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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 May 2013 (16.05.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/068097 A1

(51) International Patent Classification:
H04W 12/08 (2009.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/EP2012/004611

(22) International Filing Date:
6 November 2012 (06.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11008890.3 8 November 2011 (08.11.2011) EP

(71) Applicant: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Inventors: **BOSVED, Jan**; Kantarvägen 25, S-131 40 Nacka (SE). **HULT, Jorgen**; Eklidsvägen 17, S-146 40 Tullinge (SE).

(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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, RS, 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:

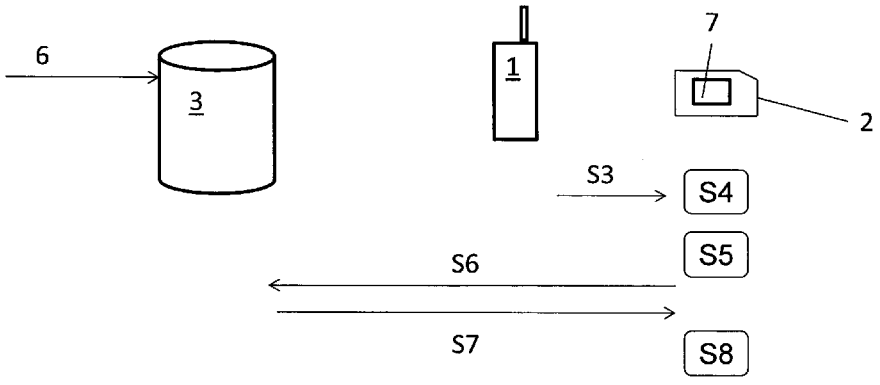
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

(54) Title: METHOD OF PREVENTING FRAUDULENT USE OF A SECURITY MODULE

FIG 1



(57) Abstract: A method of preventing fraudulent use of a security module (2) in a device (1), wherein the security module (2) is designed to perform the following steps. Retrieve (S3) a device identifier of the device (1) from the device (1). Check (S4) whether negative allowance information is stored in the security module (2) for the retrieved device identifier and transmit (S6) a security module identifier of the security module (2) and said retrieved device identifier to a server (3). Receive (S7) a response from said server (3) regarding whether the security module (2) is allowed to operate with the identified device (1) and store (S8) negative allowance information in the security module for the retrieved device identifier, if the security module (2) is not allowed to operate with the identified device (1) according to the server response. The invention also refers to a security module and a system comprising the security module, the device and the server.

WO 2013/068097 A1

Method of preventing fraudulent use of a security module

The present invention refers to a method of preventing fraudulent use of a security module, such as a SIM card, and a device, such as a mobile device, and also to a security module.

Mobile terminals using the Global System for Mobile communication (GSM) and 3rd Generation Partnership Program (3GPP) specifications as standards for digital wireless communication are called GSM-3G phones, below called mobile device.

Normally a SIM (Subscriber Identity Module) card for a mobile device (ME) such as a mobile telephone can be used in any mobile device. Thus it is possible to steal a SIM card belonging to an owner and to use the SIM card in a mobile device of the thief. The result will be that the owner will be billed for services used with the SIM card. One problem is however that the thief must know the PIN code of the SIM card in order to be able to use the SIM card.

SIM cards residing in machines are not easily supervised and may be placed in environments that make supervision difficult. For example, SIM cards are placed in traffic light equipments, in alarm installations, in vehicles, boat motors, and other equipment that shall be remotely monitored.

Such SIM cards do not normally need a PIN code to make them operate. Therefore, such SIM cards may be stolen and used in a mobile device or another stationary device. Certainly the proprietor of the SIM card will be billed. The present invention is thus also applicable regarding stationary devices having a SIM card and operating over a mobile telephone communication network.

Another problem is that mobile devices (ME) may be stolen, where the thief may steal a more sophisticated mobile telephone and then use his or her SIM card in the stolen telephone.

