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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2012 (18.10.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/139629 A1

(51) International Patent Classification:
G06Q 10/00 (2012.01) *H01L 29/00* (2006.01)
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/EP2011/055652

(22) International Filing Date:
12 April 2011 (12.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FIN-02610 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MARHOEFER, Michael** [DE/DE]; Wendelsteinstr. 6, 82041 Deisenhofen (DE). **SEIDL, Robert** [DE/DE]; Laurenziweg 5, 82549 Königsdorf (DE). **BAUER-HERMANN, Markus** [DE/DE]; Hofmarkstraße 37, 94529 Aicha vorm Wald (DE).

(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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

WO 2012/139629 A1

(54) **Title**: METHOD AND APPARATUS FOR SHARING USER DATA

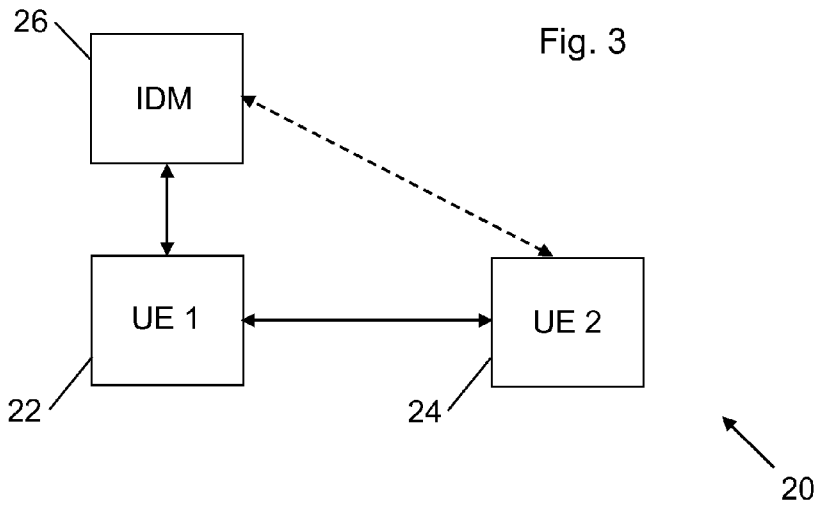

Fig. 3

(57) **Abstract**: A mechanism for dynamically generating a set of user attributes is described. The user attributes are triggered and tailored by the user for a specific purpose and then optionally sent to a communication partner. The user attributes are provided in a form that enables the communication partner to obtain the user attributes included in said list.

Description

Title

Method and Apparatus for Sharing User Data

The present invention is directed to a method and apparatus for sharing user data, such as identity data and user attributes. In particular, the present invention enables a user to be involved in the process of sharing at least some of his/her user data.

Figure 1 is a block diagram of a system, indicated generally by the reference numeral 1. The system 1 comprises a user 2 and a service provider 4. The user is in two-way communication with the service provider 4.

In the use of the system 1, the service provider 4 needs to know information regarding the user 2 in order to function correctly. For example, the service provider may be an Internet-based shop that needs to know name, address and credit card details of the user 2 in order to fulfil an order.

As is well known in the art, the user 2 may provide the information required by the service provider 4 directly to the service provider. This is a simple procedure, but it requires the user 2 to provide this information each time the service provider 4 is used. In an alternative use of the system 1, the service provider 4 may store data relating to the user 2 (such as name, address and credit card details) so that the user only needs to provide such data once. This is more convenient for the user, but the storing of user data at the service provider 4 represents a potential security concern. Many users may not be willing to make use of a service provider that stores potentially sensitive user data. Furthermore, data stored at the service provider 4 may become obsolete. By way of example, in the Internet-shop example

considered above, an order may be made but incorrectly completed due to obsolete data.

Figure 2 is a block diagram of a system, indicated generally by the reference numeral 10. The system 10 comprises a user 12, a service provider 14 and an identity management (IDM) system 16. The user 12 is in two-way communication with both the service provider 14 and the IDM 16. The service provider 14 is additionally in two-way communication with the IDM 16.

User attributes for the user 12 are stored at the IDM 16. Accordingly, when the service provider 14 needs to know information regarding the user 12 in order to function correctly, the service provider requests this information from the IDM 16.

Considering again the Internet-shop example discussed above, in the event that the user 12 places an order at the service provider 14 for which the service provider requires name, address and credit card information concerning the user 12, the service provider 14 requests this information from the IDM 16. In the event that the IDM 16 trusts the service provider 14, that data may be provided. Importantly, this data will be provided by the IDM as required and so will always be up-to-date and does not need to be stored at the service provider, thereby overcoming two of the problems outlined above with respect of the system 1.

In the system 10, a dialogue is carried out between the service provider 14 and the IDM 16. A privacy policy for the user 12 may be stored at the IDM 16 to enable the IDM to determine whether (and to what extent) potentially sensitive user data can be shared with the service provider 14. Such privacy policies can be inflexible. Furthermore, such privacy policies risk either being too restrictive (potentially preventing a full operation of the service provider 14) or insufficiently restrictive (potentially leading to a user data being provided to a service provider

that the user may prefer to be kept secret from that service provider).

The present invention seeks to address at least some of the problems outlined above.

The invention provides a method comprising: receiving instructions (typically via a user interface of a personal data portal) from a first user for the generation of a list of user attributes of said first user for sending to a communication partner, wherein the list of user attributes is a subset of user attributes of the first user (e.g. a subset of the attributes of the first user available to said personal data portal); generating said list of user attributes; and providing said list in a form that enables the said communication partner to obtain said user attributes included in said list. In some embodiments, the list of user attributes does not provide the attributes themselves to the communication partner. The said personal data portal is typically provided as part of an identity management system.

