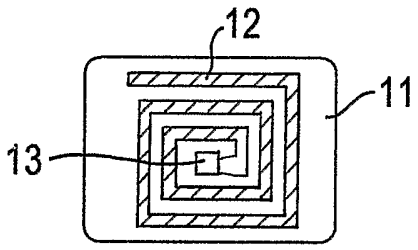



Fig. 1

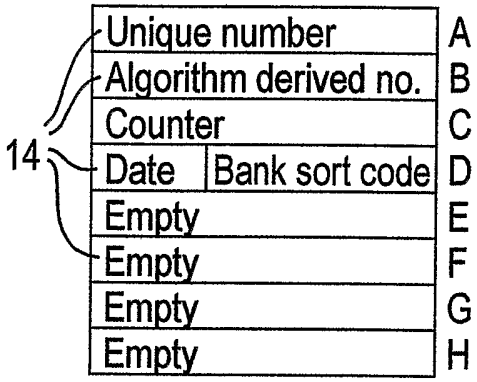



Fig. 2

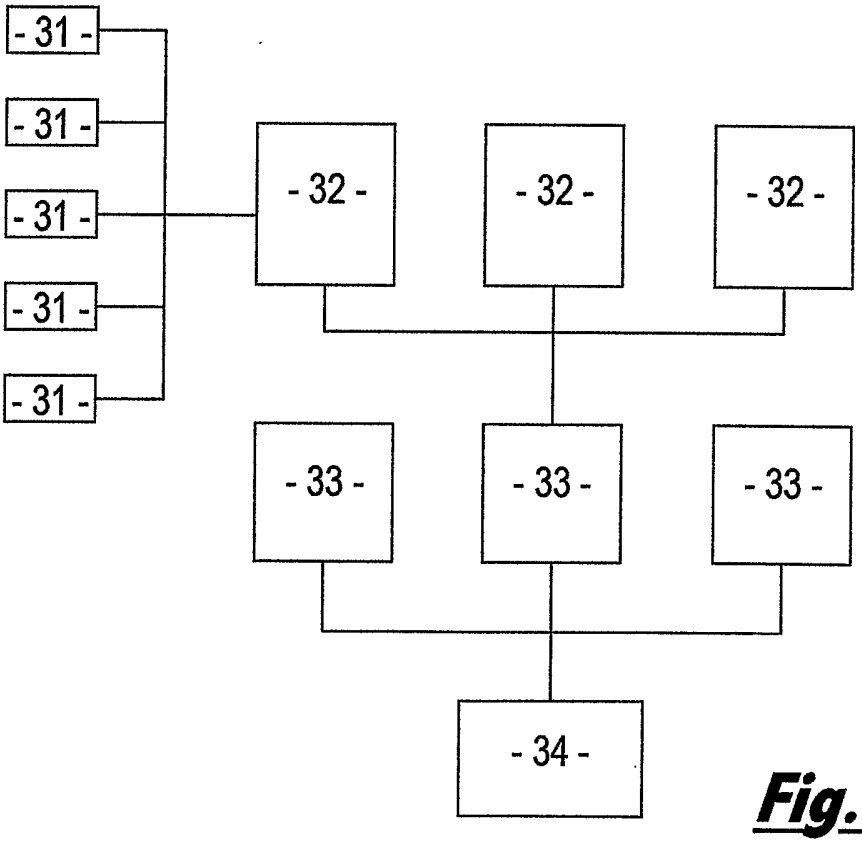



Fig. 3

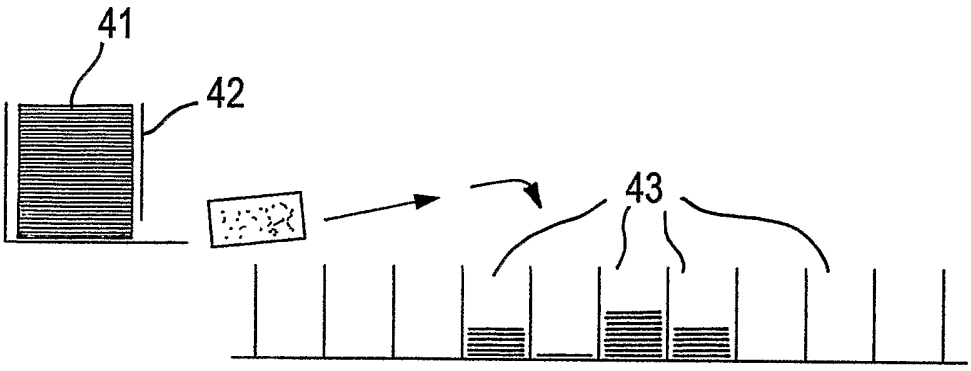

41
42
43

Fig. 4

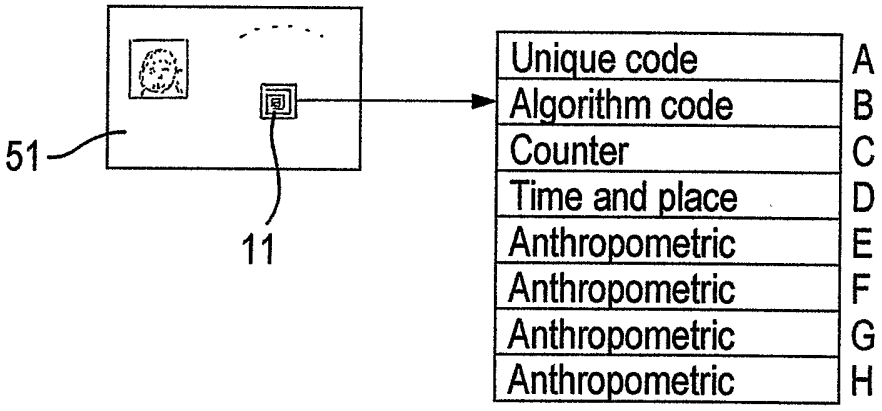

51
11
Unique code
Algorithm code
Counter
Time and place
Anthropometric
Anthropometric
Anthropometric
Anthropometric
A
B
C
D
E
F
G
H

Fig. 5

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB2005/001627

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07D7/00

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)
IPC 7 G07D G06K B42D

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)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | HENRICI D ET AL: "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers" PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, 2004. PROCEEDINGS OF THE SECOND IEEE ANNUAL CONFERENCE ON, PISCATAWAY, NJ, USA,IEEE, 14 March 2004 (2004-03-14), pages 149-153, XP010689745 ISBN: 0-7695-2106-1 the whole document | 1-13 |
| X | US 2003/052788 A1 (KWONG-TAI CHUNG KEVIN) 20 March 2003 (2003-03-20) paragraph '0001! - paragraph '0047! paragraph '0081! - paragraph '0107! | 1-13 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 | Date of mailing of the international search report |
|---|---|
| 3 August 2005 | 24/08/2005 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016 | Reino, B |

Form PCT/ISA/210 (second sheet) (January 2004)

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB2005/001627