So far the prevention of illegal use has focused on illegal use of mobile devices. For example, there is a standardized register, the EIR (Equipment Identity Register) where network operators may check if a device is stolen by looking up the IMEI (International Mobile Equipment Identifier) in the EIR. That is no longer sufficient.

The network operators certainly keep track of, and shut off, subscriptions reported stolen. This procedure is based on mobile users being missing their mobile telephone and reporting it stolen. However, subscriptions residing in millions of mobile devices will not be missed.

Once SIM cards are being distributed over millions of machines and devices there is a strong desire to make it possible to automatically monitor that the SIM cards, i.e. the subscriptions are not operated illegally in a device other than the intended ones.

Document WO 2009/029156 relates to a method of activating a mobile device for use with a certain service provider. The document describes a method where it is not necessary to lock the mobile device to a certain service provider. An activation server that is in connection with the service provider can issue an activation ticket that is transmitted to the mobile device in order to lock up the device for further communication depending on the identity of the SIM card.

In US 5,809,413 the EIR locks the terminal to the SIM and the SIM to the terminal, if the IMEI of a terminal is listed as stolen. In EP 1 562 394 A2 the terminal generates a code value based on terminal and card numbers and blocks the terminal functions for listed code values. The terminal checks the list and the EIR checks if the terminal is stolen.

However, there is a strong desire for a method of preventing fraudulent use of a security module, such as a SIM card. This problem is solved by the subject matters of the independent claims. The dependent claims are directed to preferred embodiments of the invention.

A preferred solution refers to a method of preventing fraudulent use of a security module, such as a SIM (Subscriber Identity Module) card, and fraudulent use of a device using said security module, such as a mobile equipment (ME). The invent-

ion is characterized in that at the time a security module is issued or sold or at a later time the IMEI (International Mobile Equipment Identifier) of the device for which the security module is designated and at least one identifier of the security module, such as the ICCID (Integrated Circuit Card ID) of a SIM card and/or the IMSI (International Mobile Subscriber Identity) stored on a SIM card, are caused to be stored in a server to which the device can be connected, in that said server contains information on what identity of a security module is allowed to operate with what device identified by its IMEI, in that an application is stored in the security module, which application is designed to retrieve the IMEI of the device and designed to connect the security module to said server and transmit said identity of the security module and of the device to the server, in that the security module designed to receive a response from said server regarding whether the security module is allowed to operate with the identified device, in that at least when the device is turned on for the first time with a new security module said application asks the server whether the transmitted identity of the security module and the device is allowed to operate together or not, and in that in case the security module and said device are allowed to operate together the security module and the device are started for further communication.

Below the present invention is described in more detail together with exemplifying embodiments and in connection with a drawing, where Figure 1 shows a schematic block diagram.

Even if the present invention is exemplified below with a "mobile device" the invention also relates to stationary devices having a security module, such as a SIM card, as exemplified below.

Further, the present invention is exemplified below in connection with a SIM card, but it shall be understood that the present invention is not restricted to SIM cards, but any security module. The security module is preferably a hardware security module. The security module may be a portable data carrier and hence reversibly removable from the device. Examples for such portable data carriers are SIM card for mobile or station-

ary communication, a secure multimedia card or USB Token. Still further the security module may be built-in in the device (as a fixture), such as a TPM (Trusted Platform Module) or a secure NFC (Near Field Communication) module.

Thus, the present invention refers to a method of preventing fraudulent use of a security module, such as a SIM (Subscriber Identity Module) card, and fraudulent use of a device using said security module, such as a mobile equipment (ME) as well as a security module to be used with the method.

According to the invention, at the time a security module 2 is issued or sold or at a later time the IMEI (International Mobile Equipment Identifier) of the device 1 for which the security module 2 is designated and at least one identifier of the security module, such as the ICCID (Integrated Circuit Card ID) of a SIM card and/or the IMSI (International Mobile Subscriber Identity) stored on a SIM card, is caused to be stored in a server 3 to which the device 1 can be connected. Alternatively to storing predetermined identifiers, rules may be stored on the server which pairs of identifiers are allowable to operate together.

