(54) Title: AUTHORIZING PROVISION OF DATA IN A COMMUNICATIONS NETWORK

(57) Abstract: A method of passing location data within a communication network to a destination application, the location data being indicative of a geographical position of a mobile telecommunications device, the method including the steps of determining the location data associated with the telecommunications device, receiving from the mobile telecommunications device an access request including the destination application and a security token generated in the mobile telecommunications device, authorising supply of the location data to the destination application based on the security token, supplying the location data to the destination application, and forwarding the access request to the destination application.
AUTHORISING PROVISION OF DATA IN A COMMUNICATIONS NETWORK

FIELD OF INVENTION

5 The present invention relates to authorisation of data transmission within a mobile telecommunications network.

The invention has been developed primarily for use where a subscriber wishes to authorise provision of location data associated with the subscriber's mobile telecommunications device to a third party application, and for the most part will be described in relation to this scenario. However, it will be appreciated that the invention can be applied where other types of data are to be sent, and such data can also be sent to destinations within and outside the communications network.

Also, the invention has been developed for use within third generation (UMTS) networks and will be described primarily with reference to this application. However, it will be appreciated that the invention may have application under many other standards and protocols.

BACKGROUND OF INVENTION

25 Communication systems providing mobility for the users thereof are known. A well-known example of such mobile communication systems is the public land line mobile network (PLMN), of which cellular communications networks are an example. Another example is a mobile communication system that is based, at least partially, on use of communication satellites.

In such systems, the mobile network apparatus and/or user equipment such as a mobile station can be employed for provision of information regarding the geographical location
of the user equipment and thus the user thereof. The position of mobile user equipment, and the equipment's user, can be positioned by various techniques. For example, fairly accurate geographical location information can be obtained based on the known satellite based GPS (Global Positioning System). More accurate location information can be obtained through differential GPS techniques.

Another possibility is to use a location service based on a cellular telecommunications system. In this approach, the cells or similar geographically limited radio access entities and associated controllers of the communication system are utilised in production of at least a rough estimate of the current location of the mobile user equipment. To improve the accuracy of the location information the communication system may be provided with specific location measurement units that provide more accurate data concerning the location of user equipment within the service area of the cellular system. It is also possible to ascertain a geographical location when the mobile user equipment is located within the coverage area of a visited or "foreign" network. The visited network may be made capable of transmitting the location of the mobile user equipment back to the home network, e.g. to support services that are based on location information or for the purposes of routing and charging. The particular way in which location data is produced does not form an essential element of the present invention, and is thus not described in any greater detail herein.

The location data may be processed in a specific location service entity that is implemented either within the cellular system or connected thereto. The location service entity
provided by the communication system may serve different clients via an appropriate interface.

The location information may be used for various purposes, such as for location of a mobile telephone that has made an emergency call, for locating vehicles or given mobile subscribers and so on. In general, a client such as a user equipment UE or another entity wishing to receive location information regarding a user equipment may send a request for such information to the location service provision entity. The location service provisioning entity will then process the request, obtain the required data and generate an appropriate response.

An example of the provision of the location information by a PLMN is described in more detail 3rd Generation Partnership Project (3GPP) technical specifications, see e.g. 3GPP TS 23.271 version 4.2.0, titled “Functional stage 2 description of LCS”, June 2001.

According to the 3GPP specification a location service (LCS) server entity referred to as a Gateway Mobile Location Center (GMLC) is provided for managing the location services. The GMLC is for gathering and storing various data that may be used in provision of location information for location service clients (LCS clients). The LCS Client may make use of that location information for various services/applications. A possible application comprises a LCS client arranged to provide location information in response to a request for non-call related location information. Such a request for location information is referred to in the 3GPP
specifications as a non-call related MT-LR (Mobile Terminated Location Request).

Use of a so-called "Authorized UE List" has been proposed. This list contains Mobile Subscriber ISDN (MSISDN) numbers or groups of MSISDNs which are authorised to initiate a location information provision procedure. That is, MSISDNs or groups of MSISDN are listed for which the LCS Client may issue a non-call related MT-LR. Separate lists of MSISDNs may be associated with each distinct external or non-call related client identity.

The LCS Client who is external to the PLMN system may only be enabled to validly issue location information requests for those MSISDNs that are found on the "Authorized UE List". That is, the LCS client’s request may only be responded for subscribers who subscribe to the location services provided by the PLMN, as their MSISDNs would not otherwise appear on the list.