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 00/07151 A (SIEMENS AKTIENGESELLSCHAFT; BROSOW, JOERGEN) 10 February 2000 (2000-02-10) page 1, line 1 - page 6, line 12 | 1-13 |
| X<br>A | US 2003/164611 A1 (SCHNEIDER WALTER ET AL) 4 September 2003 (2003-09-04) paragraph '0009! - paragraph '0011! paragraph '0035! - paragraph '0043! | 1-3,8,9, 11-13<br>4,5,10 |
| X | US 4 870 260 A (NIEPOLOMSKI ET AL) 26 September 1989 (1989-09-26) column 1, line 59 - column 2, line 65 | 1,6, 11-13 |
| X | JUELS, A. PAPPU, R.: "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes" FINANCIAL CRYPTOGRAPHY 2003, vol. 2742, 1 January 2003 (2003-01-01), pages 103-121, XP002338983 Berlin the whole document | 1-5, 11-13 |
| A | US 4 463 250 A (MCNEIGHT ET AL) 31 July 1984 (1984-07-31) cited in the application the whole document | 1 |
| A | US 2003/163696 A1 (RANCIEN SANDRINE) 28 August 2003 (2003-08-28) paragraphs '0015!, '0059!, '0060! | 1-3,8,9, 11-13 |
| A | TAKARAGI K ET AL: "An ultra small individual recognition security chip" IEEE MICRO IEEE USA, vol. 21, no. 6, November 2001 (2001-11), pages 43-49, XP002339046 ISSN: 0272-1732 the whole document | 1-5, 11-13 |
| A | "Read/Write Transponder TK5552" 'Online! April 2003 (2003-04), ATMEL CORPORATION , XP002339001 Retrieved from the Internet: URL:http://www.atmel.com/dyn/resources/prod_documents/doc4698.pdf> 'retrieved on 2005-08-03! the whole document | 1-5, 11-13 |
| A | WO 03/050757 A (TAGSYS AUSTRALIA PTY LTD; COLE, PETER, HAROLD) 19 June 2003 (2003-06-19) page 5, line 16 - line 20; figures 3,5 | 1-3,6, 10,13 |