The mobile device can thereafter be connected to the server, as illustrated with the arrows S6, S7 in Figure 1. For example said identifiers can be fed into the server by personnel in a store where the security module is purchased, as illustrated by arrow 6 in Figure 1.

Said server 3 contains information on what identity of a security module 2 is allowed to operate with what device 1 identified by its device identifier (IMEI).

Further, an application 7 is stored in the security module 2, which application is designed to retrieve the IMEI of the device 1 and designed to connect the security module 2 to said server 3 and transmit said identity of the security module 2 and of the device 1 to the server 3. The security module 2 is designed to receive a response from said server

3 regarding whether the security module 2 is allowed to operate with the identified device 1.

A security module being allowed to operate with the device enables at least one function required for the device. A security module being not allowed to operate with the device disables at least one function required for the device. Preferably the function of the security module is required for authenticating the device (and/or the user of the device) in the network.

Still further, at least when the device 1 is turned on for the first time with the (new) security module 2 said application 7 asks the server 3 whether the transmitted identifiers of the security module and the device are allowed to operate together or not. In case the security module 2 and said device 1 are allowed to operate together the security module and the device are started for further communication, i.e. are allowed to use the mobile network.

According to one exemplifying embodiment of the invention the flow in case a mobile device 1 with a stolen SIM card 2 is switched on is described below.

1. The mobile device 1 connects to the mobile network.
2. When the power is switched on there is an event in the mobile device triggering the application 7 on the SIM card 2.
3. The application 7 reads S3 the IMEI of the mobile device (ME).
4. The application 7 checks S4 if there is a forbidden device flag set in a memory of the SIM card 2 for the read IMEI. There is no forbidden flag for the read IMEI.
5. The application 7 compares S5 the read IMEI with allowed IMEI´s on a list in the memory of the SIM card 2, if there are any. The IMEI is not on such list.
6. The application 7 sends S6 a request to said server 3 regarding the IMEI.
7. The server 3 responds S7 to the application 7 that the ME with the read IMEI is forbidden.

8. The application 7 sets a forbidden flag for the read IMEI in the memory of the SIM card 2.

9. At next power on the said event triggers the application 7, the application 7 will detect the forbidden flag (in step S4) and will prevent the mobile device 1 from connecting to the mobile network.

10. The application 7 re-sets the forbidden flag.

It should be considered that step 1 of connecting to the mobile network is preferably performed as a step 4a (after step S4). In particular this step will be performed only, if the forbidden flag is not set for this IMEI.

According to said exemplifying embodiment of the invention the flow in case a mobile device 1 with an allowed SIM card 2 is switched on for the first time is described below.

1. The mobile device 1 connects to the mobile network.

2. When the power is switched on there is an event in the mobile device 1 triggering the application 7 on the SIM card

3. The application 7 reads S3 the IMEI of the mobile device (ME).

4. The application 7 checks S4 if there is a forbidden device flag set in a memory of the SIM card 2 for the read IMEI. There is no forbidden flag for the read IMEI.

5. The application 7 compares S5 the read IMEI with allowed IMEI's on a list in the memory of the SIM card, if there are any. The IMEI is not on such list.

6. The application 7 sends a request S6 to said server 3 regarding the IMEI.

7. The server 3 responds S7 to the application 7 that the ME with the read IMEI is allowed.

8. The application saves S8 the IMEI on a list in the memory of the SIM card 2.

9. The application 7 opens the mobile device 1 for further communication.

According to said exemplifying embodiment of the invention the flow in case a mobile device 1 with an allowed SIM card 2 is switched on again is described below.