Requests from the LCS Client are authenticated based on a combination of a Client ID and password stored in an LCS Client profile at the LSC server (e.g. the GMLC) and authorized based on the "Authorized UE List". That is, the LCS client is authorised to receive location information from the GMLC entity if the requesting user equipment (UE) is found from the list.

One difficulty that can arise in this situation is the need for the Authorized UE List to include every UE that has authorised provision of its location information to a particular LCS client. In some cases, such as when the UE is
roaming outside its home network, an access to an LCS client by the UE might be a one-off situation that does not warrant updating of UE authorizations within the network. It would therefore be desirable to allow one-off or occasional access to an LCS application for a UE without needing to update an Authorized UE Authorization List within the network.

SUMMARY OF THE INVENTION

In a first aspect, the present invention provides a method of passing location data within a communication network to a destination application, the location data being indicative of a geographical position of a mobile telecommunications device, the method including the steps of:

determining the location data associated with the telecommunications device;

receiving from the mobile telecommunications device an access request including the destination application and a security token generated in the mobile telecommunications device;

authorising supply of the location data to the destination application based on the security token;

supplying the location data to the destination application; and

forwarding the access request to the destination application.

Preferably, the token is digitally signed data. More preferably, the token is the access request digitally signed. In that case, it is preferred that the access request is signed digitally with a private key, most preferably with the private key of a subscriber associated with the mobile telecommunications device.
In a preferred form, the request includes:
    an address of the destination application;
    a time stamp; and
    a serial number for revoking the token after use.

Preferably, the token takes the form of a one-off password.
More preferably, the time is network time, the mobile telecommunications device using network time as a reference.

In a particularly preferred embodiment, the destination application is an LCS client application.

In one embodiment the application is a WAP gateway.

In a preferred form, the access request is included in an SMS message.

Preferably, the location data is ascertained in a location service client entity adapted for provision of location services for the users of the communication network. More preferably, the location service client is a GMLC/SMLC.

In a second aspect, the present invention provides a method of authorising data transfer within a communication network from a source to a destination application, the method including the steps of:
    receiving from the mobile telecommunications device a request for the data, the request including the destination application to which the data is to be sent and a security token generated in the mobile telecommunications device;
    validating the security token;
authorising supply of the data to the destination application based on validation of the security token; and
supplying the data to the destination application; and
forwarding the access request to the destination application.

Preferably, the data is associated with the telecommunications device. More preferably, the data is location data indicative of a geographical position of a mobile telecommunications device.

It is particularly preferred that the destination application is hosted remote from the communications network. In one form, the destination application is hosted on the mobile telecommunications device.

In a third aspect, the present invention provides communications apparatus within a network for passing location data to a destination application, the location data being indicative of a geographical position of a mobile telecommunications device, the communications apparatus being configured to:

- determine the location data associated with the telecommunications device;

- receive from the mobile telecommunications device an access request including the destination application and a security token generated in the mobile telecommunications device;

- authorise supply of the location data to the destination application based on the security token;

- supply the location data to the destination application;

and
forward the access request to the destination application.

Preferably, the token is digitally signed data. More preferably, the token is the access request digitally signed, most preferably with a private key of a subscriber associated with the mobile telecommunications device.

In a fourth aspect, the present invention provides communications apparatus of authorising data transfer within a communication network from a source to a destination application, the method including the steps of:

- receiving from the mobile telecommunications device a request for the data, the request including the destination application to which the data is to be sent and a security token;
- validating the security token;
- authorising supply of the data to the destination application based on validation of the security token generated in the mobile telecommunications device; and
- supplying the data to the destination application; and
- forwarding the access request to the destination application.

Preferably, the data is associated with the telecommunications device. More preferably, the data is location data indicative of a geographical position of a mobile telecommunications device.

In a preferred form, the destination application is hosted remote from the communications network.
In a preferred embodiment, the destination application is hosted on the mobile telecommunications device.

By using subscriber-based authorisation in this fashion, the need for updating authorisation lists within a network can be avoided where a subscriber wants an entity to send data to or a third party (which could include the subscriber's mobile device). This is especially useful where a subscriber is roaming and may only need to use a service once or at most a small number of times.