-/--

# INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/GB2005/001627

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 2003/006121 A1 (LEE KENNETH YUKOU ET AL) 9 January 2003 (2003-01-09) paragraphs '0002!, '0018! | 1,2, 11-13 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB2005/001627

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2003052788 A1 | 20-03-2003 | US 2005110640 A1 | 26-05-2005 |
| | | AU 9701201 A | 22-04-2002 |
| | | US 2005150952 A1 | 14-07-2005 |
| | | US 2003006878 A1 | 09-01-2003 |
| | | US 2004036623 A1 | 26-02-2004 |
| | | US 2003209601 A1 | 13-11-2003 |
| | | AU 1312802 A | 29-04-2002 |
| | | CA 2456098 A1 | 13-02-2003 |
| | | EP 1514247 A2 | 16-03-2005 |
| | | EP 1421459 A2 | 26-05-2004 |
| | | WO 0233511 A2 | 25-04-2002 |
| | | WO 0231629 A2 | 18-04-2002 |
| | | WO 03012595 A2 | 13-02-2003 |
| | | US 2003026462 A1 | 06-02-2003 |
| | | US 6657543 B1 | 02-12-2003 |
| | | US 2005092835 A1 | 05-05-2005 |
| | | US 2003062411 A1 | 03-04-2003 |
| | | US 2003173404 A1 | 18-09-2003 |
| | | WO 03063055 A2 | 31-07-2003 |
| | | WO 03062961 A2 | 31-07-2003 |
| | | US 2003138135 A1 | 24-07-2003 |
| | | US 2003136835 A1 | 24-07-2003 |
| | | US 2004156537 A1 | 12-08-2004 |
| | | US 6703935 B1 | 09-03-2004 |
| | | US 2004164864 A1 | 26-08-2004 |
| WO 0007151 A | 10-02-2000 | DE 19833746 A1 | 03-02-2000 |
| | | DE 19849762 A1 | 04-05-2000 |
| | | AT 283524 T | 15-12-2004 |
| | | AU 758692 B2 | 27-03-2003 |
| | | AU 5507299 A | 21-02-2000 |
| | | BR 9913342 A | 15-05-2001 |
| | | CA 2338661 A1 | 10-02-2000 |
| | | CN 1320251 A | 31-10-2001 |
| | | DE 59911151 D1 | 30-12-2004 |
| | | WO 0007151 A1 | 10-02-2000 |
| | | EP 1501054 A2 | 26-01-2005 |
| | | EP 1101203 A1 | 23-05-2001 |
| | | JP 2004500606 T | 08-01-2004 |
| | | MX PA01001024 A | 04-06-2002 |
| | | US 6918535 B1 | 19-07-2005 |
| US 2003164611 A1 | 04-09-2003 | DE 10032128 A1 | 17-01-2002 |
| | | AU 7637901 A | 14-01-2002 |
| | | CA 2414746 A1 | 03-01-2003 |
| | | CN 1443118 A ,C | 17-09-2003 |
| | | CZ 20030017 A3 | 18-06-2003 |
| | | WO 0202350 A1 | 10-01-2002 |
| | | EP 1301355 A1 | 16-04-2003 |
| | | HK 1058057 A1 | 18-03-2005 |
| | | JP 2004501809 T | 22-01-2004 |
| US 4870260 A | 26-09-1989 | CH 669275 A5 | 28-02-1989 |
| | | AT 56552 T | 15-09-1990 |
| | | BE 904689 A1 | 18-08-1986 |
| | | DE 3674118 D1 | 18-10-1990 |
| | | EP 0215187 A1 | 25-03-1987 |
| | | JP 62046391 A | 28-02-1987 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB2005/001627

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 4463250 A | 31-07-1984 | GB 2101376 A ,B | 12-01-1983 |
| US 2003163696 A1 | 28-08-2003 | FR 2812740 A1 | 08-02-2002 |
| | | AU 8224801 A | 13-02-2002 |
| | | BR 0112868 A | 22-04-2003 |
| | | CA 2424972 A1 | 07-02-2002 |
| | | EP 1305776 A1 | 02-05-2003 |
| | | WO 0211078 A1 | 07-02-2002 |
| WO 03050757 A | 19-06-2003 | WO 03050757 A1 | 19-06-2003 |
| | | AU 2002349180 A1 | 23-06-2003 |
| | | EP 1454291 A1 | 08-09-2004 |
| | | US 2005017844 A1 | 27-01-2005 |
| US 2003006121 A1 | 09-01-2003 | NONE | |