1. The mobile device 1 connects to the mobile network.
2. When the power is switched on there is an event in the mobile device 1 triggering the application 7 on the SIM card 2.
3. The application 7 reads S3 the IMEI of the mobile device (ME).
4. The application 7 checks S4 if there is a forbidden device flag set in a memory of the SIM card 2 for the read IMEI. There is no forbidden flag for the read IMEI.
5. The application 7 compares S5 the read IMEI with allowed IMEI´s on a list in the memory of the SIM card 2, if there are any. The IMEI is on such list.
9. The application 7 opens the mobile device for further communication.

According to a preferred embodiment the identifier of the security module 2 and the identifier of the device 1 are caused to be coupled to each other to form a pair of numbers and caused to be stored in said server 3 to which the device 1 can be connected. Said application 7 is designed to connect the security module 2 to said server 3 and transmit said pair to the server and designed to receive a response from said server 3 regarding if said pair is stored in said server, at least when the device 1 is turned on for the first time with a new security module 2. In case the said pair is stored on said server 3 the security module and the device are started for further communication.

According to a preferred embodiment, as described above, of the present invention in case said identifiers are stored on said server 3 as being allowed together, said pair is stored as allowed in a memory of the security module 2. When the device 1 is turned on the next time said application 7 on the security module 2 is caused to check said identifiers against said memory of the security module 2. In case the said identifiers are stored as allowed in the memory of the security module, the security module and the device are started for further communication.

According to another preferred embodiment, as described above, in case said identifiers are not stored on said server 3, said identifiers are stored as being not allowed in the memory of the security module 2. When the device 1 is turned on the next time said application 7 on the security module 2 is caused to check said pair against said memory

of the security module 2. In case the said identifiers are stored as being not allowed in the memory of the security module, the security module and the device are not started for further communication.

According to still another preferred embodiment, as described above, in case the application 7 on the security module 2 has denied the device 1 further communication, the application 7 is arranged to delete the identifiers that are not allowed from a memory of the security module 2.

This enables a dynamic approach. A device (ME) that is forbidden at a certain time might be allowed at a later time. As the SIM card 2 application 7 makes a check each time the device is powered on, a forbidden device can be changed to an allowed device for the SIM card 2 in question.

According to still another preferred embodiment of the invention the number of said allowed combination of identifiers which may be stored in the memory of said security module 2 may be two or more.

This allows an owner of several mobile telephones (ME) to be able to use all of them, one at a time.

As indicated before said identifiers can also be defined by rules in said server 3. For example, security modules with numbers starting with XXXX are allowed in devices with numbers starting with AAAA, BBBB and CCCC but are not allowed in devices with numbers starting with AAAD. Such rules may define a group of devices, such as traffic lights or burglar alarm installations. Certainly it is up to the man skilled in the art to design appropriate rules.

Further, the identifiers can be stored in the memory of the security module 2 only temporarily. Temporarily can mean either for a certain duration of time, such as an hour or a day, and/ or for a number of accesses, e.g. implemented as a counter. Tempo-

rarily stored identifiers can be provided by the server 3 as well as start values of the corresponding counter or counters.

A mobile operator can deploy a system and a method to ensure that SIM cards 2 are not used illegally, because the mobile equipment (ME) must belong to a partner of the network operator who is actually paying for the communication with the mobile device.

As is apparent from the above said the application 7 on the SIM card 2 prevents together with the server 3 the use of a subscription in a forbidden device.

The server 3 keeps track of what combination of a SIM card and a mobile device (ME) is allowed for use. Thus, the forbidden device need not be a stolen device registered with an EIR. The mobile operator may dynamically decide what devices are forbidden at a certain point of time for any subscription.

Further, the application 7 need not communicate with the server 3 if the mobile equipment (ME) is registered as allowed in the memory of the SIM card 2.

It is apparent that the present invention solves the problem described above.

Above several embodiments of the present invention have been described. However, the present invention shall not be regarded as restricted to the various embodiments, but can be varied within the scope of the claims.