BRIEF DESCRIPTION OF DRAWINGS
Preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic overview of entities involved in authorization of an LCS client request, in accordance with the invention; and

Figure 2 is a schematic overview of entities involved in an alternative embodiment of authorization of an LCS client request.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT OF THE INVENTION
It should be appreciated that even though the exemplifying telecommunications network shown and described in more detail uses the terminology of the third generation (3G) UMTS (Universal Mobile Telecommunications System) public land mobile network (PLMN), the proposed solution can be used in any system providing mobile communications for users and some kind of location information service. Examples of other telecommunications systems include, without limiting to these, standards such as the GSM (Global System for Mobile
communications) or various GSM based systems (such as GPRS: General Packet Radio Service), AMPS (American Mobile Phone System) or DAMPS (Digital AMPS), IMT 2000 (International Mobile Telecommunications system 2000), i-phone and so on.

5

Turning to the Figure 1, there is shown an arrangement in which base stations (not shown) of a cellular system 1 provide radio coverage areas within cells 2. Each radio coverage area 2 is typically served by a base station. It should be appreciated that one cell may include more than one base station site. A base station apparatus or site may also provide more than one cell. The shape and size of the cells 2 depend on the implementation and may be different from the illustrated shapes. The shape and size of the cells may also vary from cell to cell. It should be appreciated that in some systems the base station may be referred to as Node B.

User equipment in the form of mobile station (MS) 6 is also shown. It shall be appreciated that typically a number of MSs will be in simultaneous communication with each base station, although for the sake of clarity only a single MS 6 is shown in this case. Each base station is arranged to transmit signals to and receive signals from the MS 6 via a wireless interface, as is well understood by those skilled in the art.

Likewise, the MS 6 is able to transmit signals to and receive signals from the base station.

Each of the base stations is connected to an access network controller such as a radio network controller (RNC) of a UMTS terrestrial radio access network (UTRAN). The radio network controller may be connected to appropriate core network entities of the cellular system, such as a MSC (mobile
switching centre) and/or SGSN (serving general packet radio service support node), via a suitable interface arrangement. These, however, do not form an essential element of the invention and are thus not explained in any greater detail.

5 The location of the MS 6 may vary in time as the user moves within the coverage area of a base station and also from coverage to coverage area. Modern communication systems are capable of providing information regarding the geographical location of an MS within the coverage area thereof. The geographical location may be defined on the basis of the position of the mobile station relative to the base station(s) of the mobile telecommunications network. The geographical location of the user equipment may be defined, for example, in X and Y co-ordinates or in latitudes and longitudes. It is also possible to define the location of the base stations and/or mobile stations in vertical directions.

20 In the examples of Figures 1 and 2, the location service (LCS) functionality of the communication system is provided by a Gateway Mobile Location Center (GMLC) entity 10. The GMLC location service node 10 is for gathering and storing data that is required for the provision of the location information. The location service node 10 is arranged to receive via appropriate interface means information concerning the location of the mobile user equipment from the cellular system.

30 The cellular system may be provided with various means for processing information gathered from the cells and/or some other parameters and/or for computing by processor means
appropriate calculations for determining and outputting the geographical location of the target user equipment. The location information may be obtained by using one or more of the appropriate location techniques. At least a part of the location information may be provided based on information provided by system that is separate from the communication system, such as by means of the Global Positioning System (GPS) or similar. Since there are various possibilities how to implement the location services in the cellular system and since the invention is not dependent on the used location determination technology, these are not described in any greater detail herein.

The location service node may provide the location information in a predefined manner to a destination application 12. Such destination applications can include any entity that makes use of the location information, and can be considered a logical functional entity that may make a request to the location service entity 10 for the location information of one or more target MSs.

As shown by Figure 1, the destination application 12 can be external to the communication network 1, the client entity 12 being provided in an ASP domain 4. The destination application can alternatively be an internal client (ILCS) residing in any entity or node (including a mobile station) within the communication system 1.

The destination application is entitled to receive at least some degree of information concerning the location (or location history) of the MS 6. The particular requirements and characteristics of a destination application is typically
known to the location service server of the communication system by its LCS client subscription profile.

A location server associated with the GMLC 10 provides a platform supporting location based services in parallel with other telecommunication services such as speech, data, messaging, other teleservices, user applications and supplementary services. The location server may thus be configured to provide the destination application 12, on request or periodically, the current or most recent geographic location (if available) of the target user equipment or, if the location fails, an error indication and optionally the reason for the failure. A more detailed description of a LCS entity that may be employed in the embodiments of can be found e.g. from the above referenced 3GPP technical specification No. 3GPP TS23.271.

Middleware including a server 11 manages requests for location data from the external application 12. In particular, it is able to communicate with a privacy profile register 13 that stores data relating to the security tokens that can be sent by a user.