The invention also provides an apparatus (e.g. a data portal and/or an IDM or some other central point for the management of communication cards) comprising: a first input for receiving instructions (typically via a user interface of the personal data portal) from a first user for the generation of a list of user attributes for the first user, wherein the list of user attributes is a subset of the user attributes for the first user stored, wherein said the user attributes included in (or omitted from) said subset is (at least partially) controlled by the first user; a processor for generating said list of user attributes; and a first output for providing said list (typically in a form that enables a communication partner to obtain said user attributes included in said list). A database may be provided for storing user attributes for the first user from which the subset is selected. In some forms of the invention, the apparatus may have access to an external database of such data.

Thus, the present invention provides a mechanism for dynamically generating a set of user attributes. The user attributes can typically be triggered and tailored by the user for a specific purpose and then optionally sent to a communication partner. The user attributes can be provided in a form that enables the communication partner to obtain the user attributes included in said list.

The communication card of the present can therefore provide fine-grained enforcement of each user's privacy preferences, but can also provide enhanced user convenience, since, for example, no unwanted or outdated or redundant information need be stored at a communication partner.

In many forms of the invention, the first user selects at least some of said user attributes for inclusion in said list. For example, at least some of said instructions may be received using a check-box input.

At least some of said instructions may include details of how to modify an existing list of user attributes. For example, a list may be generated (or previously stored) and the first user may be able to add attributes to the list and/or to remove attributes from the list. Thus, a simple user-interface can be provided that enables a user to easily make use of the principles of the present invention.

In some forms of the invention, the first user selects one or more recipients of said list. Thus, a list may be generated specifically for a particular recipient or purpose.

In some forms of the invention, the first user defines validity conditions for one or more of said user attributes included in said list. The said validity conditions may include a time period during which a selected user attribute is available to be viewed. Alternatively, or in addition, the said validity conditions may include a level of

abstraction of a user attribute. Other validity conditions could readily be provided.

In some forms of the invention, the user attributes are not themselves included in the list (but a means for obtaining those user attributes is included). For example, the said user attributes may be obtainable from an identity management system. In other forms of the invention, the said user attributes are included in said list in encrypted form. For example, the principles of digital rights management may be used to control access to user data.

The invention also provides a communication card comprising a list of user attributes for a first user, wherein the list of user attributes is a subset of the user attributes for the first user, wherein said the user attributes included in (or omitted from) said subset is controlled by the first user, wherein the list is provided in a form that enables a communication partner to obtain said user attributes included in said list (but does not necessarily actually provide the attributes themselves to the communication partner). Thus, a communication card can be provided that can be used to dynamically generate a set of personal attributes/data of one user, possibly triggered and tailored by the subject of these personal data for a specific purpose, and then optionally sent to his/her communication partner. That communication partner may have the option of sending his specific communication card in return to build a trusted relationship.

At least some of the user attributes included in said list may have limited validity. For example, said validity may be limited in duration. Alternatively, or in addition, at least some of said attributes may be abstracted.

In some forms of the invention, the user attributes are not themselves included in the list (but a means for obtaining those user attributes is included). For example, the said user attributes may be obtainable from an identity management

system. In other forms of the invention, the said user attributes are included in said list in encrypted form.

The invention yet further provides an apparatus (e.g. a user device) for generating a communication card (or a list of user attributes) comprising: a first interface for communicating with a user of said apparatus; and a second interface for communicating with a personal data portal, wherein the personal data portal is configured to receive instructions for the generation of a list of user attributes of the user of said apparatus for sending to a communication partner of said user, wherein the list of user attributes is a subset of user attributes of the first user available to said personal data portal. A third interface may be provided for communicating with the said communication partner. The said third interface may be configured to receive a communication card (or a list of user attributes) for said communication partner.

The invention yet further provides a method comprising: receiving, at a first user device, a list of attributes from a communication partner, wherein the list is provided in a form that enables the apparatus to obtain the user attributes included in the list and wherein the user attributes are a subset of the user attributes of said communication partner; and obtaining the said user attributes. The method may further comprise providing a list of user attributes of a user of said first user device to said communication partner.

The invention also provides a computer program comprising: code (or some other means) for receiving instructions (e.g. via a user interface of a personal data portal) from a first user for the generation of a list of user attributes of said first user for sending to a communication partner, wherein the list of user attributes is a subset of user attributes of the first user; code (or some other means) for generating said list of user attributes; and code (or some other means) for providing said list in a form that enables the said

communication partner to obtain said user attributes included in said list (but may not actually provide the attributes themselves to the communication partner). The computer program may be a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.

The invention yet further provides a computer program comprising code (or some other means) for receiving, at a first user device, a list of attributes from a communication partner, wherein the list is provided in a form that enables the obtaining of the user attributes included in the list and wherein the user attributes are a subset of the user attributes of said communication partner; and code (or some other means) for obtaining the said user attributes. The computer program may be a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.

Exemplary embodiments of the invention are described below, by way of example only, with reference to the following numbered drawings.

Figure 1 is a block diagram of a known system for providing user data;

Figure 2 is a block diagram of a known system for providing user data;

Figure 3 is a block diagram of a system in accordance with an aspect of the present invention;

Figure 4 is a flow chart showing an algorithm in accordance with an aspect of the present invention;

Figure 5 is a flow chart showing an algorithm in accordance with an aspect of the present invention;

Figure 6 is a flow chart showing an algorithm in accordance with an aspect of the present invention;

Figure 7 is a flow chart showing an algorithm in accordance with an aspect of the present invention;

Figure 8 is a block diagram of a system in accordance with an aspect of the present invention;
Figure 9 is a flow chart showing an algorithm in accordance with an aspect of the present invention; and
Figure 10 is a block diagram of a system in accordance with an aspect of the present invention.

Figure 3 is a block diagram, indicated generally by the reference numeral 20, of a system in accordance with an aspect of the present invention. The system 20 comprises a first user 22 (typically in the form of a user device, such as a mobile communication device), a second user 24 and an identity management (IDM) system 26. The first user 22 is in two-way communication with both the second user 24 and the IDM 26. As indicated by the dotted arrow, the second user 24 may, in some embodiments, be in two-way communication with the IDM 26.