Claims

1. A method of preventing fraudulent use of a security module (2) in a device (1), wherein the security module (2) is designed to perform the following steps:
- retrieve (S3) a device identifier of the device (1) from the device (1),
- check (S4) whether negative allowance information is stored in the security module (2) for the retrieved device identifier,
- transmit (S6) a security module identifier of the security module (2) and said retrieved device identifier to a server (3), said server (3) contains information on what security module identity is allowed to operate with what device identity,
- receive (S7) a response from said server (3) regarding whether the security module (2) is allowed to operate with the identified device (1) and
- store (S8) negative allowance information in the security module for the retrieved device identifier, if the security module (2) is not allowed to operate with the identified device (1) according to the server response.

2. Method according to claim 1, characterized in that the security module (2) deletes the stored negative allowance information when a predetermined criteria is reached.

3. Method according to claim 2, characterized in that the predetermined criteria is reached when a counter, preferably a reset counter, reaches a given value.

4. Method according to claim 2, characterized in that the predetermined criteria is a time criteria.

5. Method according to claim 2, characterized in that the security module deletes the negative allowance information when it has been used once in the step of checking.

6. Method according to one of claims 1 to 5, characterized in that the security module (2) disables at least one of its functions when it stores negative allowance information for the retrieved device identifier.

7. Method according to one of claims 1 to 6, characterized in that, in case said identifiers are allowed together, said device identifier is stored as allowed in a memory of the security module (2).

8. Method according to one of claims 1 to 7, characterized in that the security module performs a further step of checking (S5) whether positive allowance information is stored in the security module for the retrieved device identifier.

9. Method according to one of claims 6 to 8, characterized in that the security module enables the at least one of its functions when it stores positive allowance information for the retrieved device identifier.

10. Method according to one of claims 1 to 9, characterized in that the number of said device identifiers stored as or stored with positive and/or negative allowance information stored in the memory of said security module (2) may be two or more.

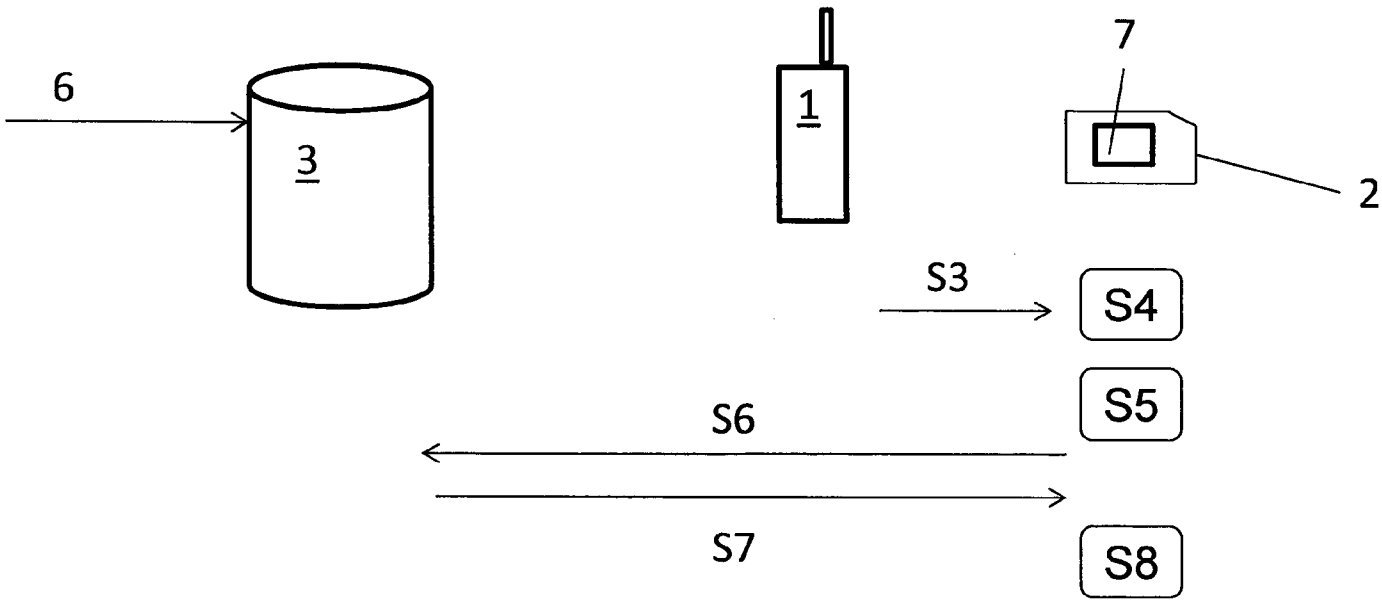
11. Method according to one of claims 1 to 10, characterized in that the device identifier is an IMEI (International Mobile Equipment Identifier) and/or the security module identifier is an ICCID (Integrated Circuit Card ID) and/or the IMSI (International Mobile Subscriber Identity).