In the embodiment in Figure 1, the user of MS 6 wishes to use a service associated with external application 12. However, in this case the MS 6 is roaming away from its home network and the service is not listed in any authorization list associated with the MS 6. Rather than generate or update any such authorisation list for the MS within the network, the MS 6 is configured to send a token 14 to be transmitted to middleware. The token means that the user wants to skip the normal privacy checks and authorize a location request,
irrespective of whether the LCS Client in question is in his/her privacy profile. The token 14 includes the LCS client ID (effectively the address of the application 12), a time stamp and a serial number. The time stamp is generated on the basis of the network clock, with which the MS 6 is synchronised. It will be appreciated that the time synchronisation can be done by other means, such as, for example, access to a remote time source via the internet, as long as the Privacy Profile Register and MS are on the same time. The data in the token is digitally signed by the MS 6 using a private key. Typically, this will be the private key of the subscriber that is operating the MS 6.

Signing can be handled by a WIM (WAP Identity Module)/SWIM (Subscriber WAP Identity Module), as presently proposed under WAP 1.2.1, with reference to ETSI 11.11 and 11.14.

Alternative methods of generating the security token can also be used. For example, by using a secure programming platform on the MS 6, encryption software can be installed and used to generate the token. There are already some applications for Secure Computing Platform (SCP) in terminals. The Nokia 9210 Communicator, for example, provides a basic SCP, although other secure platforms yet to be developed or released commercially can also be used.

The request is routed via the network to the application 12, which decodes the request and forwards the token on to middleware server 11. The middleware refers to the privacy profile register 13 to verify the digital signature of the token. This is done in accordance with standard principles, which involves ensuring that the signature provided in
relation to the token was, in fact, generated by the MS 6 sending the access request. Verification of digital signatures is well known to those skilled in the art, and so will not be described in detail in this specification.

Once the digital signature has been verified, the middleware also ensures that the request has been received within a predetermined time of generation, by using the timestamp. The serial number of the token is checked to ensure that the token has not been presented previously. This is to prevent duplicates of authentic tokens being used to illegitimately gain access to services once the original token has been verified.

Assuming all of these checks are passed, the token serial number is recorded to ensure that the token cannot be used again, and the middleware server 11 passes the requisite location data from the GMLC/SMLC to the application 12.

Handling of private keys must be done in a secure manner, as is well known to those skilled in the art. It is not the intention of the present invention to overcome any of the usual problems and restrictions of PKI, distribution of keys and verification of certification.

Turning to the embodiment of Figure 2, again a token 14 is generated in the MS 6 and sent to the destination application 12 via the network. To generate the token, the MS 6 uses an algorithm based on a crypto-graphic. The algorithm is able to generate unique keys by using, for example, the following three initial values:

- secret key
- time
- initialization value (e.g. PIN)

These provide an isometric number/value that can be used as a one-time-password. The password is time dependent, and so is constantly changing with the time value used. The encrypted value can be transmitted via the LCS Client to the Privacy Profile Register and no digital signature is needed. PPR knows the same initial values and compares own, active one-time-password and the one that user has sent. If the values match, the token can be validated.

The location data itself can take the form of simple coordinate (x, y) information or contain more value added services like a reverse-geocoded response provided with a street name or a map reference. The response may even comprise a map and a pointer on the map.

In an alternative embodiment, the invention can be applied to the case where the mobile telecommunications apparatus wants to authorise transfer of data to itself. Using the location data example from the preferred embodiment, a mobile communications equipped personal digital assistant (PDA) can send a security token to the network along with a request for location data relating to its own location. The security token is again used within the network to ascertain that the authorisation is valid for the subscriber sending the request, and once validated, the data is sent to the PDA. Again, the need for checking authorisation lists associated with the subscriber’s mobile telecommunications device is avoided.
It is also possible for additional commands and parameters to be added to the access request or token. For example, information telling the network what type of device is sending the request can be included, as can time limits for token validity or any other data that is needed or useful for supplying data to the device via the network.

An exemplary token is:

```
TOKEN
Serial#: 902805935
Time: 14.13:02:2|24012002
APP#: aa_presence_server
Command: set_user_away
Command_param1: time=2h
Signature: 20ueGDS()ase"#hy9p8aq4y890
```

It will be noted that in this case the token is valid for two hours from when it is sent.