The first user 22 is similar to the user 12 described above. The second user 24 may be a service provider (similar to the service provider 14 described above), but this is not essential. As discussed in detail below, the second user 24 may be another user, and may therefore be similar to the first user 22 (and may be in the form of a user device, such as a mobile communication device).

Figure 4 is a flow chart showing an algorithm, indicated generally by the reference numeral 30, showing, in broad terms, an exemplary use of the system 20.

The algorithm 30 starts at step 32, where the user 22 generates a set of attributes, referred to herein as a "communication card".

The term communication card is used herein to refer to a dynamically generated set of personal attributes/data of one user (such as the first user 22), triggered and tailored by the subject of these personal data for a specific purpose,

and then optionally sent to his/her communication partner (such as the second user 24). The second user may have the option of sending his specific communication card to the first user as another contribution to build a trusted relationship between the two communicating users, but this is not essential to all forms of the invention.

The communication card could be stored in XML format containing the configuration for the card or a binary format. The communication card may be digitally signed by the IDM 26 to be secure against tampering. Another possible implementation (which is discussed in further detail below) could be that the card would also contain the values of the attributes, encrypted by a digital rights management (DRM) key or other similar method.

Once the communication card has been generated, thereby completing step 32 of the algorithm 30, the algorithm moves to step 34, wherein the communication card is transferred to a communication partner of the first user (the second user 24 in this example).

Finally, at step 36, the second user receives the communication card and uses the communication card to obtain attributes or other user data concerning the first user 22. As discussed in detail below, the attributes may not themselves be included in the communication card sent from the first user to the second user; rather, the communication card enables the second user to obtain that data, for example from the IDM 26. In other forms of the invention, the attributes may be included in the communication card, but in encrypted form.

Figure 5 is a flow chart showing an algorithm, indicated generally by the reference numeral 40, showing further details of how the communication card may be generated in step 32 of the algorithm 30.

The algorithm 40 starts at step 42, where the first user 22 logs into the IDM 26. By way of example, the IDM 26 may provide a personal data portal that the first user 22 needs to login to in order to generate communication cards.

The personal data portal may, for example, be used to store both the user's personal identity attributes (e.g. address, photos, etc.) and the user's privacy preferences (e.g. regarding the forwarding of his/her personal ID attributes). The profile data for the user 22 may be viewable at the personal data portal.

Next, at step 44 of the algorithm 40, the first user 22 selects a sub-set of the user attributes to be included in a particular communication card. The subset may, for example, be selected by activating one or more checkboxes at the personal data portal of the IDM 26. Of course, this step could be implemented in many other ways; for example, the user could modify an existing communication card or the subset of attributes could be selected automatically, perhaps based on a generic set of attributes which is filtered by the user's pre-defined privacy preferences or some other policy regarding the communication cards.

In one form of the invention, the personal data portal may generate a communication card and then enable the first user 22 to edit the card according to his/her personal preferences in this moment and situation, e.g. by removing/adding or abstracting or otherwise generalizing certain personal data.

With the content for the communication card defined, the first user 22 may now define one or more validity conditions for the card at step 46 of the algorithm 40. For example, the first user 22 may define that the user attributes should only be made available to the second user for a limited period of time.

By way of example, the communication card could contain attributes with varying viewing policies and access durations. For example, the first user 22 could determine that the second user 24 should be able to see his mobile telephone number for one year, but see his current location (which would be an on-demand fetchable attribute) for one month. After one month the second user 24 should be able to see his location for another five months in an abstracted way (e.g. just the town) and then the location attribute should no longer be visible to the second user.

Finally, the first user 22 selects one or more recipients of that communication card (step 48 of the algorithm 40). This may be done, for example, by moving to a new page at the IDM 26, where group of persons (given the case that his IDM offers to sort his contacts to groups) that should be allowed to see the communication card can be selected.

It should be noted that the algorithm 40 is provided by way of example only. The order of steps could readily be altered. For example, the recipient(s) of the communication card could be selected earlier in the process. Further, one or more of the steps could be omitted; for example, validity conditions (step 46 of the algorithm) may not be required in all circumstances. Moreover, the generation of the communication card could be implemented in other ways; for example, the communication card could be generated automatically, perhaps by selecting those attributes that are acceptable based on the user's privacy preferences for sending attributes to a particular recipient.

With the communication card generated, the first user 22 could now download the communication card first to his device or directly forward it to another service or person (such as the second user 24), thereby implementing step 34 of the algorithm 30.

As mentioned above, the communication card does not generally include the user attributes for the first user, but includes information required to enable the second user to obtain those details. In order for the second user to view attributes for the first user (thereby implementing step 36 of the algorithm 30), the second user may obtain the attributes from the IDM 26 (as described below with reference to Figure 6). In an alternative implementation, the second user needs to decrypt the values that were already stored in the card (as described below with reference to Figure 7), for example using DRM technology.

Figure 6 is a flow chart showing an algorithm, indicated generally by the reference numeral 50, showing an exemplary implementation of step 36 of the algorithm 30.

The algorithm 50 starts at step 52, where the second user 24 receives the communication card, for example from the first user 22. The communication card includes information required to enable the second user to obtain those details. Accordingly, at step 54 of the algorithm 50, the second user 24 fetches the required attributes from the IDM 26 in accordance with the information included in the information card received at step 52, for example in accordance with the principles outlined above.

Figure 7 is a flow chart showing an algorithm, indicated generally by the reference numeral 60, showing an alternative implementation of step 36 of the algorithm 30.

The algorithm 60 starts at step 62, where the second user 24 receives the communication card, for example from the first user 22.