12. A security module adapted for preventing fraudulent use of the security module (2) by performing the steps of one of claims 1 to 11.

13. The security module according to claim 12 comprising an application (7) adapted to perform the steps.

14. A system comprising a security module (2) according to claim 11 or 12 arranged in a device (1) and the server (3), which contains the information on what security module identity is allowed to operate with what device identity.

FIG 1



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/004611

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/08 H04L29/06
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)
H04W H04L G08B

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 practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 809 413 A (MECHE PAUL S [US] ET AL) 15 September 1998 (1998-09-15) column 1, line 50 - column 2, line 31; figures 2-4, 6 column 3, line 34 - line 67 column 4, line 22 - column 6, line 63 column 7, line 43 - line 67 column 9, line 24 - column 10, line 11 -----	1-14
X	EP 1 562 394 A2 (LG ELECTRONICS INC [KR]) 10 August 2005 (2005-08-10) paragraph [0006] - paragraph [0010]; figures 1-2 paragraph [0013] - paragraph [0020] paragraph [0025] paragraph [0031] ----- -/--	1-14

[X] Further documents are listed in the continuation of Box C. [X] 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 application or patent 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
22 February 2013	28/02/2013

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, Fax: (+31-70) 340-3016	Figiel, Barbara

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/004611

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102 026 180 A (CHINA MOBILE COMM CORP) 20 April 2011 (2011-04-20) abstract	1,12,14
A	WO 2010/102954 A1 (GEMALTO SA [FR]; THILL MICHEL [FR]; BARBE SERGE [FR]) 16 September 2010 (2010-09-16) page 1, line 4 - line 12 page 3, line 4 - page 5, line 19 page 8, line 4 - line 11 page 10, line 13 - page 11, line 12	1,12,14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/004611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5809413 A	15-09-1998	DE 69635328 D1	01-12-2005
		DE 69635328 T2	20-07-2006
		DE 69637053 T2	03-01-2008
		EP 0757502 A2	05-02-1997
		EP 1596622 A2	16-11-2005
		JP 3935994 B2	27-06-2007
		JP 9121387 A	06-05-1997
		US 5600708 A	04-02-1997
		US 5809413 A	15-09-1998
EP 1562394 A2	10-08-2005	AT 526800 T	15-10-2011
		CN 1655643 A	17-08-2005
		EP 1562394 A2	10-08-2005
		JP 4040047 B2	30-01-2008
		JP 2005223900 A	18-08-2005
		KR 20050079128 A	09-08-2005
		US 2005170813 A1	04-08-2005
CN 102026180 A	20-04-2011	NONE	
WO 2010102954 A1	16-09-2010	EP 2229019 A1	15-09-2010
		EP 2406977 A1	18-01-2012
		US 2012009979 A1	12-01-2012
		WO 2010102954 A1	16-09-2010