It should be appreciated that the elements of the location service functionality may be implemented anywhere in the telecommunications system. The location service implementation may also be distributed between several elements of the system.

Furthermore, although the above describes embodiments employing a specific LCS client node, this is not a necessity. The request for location information may be addressed directly to a location service entity of the communication system, such as to the GMLC or any other
element associated with the provision of location information. If a LCS client is used, it does not need to be an external element, but may also be implemented within the communication network and/or be run by the operator of the network.

Moreover, whilst the preferred embodiments describe the location (or other) data as being processed and sent from middleware within the network, this is not a strict requirement. For example, a third party outside the network could provide the data being requested by the subscriber. It is preferred that authorisation still take place within the network, but again this is not mandatory.

It should be appreciated that whilst embodiments of the present invention have been described in relation to user equipment such as mobile stations, embodiments of the present invention are applicable to any suitable type of user equipment such as PDAs or mobile telephones (whether or not WAP/internet enabled).

Although the invention has been described with reference to a specific example, it will be appreciated that the invention can be embodied in many other forms.
CLAIMS:

1. A method of passing location data within a communication network to a destination application, the location data being indicative of a geographical position of a mobile telecommunications device, the method including the steps of:
   determining the location data associated with the telecommunications device;
   receiving from the mobile telecommunications device an access request including the destination application and a security token generated in the mobile telecommunications device;
   authorising supply of the location data to the destination application based on the security token;
   supplying the location data to the destination application; and
   forwarding the access request to the destination application.

2. A method according to claim 1, wherein the token is digitally signed data.

3. A method according to claim 2, wherein the token is the access request digitally signed.

4. A method according to claim 1 or 2, wherein the access request is signed digitally with a private key.

5. A method according to claim 4, wherein the private key is that of a subscriber associated with the mobile telecommunications device.
6. A method according to any one of claims 2 to 5, wherein the request includes:
   an address of the destination application;
   a time stamp; and
   a serial number for revoking the token after use.

7. A method according to claim 1, wherein the token takes the form of a one-off password.

8. A method according to claim 7, wherein the password supplied by the mobile telecommunications device is time dependent.

9. A method according to claim 8, wherein the time is network time, the mobile telecommunications device using network time as a reference.

10. A method according to claim 8 or 9, wherein the destination application is an LCS client application.

11. A method according to any one of the preceding claims, wherein the application is a WAP gateway.

12. A method according to any one of the preceding claims, wherein the access request is included in an SMS message.

13. A method according to any one of the preceding claims, wherein the location data is ascertained in a location service client entity adapted for provision of location services for the users of the communication network.
14. A method according to claim 13, wherein the location service client is a GMLC/SMLC.

15. A method of authorising data transfer within a communication network from a source to a destination application, the method including the steps of:
   - receiving from the mobile telecommunications device a request for the data, the request including the destination application to which the data is to be sent and a security token generated in the mobile telecommunications device;
   - validating the security token;
   - authorising supply of the data to the destination application based on validation of the security token; and
   - supplying the data to the destination application; and
   - forwarding the access request to the destination application.

16. A method according to claim 15, wherein the data is associated with the telecommunications device.

17 A method according to claim 15 or 16, wherein the data is location data indicative of a geographical position of a mobile telecommunications device.

18. A method according to any one of the preceding claims, wherein the destination application is hosted remote from the communications network.

19. A method according to any one of the preceding claims, wherein the destination application is hosted on the mobile telecommunications device.
20. Communications apparatus within a network for passing location data to a destination application, the location data being indicative of a geographical position of a mobile telecommunications device, the communications apparatus being configured to:

determine the location data associated with the telecommunications device;
receive from the mobile telecommunications device an access request including the destination application and a security token generated in the mobile telecommunications device;
authorise supply of the location data to the destination application based on the security token;
supply the location data to the destination application;
and
forward the access request to the destination application.

21. Communications apparatus according to claim 20, wherein the token is digitally signed data.

22. Communications apparatus according to claim 21, wherein the token is the access request digitally signed.

23. Communications apparatus according to claim 20 or 21, wherein the access request is signed digitally with a private key.

24. Communications apparatus according to claim 23, wherein the private key is that of a subscriber associated with the mobile telecommunications device.
25. Communications apparatus according to any one of claims 21 to 24, wherein the request includes:
   an address of the destination application;
   a time stamp; and
   a serial number for revoking the token after use.

26. Communications apparatus according to claim 20, wherein the token takes the form of a one-off password.

27. Communications apparatus according to claim 26, wherein the password supplied by the mobile telecommunications device is time dependent.