Next, at step 64, the second user obtains the information required to decode the user data included in the communication card. For example, the second user may need to acquire and validate his DRM key (or similar technique) to be

able to decrypt the values that were already stored in the card. This can be done e.g. by applying WS-* protocols or a SAML AttributeQuery. For the authorization of the access there could be included within the card a special access token. Of course, step 64 could be implemented before step 62 in the algorithm 60.

Finally, at step 66, the second user 24 decodes the data included in the communication card to extract the user data.

The card generated at step 32 of the algorithm 30 may be an XML file containing an encrypted block. For decryption, the combination of the encryption algorithm used, keys used for encryption and any other parameters is required. The step 66 of the algorithm 60 may be implemented using a communication card viewer. Such a viewer might typically be implemented as a piece of software and/or hardware. The viewer understands the encryption algorithm used, but needs to acquire the keys necessary to decrypt the data included in the encrypted block of the XML file, initialize the decoding algorithm and perform the decryption. In order to do so, the communication card viewer may retrieve some data from external sources and authorize itself against the external sources.

Figure 8 is a block diagram of a system, indicated generally by the reference numeral 80, in accordance with an aspect of the present invention.

The system 70 comprises a first user 72 (similar to the first user 22 described above), a second user 74 (similar to the second user 24 described above), a first IDM system 76 (similar to the IDM system 26 described above) and a second IDM system 78.

The first user 72 is in two-way communication with the second user 74, the first IDM system 76 and the second IDM system 78. Similarly, the second user 74 is in two-way

communication with the first user 72, the first IDM system 76 and the second IDM system 78.

Figure 9 is a flow chart showing an algorithm, indicated generally by the reference numeral 80, showing an exemplary use of the system 70.

The algorithm 80 starts at step 82, where the first user 72 generates a communication card. The communication card may be generated for the purpose of sending the communication card to the second user 74, for example using the algorithm 40 described above.

The communication card generated in step 82 is sent to the second user 74 at step 84 of the algorithm 80. The second user uses the communication card to obtain attributes regarding the first user, for example by obtaining the attributes from the first IDM 76 (step 86 of the algorithm 80).

The algorithm 80 then moves to step 88, where the second user 74 generates a communication card for the purpose of sending the communication card to the first user 72. The second user may, for example, use an algorithm similar to the algorithm 40 for this purpose.

The communication card generated by the second user 74 is sent to the first user 72 (step 90). Finally, at step 92 of the algorithm 80, the first user uses the communication card to obtain attributes regarding the second user, for example by obtaining the attributes from the second IDM 78.

After both the first 72 and second 74 users have sent their specifically tailored communication cards, then each user is potentially aware of a customized selection of ID attributes of his/her communication partner. Thus the invention allows asymmetric exchange of personal data, under the individual governance of the two communication partners.

In the event that a relationship between two users deteriorates, then each individual user may be able to disable the communication card sent to his/her communication partner remotely. For example, in the event that the communication cards enable only a copy-protected display of the communication card to be streamed to the communication partner, driven by the real data stored only in a user's personal data portal, then the communication card can be disabled by relying on technology from Digital Rights Management (DRM) for videos and paper documents like the technology behind MS Sharepoint and similar other products. Basically, the receiver of such protected information is able to "see" it for a certain period of validity (as mentioned above with reference to step 46 of the algorithm 40), and is unable to forward it to third parties. This usage right can be extended periodically, e.g. for another day, as long as there is a relationship between the two users. As soon as the relationship is deemed by one partner as deteriorating, this partner can stop the periodic extension of the usage right. Consequently, his/her partner is no longer able to read the information.

Figure 10 is a block diagram of a block diagram of a system, indicated generally by the reference numeral 100, in accordance with an aspect of the present invention. The system 100 comprises the first user device 72, second user device 74, first IDM 76 and second IDM 78 of the system 70 described above.

As shown in Figure 10, the first user device 72 comprises a processor 110, a memory 112 and a user interface 114. The processor is configured, for example, to implement the algorithms described above. The code required for implementing those algorithms may be stored within the memory 112. The user interface 114 enables the user of the user device 72 to interact with the device 72, and hence provide the input required to select the content for inclusion in a

particular communication card. The second user device 74 comprises a processor 116, which is similar to the processor 110, a memory 118, which is similar to the memory 112, and a user interface 120, which is similar to the user interface 114.

As shown in Figure 10, the first IDM 76 comprises a processor 102 and a memory 104. The processor is configured, for example, to implement the algorithms described above. The code required for implementing those algorithms may be stored within the memory 104. The memory 104 may also store the user attributes that are selectively included in the communication cards described herein. The second IDM 78 comprises a processor 106, which is similar to the processor 102, and a memory 108, which is similar to the memory 104.

The system 100 is provided by way of example only. The skilled person will be aware of many alternatives possible implementations of the principles of the present invention. For example, a similar system implementing the system 20 described above could readily be implemented using the user devices 72 and 74 to provide the user devices 22 and 24 of the system 20 and the IDM 76 to provide the IDM 26 of the system 20, but omitting the IDM 78.

In the embodiments of the invention described above, the communication card not only provides fine-grained enforcement of each user's privacy preferences, but also enhanced user convenience, since, for example, no unwanted or outdated or redundant information need be stored at a communication partner (such as the second user 24). Indeed, in many implementations of the invention, it would not be possible for the second user to store such data.

Moreover, the information stored on a communication card can be tailored by individual and/or group/company privacy policies. Communication cards can also be tailored asymmetrically and updated dynamically, based on changes of

the user's ID attributes. By way of example, as soon as the user gets a new telephone number, this new number is seen by selected communication partners of the first user, as long as they can watch his/her communication card. In the event that a user loses his end device, data loss is avoided since they are streamed from the data portals of its partners in real-time.

The embodiments of the invention described above are illustrative rather than restrictive. It will be apparent to those skilled in the art that the above devices and methods may incorporate a number of modifications without departing from the general scope of the invention. It is intended to include all such modifications within the scope of the invention insofar as they fall within the scope of the appended claims.