28. Communications apparatus according to claim 27, wherein the time is network time, the mobile telecommunications device using network time as a reference.

29. Communications apparatus according to claim 27 or 28, wherein the destination application is an LCS client application.

30. Communications apparatus according to any one of claims 20 to 29, wherein the application is a WAP gateway.

31. Communications apparatus according to any one of claims 20 to 30, wherein the access request is included in an SMS message.

32. Communications apparatus according to any one of claims 20 to 31, wherein the location data is ascertained in a location service client entity adapted for provision of location services for the users of the communication network.
33. Communications apparatus according to claim 32, wherein the location service client is a GMLC/SMLC.

34. Communications apparatus of authorising data transfer within a communication network from a source to a destination application, the method including the steps of:
   receiving from the mobile telecommunications device a request for the data, the request including the destination application to which the data is to be sent and a security token generated in the mobile telecommunications device;
   validating the security token;
   authorising supply of the data to the destination application based on validation of the security token; and
   supplying the data to the destination application; and forwarding the access request to the destination application.

35. Communications apparatus according to claim 34, wherein the data is associated with the telecommunications device.

36. Communications apparatus according to claim 34 or 35, wherein the data is location data indicative of a geographical position of a mobile telecommunications device

37. Communications apparatus according to any one of claims 34 to 36, wherein the destination application is hosted remote from the communications network.

38. Communications apparatus according to any one of claims 34 to 37, wherein the destination application is hosted on the mobile telecommunications device.
FIG. 1

Core Network
PPRs (ip) address can be within HLR

External Applications
Service

Middleware

Privacy Profile Register

1. LCD Client ID
   Time Stamp
   Serial Number
   Signature

2. GMLC / SMLC

3. Ok / Failed

4. 12

5. 10

6. 11
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04Q7/38

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 H04Q

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 98 52379 A (ERICSSON TELEFON AB L M) 19 November 1998 (1998-11-19) page 3, line 20 -page 5, line 22 page 9, line 8 - line 18 claims 1,13</td>
<td>1,15,18, 20,34</td>
</tr>
<tr>
<td>A</td>
<td>EP 1 139 688 A (HEWLETT PACKARD CO) 4 October 2001 (2001-10-04) column 9, line 44 -column 10, line 16</td>
<td>1-32</td>
</tr>
<tr>
<td>A</td>
<td>WO 01 28155 A (ERICSSON TELEFON AB L M) 19 April 2001 (2001-04-19) page 3, line 24 -page 4, line 20 claim 1</td>
<td>1-32</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C.

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 prior art claims 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
  *X* 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
  *Y* 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 novel or 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
  *X* document member of the same patent family

Date of the actual completion of the international search: 8 May 2003

Date of mailing of the international search report: 16/05/2003

Name and mailing address of the ISA
European Patent Office, P. B. 5818 Patentlaan 2 NL - 5201 HV Blispark
Tel: (+31) 70 540 3040, Tx: 31 601 epo nl, Facs (+31) 70 540 3016

Authorized officer: Dionis, M
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AU 753854 B2</td>
<td>31-10-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 7558298 A</td>
<td>08-12-1998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BR 9809817 A</td>
<td>20-06-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1256848 T</td>
<td>14-06-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 0963675 A1</td>
<td>15-12-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 9701845 A</td>
<td>17-11-1998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6442391 B1</td>
<td>27-08-2002</td>
</tr>
<tr>
<td>EP 1139688 A</td>
<td>04-10-2001</td>
<td>DE 60100071 D1</td>
<td>06-02-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1139688 A2</td>
<td>04-10-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2001320759 A</td>
<td>16-11-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002004399 A1</td>
<td>10-01-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 3915799 A</td>
<td>10-02-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1248135 A</td>
<td>22-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2000078667 A</td>
<td>14-03-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 7821400 A</td>
<td>23-04-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1377560 T</td>
<td>30-10-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1377540 T</td>
<td>30-10-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1224822 A1</td>
<td>24-07-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1216538 A1</td>
<td>26-06-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2003511771 T</td>
<td>25-03-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2003511970 T</td>
<td>25-03-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0126401 A1</td>
<td>12-04-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0128155 A1</td>
<td>19-04-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 516779 C2</td>
<td>26-02-2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 0001996 A</td>
<td>02-04-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 9903560 A</td>
<td>02-04-2001</td>
</tr>
</tbody>
</table>