CLAIMS:

1. A method comprising:

receiving instructions from a first user for the generation of a list of user attributes of said first user for sending to a communication partner, wherein the list of user attributes is a subset of user attributes of the first user;

generating said list of user attributes; and

providing said list in a form that enables the said communication partner to obtain the user attributes included in said list.

2. A method as claimed in claim 1, wherein the first user selects at least some of said user attributes for inclusion in said list.

3. A method as claimed in claim 1 or claim 2, wherein at least some of said instructions include details of how to modify an existing list of user attributes.

4. A method as claimed in any preceding claim, further comprising the first user selecting one or more recipients of said list.

5. A method as claimed in any preceding claim, further comprising the first user defining validity conditions for one or more of said user attributes.

6. A method as claimed in claim 5, wherein validity conditions include a time period during which a selected user attribute is available to be viewed.

7. A method as claimed in 5 or claim 6, wherein validity conditions include a level of abstraction of a user attribute.

8. A method as claimed in any preceding claim, wherein said user attributes included in said list are encrypted.

9. A method as claimed in any preceding claim, wherein said user attributes included in said list are obtainable from an identity management system.

10. An apparatus comprising:

a first input for receiving instructions from a first user for the generation of a list of user attributes for the first user, wherein the list of user attributes is a subset of the user attributes for the first user, wherein said the user attributes included in said subset is controlled by the first user;

a processor for generating said list of user attributes; and

a first output for providing said list.

11. An apparatus as claim in claim 10, further comprising a database storing user attributes for the first user.

12. A communication card comprising a list of user attributes for a first user, wherein the list of user attributes is a subset of the user attributes for the first user, wherein said the user attributes included in said subset is controlled by the first user, wherein the list is provided in a form that enables a communication partner to obtain said user attributes included in said list.

13. A communication card as claimed in claim 12, wherein at least some of the user attributes included in said list have limited validity.

14. A communication card as claimed in claim 12 or claim 13, wherein said user attributes included in said list are encrypted.

15. A method comprising:

receiving, at a first user device, a list of attributes from a communication partner, wherein the list is provided in a

form that enables the apparatus to obtain the user attributes included in the list and wherein the user attributes are a subset of the user attributes of said communication partner; and

obtaining the said user attributes.

16. A method as claimed in claim 15, further comprising providing a list of user attributes of a user of said first user device to said communication partner.

17. A computer program product comprising:

means for receiving instructions from a first user for the generation of a list of user attributes of said first user for sending to a communication partner, wherein the list of user attributes is a subset of user attributes of the first user;

means for generating said list of user attributes; and

means for providing said list in a form that enables the said communication partner to obtain said user attributes included in said list.

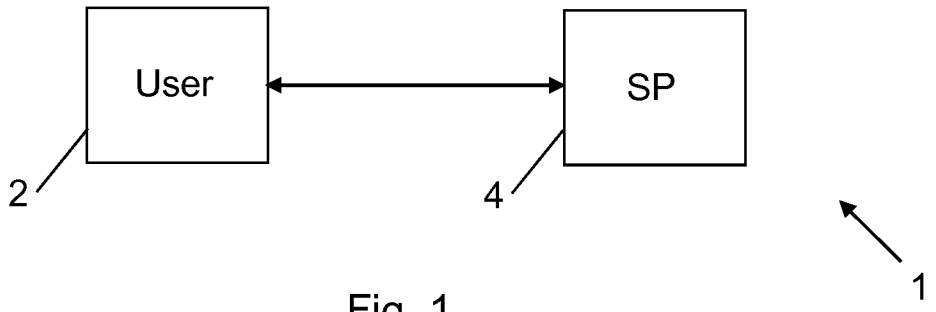

Fig. 1

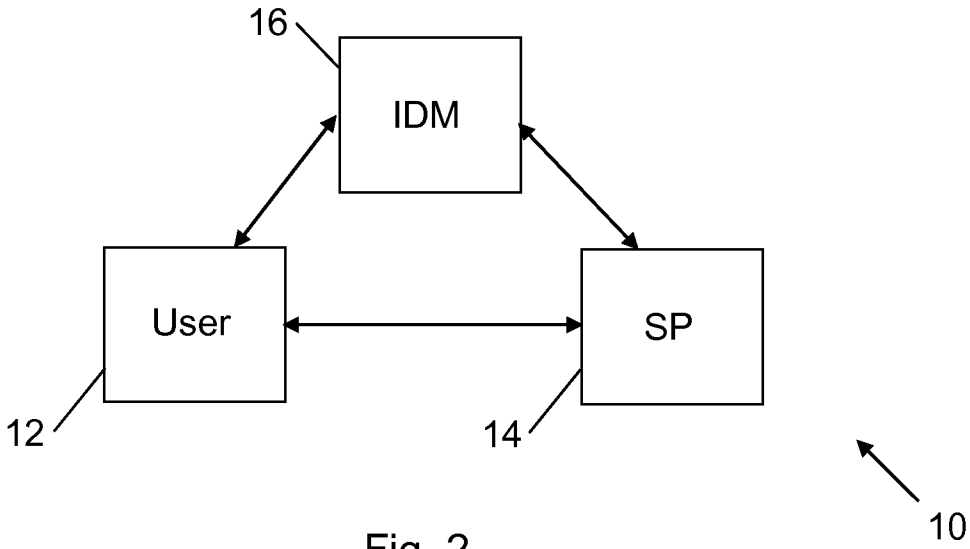

Fig. 2

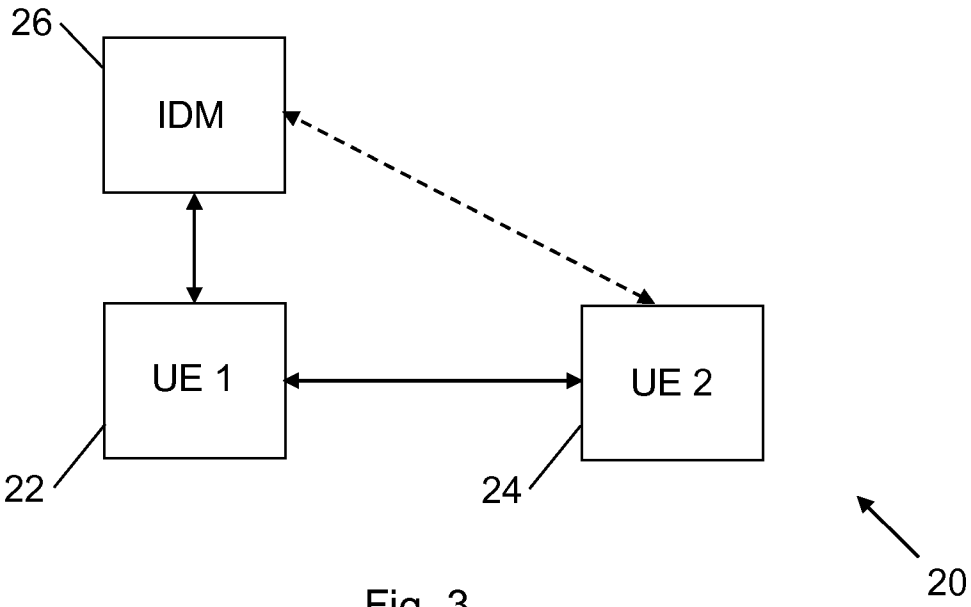
26
IDM
UE 1
UE 2
22
24
20

Fig. 3

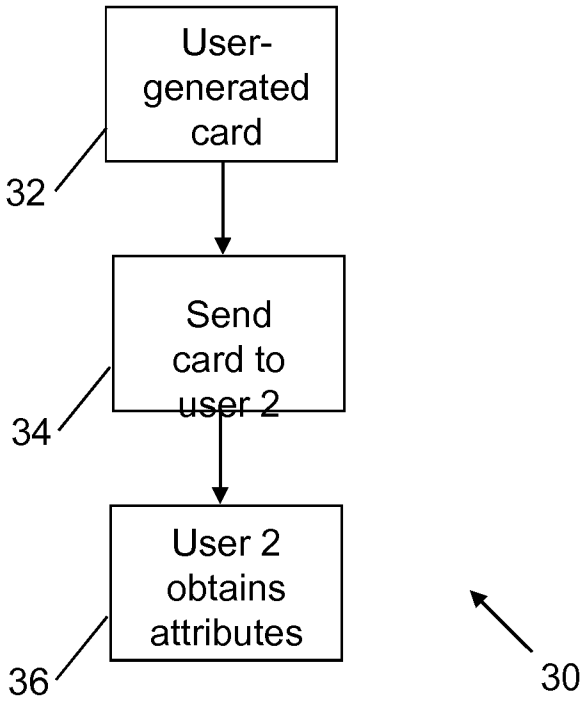
User-generated card
32
Send card to user 2
34
User 2 obtains attributes
36
30

Fig. 4

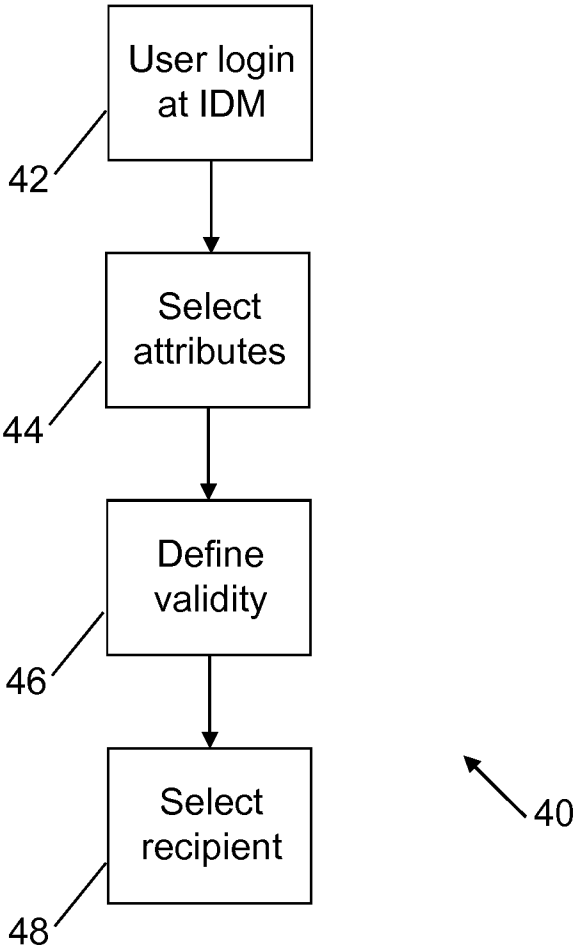
User login at IDM
42
Select attributes
44
Define validity
46
Select recipient
48
40

Fig. 5

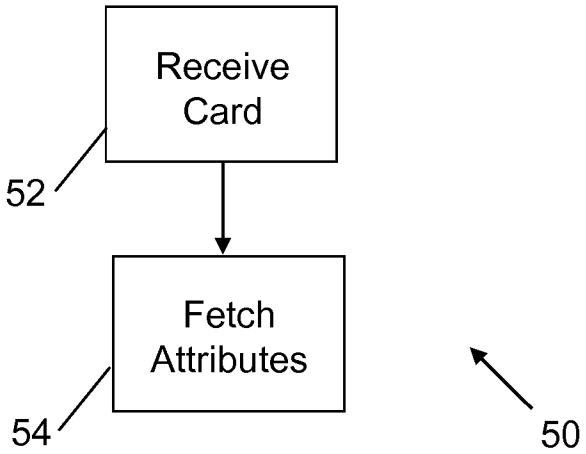
Receive Card
52
Fetch Attributes
54
50

Fig. 6

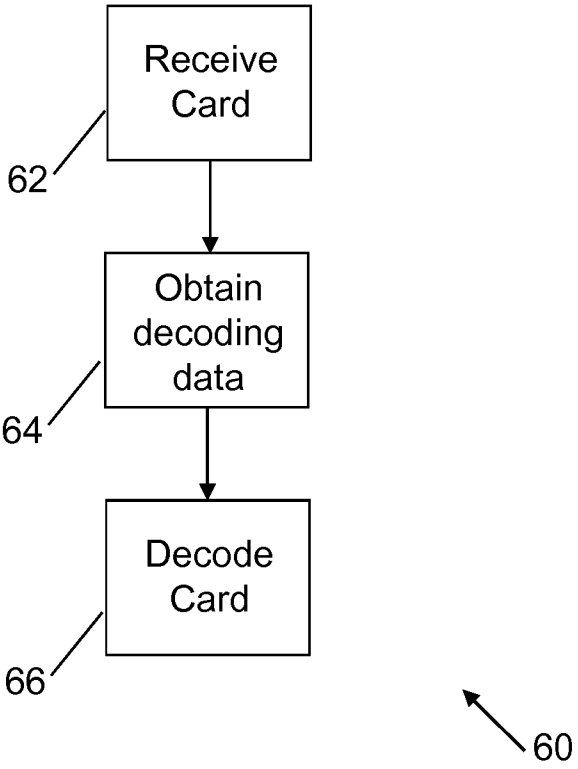
Receive Card
62
Obtain decoding data
64
Decode Card
66
60

Fig. 7

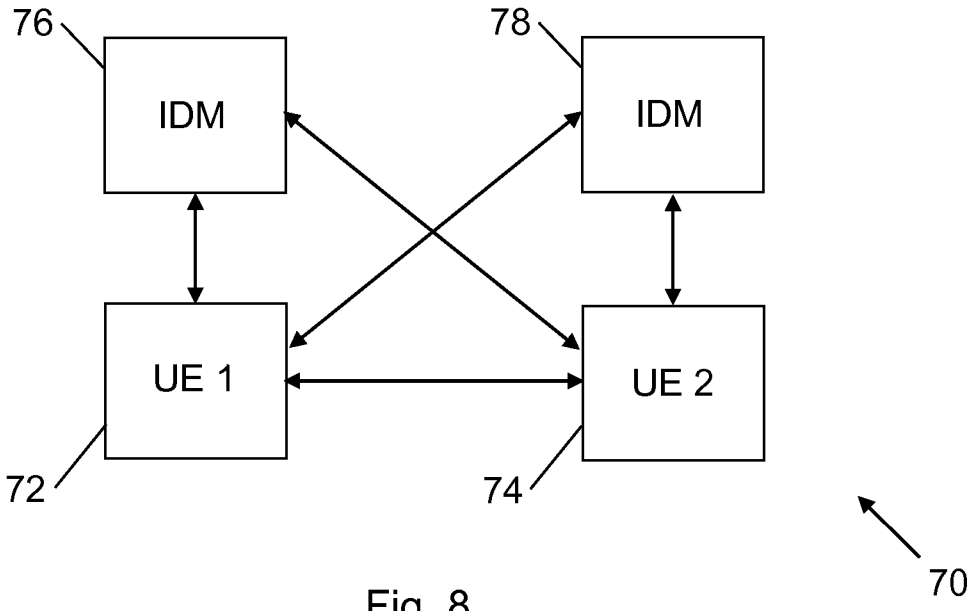
76
IDM
78
IDM
UE 1
UE 2
72
74
70

Fig. 8

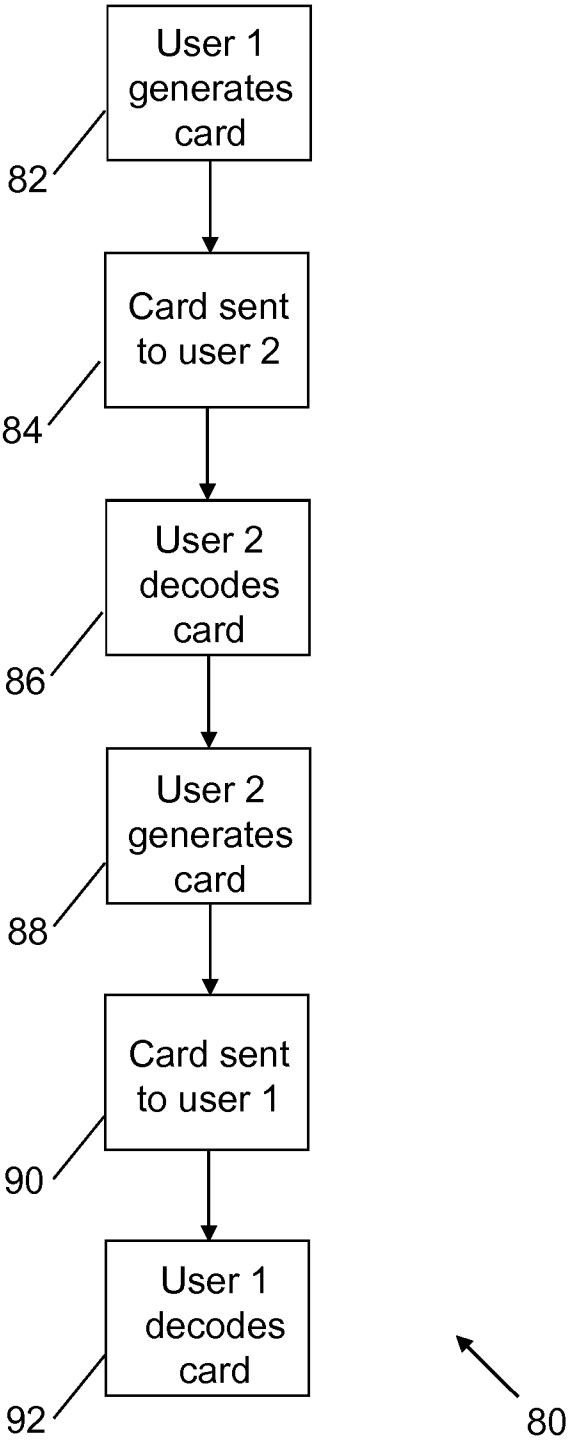
User 1 generates card
82
Card sent to user 2
84
User 2 decodes card
86
User 2 generates card
88
Card sent to user 1
90
User 1 decodes card
92
80

Fig. 9

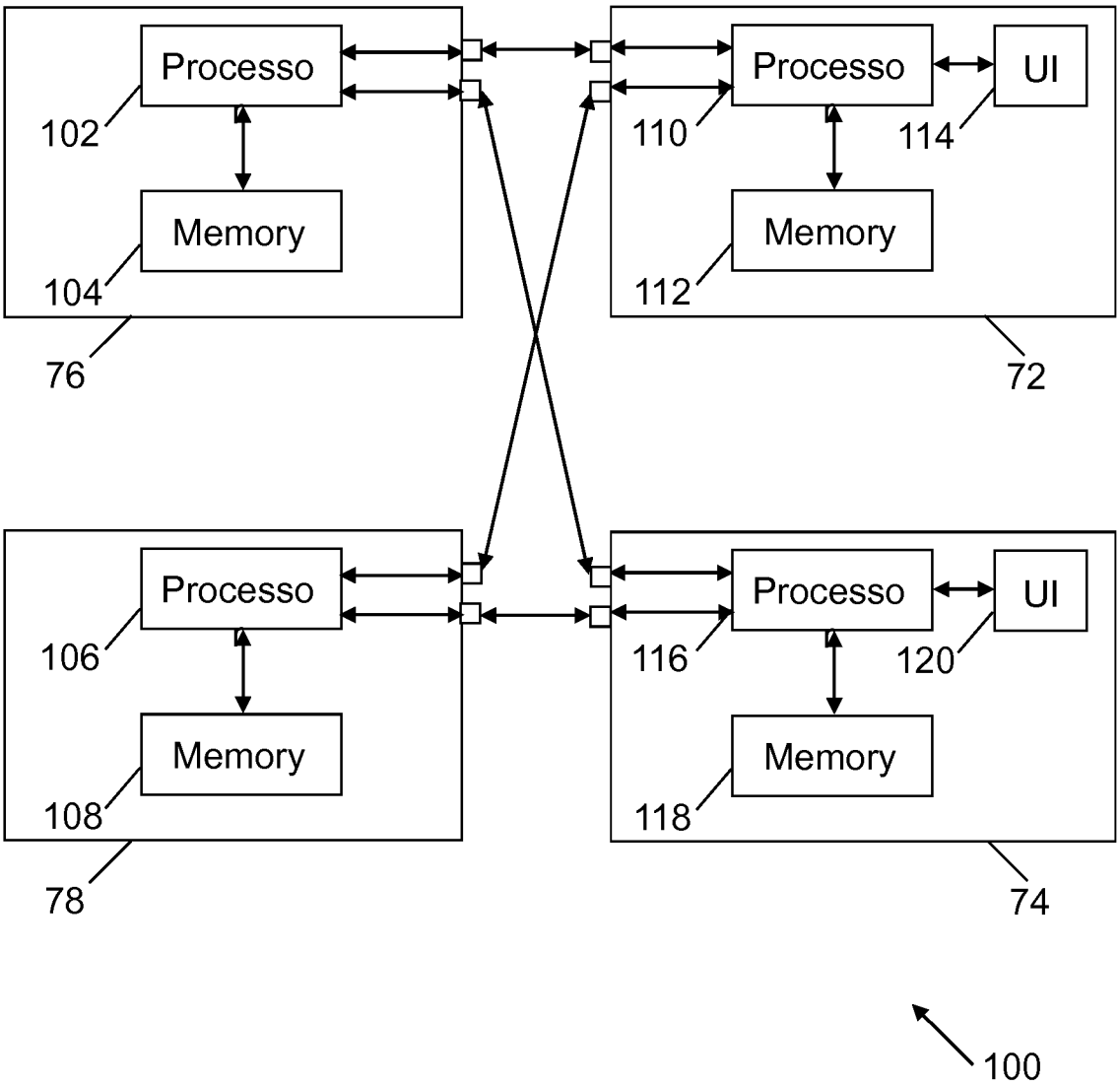
Processo
102
Memory
104
76
Processo
UI
110
114
Memory
112
72
Processo
106
Memory
108
78
Processo
UI
116
120
Memory
118
74
100

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/055652

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q10/00 G06F21/00 H04L29/00
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)
G06Q G06F H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/127239 A1 (SONY ERICSSON MOBILE COMM AB [SE]; APELQVIST JOHAN ANDERS [SE]) 22 October 2009 (2009-10-22) the whole document	1-17
A	US 2003/023726 A1 (RICE CHRISTOPHER R [US] ET AL) 30 January 2003 (2003-01-30) paragraph [0050]	5-7,13

☐ 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	Date of mailing of the international search report
11 January 2012	23/01/2012

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	Gabriel, Christiaan

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/055652

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009127239 A1	22-10-2009	EP 2286376 A1	23-02-2011
		JP 2011517821 A	16-06-2011
		US 2009265794 A1	22-10-2009
		WO 2009127239 A1	22-10-2009
US 2003023726 A1	30-01-2003	AU 2002251979 A1	04-09-2002
		EP 1368724 A2	10-12-2003
		US 2003023726 A1	30-01-2003
		WO 02067089 A2	29-08-2002