(12) UK Patent Application (19) GB (11) 2 414 140 (13) A

(43) Date of A Publication 16.11.2005

(21) Application No: 0509660.7

(22) Date of Filing: 11.05.2005

(30) Priority Data:
(31) 0410495 (32) 11.05.2004 (33) GB

(71) Applicant(s):
**Startlok Limited**
**(Incorporated in the United Kingdom)**
**Willow House, Golden Valley,**
**HORSLEY WOODHOUSE, Derbyshire,**
**DE7 8BA, United Kingdom**

(72) Inventor(s):
**Khawar Hameed**
**Mark Andrew Heath**

(74) Agent and/or Address for Service:
**Withers & Rogers LLP**
**Goldings House, 2 Hays Lane, LONDON,**
**SE1 2HW, United Kingdom**

(51) INT CL[7]:
**H04Q 7/32**

(52) UK CL (Edition X ):
**H4L** LACX

(56) Documents Cited:
**WO 2004/089016 A1** **WO 1999/024894 A1**
**WO 1997/032284 A1** **US 20020005774 A1**
**US 20010021950 A1**

(58) Field of Search:
UK CL (Edition X ) **H4L**
INT CL[7] **G06F, G07C, H04M, H04Q**
Other: **Online databases: EPODOC & WPI.**

(54) Abstract Title: **Electronic Device Security**

(57) A method of authorising the operation of an electronic device and particularly an electronic communications device such as a mobile telephone (10) or a personal data assistant (PDA). The device is symbiotically linked to a transponder (20) and an external database which verifies the device to transponder (20) relationship.

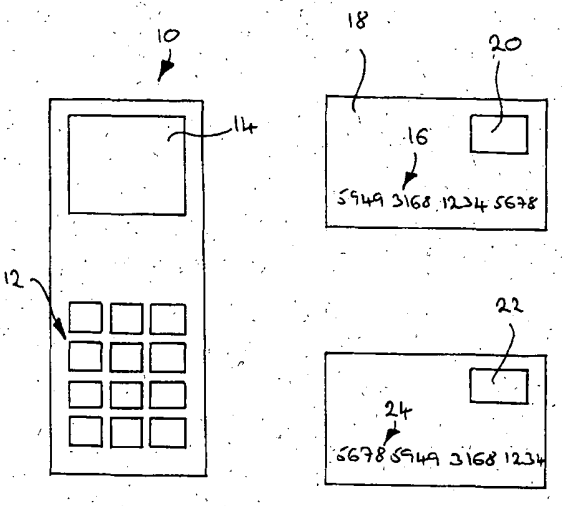


Fig. 1

GB 2 414 140 A

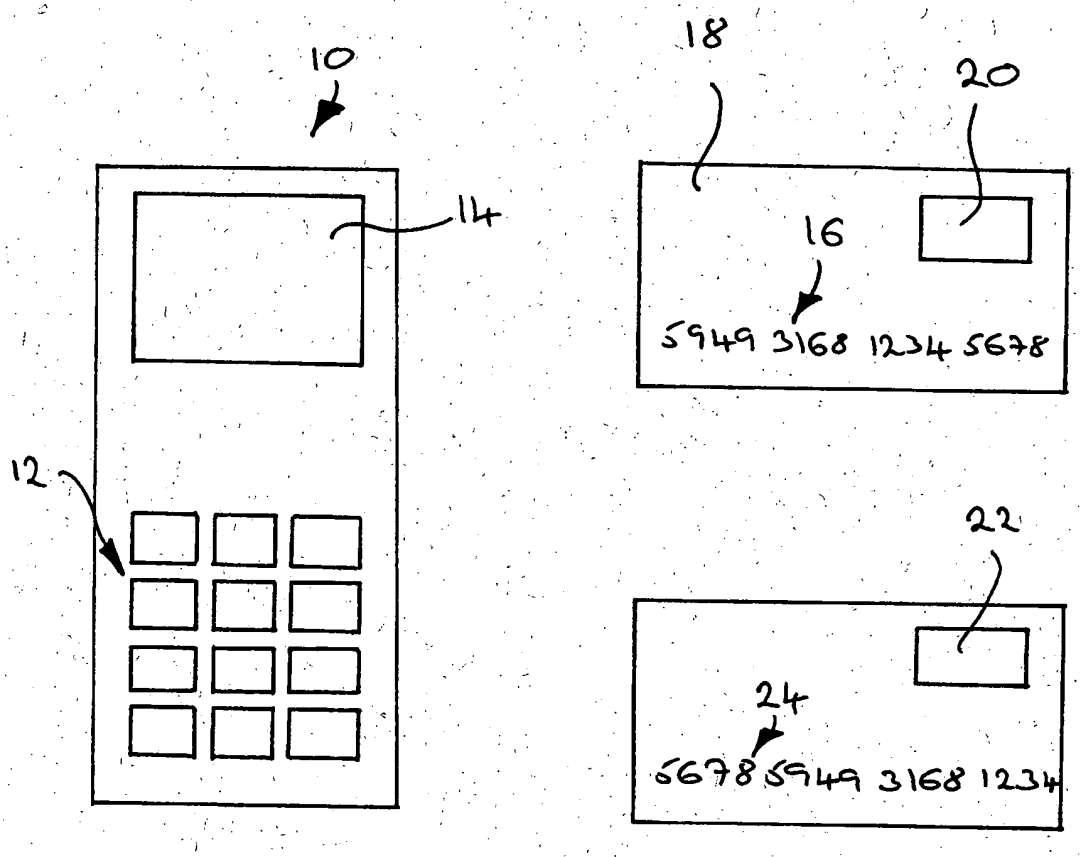


Fig. 1

P710319GB-1

# Improvements in or Relating to Electronic Device Security

The present invention relates to the security of electronic devices and in particular, though not exclusively, to the security of mobile telephones and mobile personal data assistants, commonly referred to as PDA's.

With the increasing popularity of mobile telephones there has unfortunately been a corresponding increase in the instances of mobile telephone related crime. In 2001 in the UK alone over 700,000 mobile telephone handsets were stolen, with most being taken during street robberies. Mobile telephone operating companies are generally able to disable a handset after being informed of its theft so as to prevent unauthorised use. Unfortunately it is possible with the correct knowledge and equipment to bypass the steps taken to disable the handset and thereby render it usable.

According to the present invention there is provided a method of authorising the operation an electronic communications device comprising the steps of:

providing an electronic device having an integral controller;

providing a transponder remote from and separate to the electronic device, the transponder being arranged to correspond with the controller; and

configuring the controller to permit normal operation of the electronic device in response to information received from the transponder and to restrict normal operation of the device in the absence of information received from the transponder, wherein initial start up of the device comprises the steps of:

placing the electronic device within range of the transponder,

initiating an activation sequence of the electronic device, wherein the electronic device sends an interrogation signal to the transponder, which in turn sends a replies to the electronic device,

the electronic device relaying information relating to both the identity of the device and the transponder to a remote location and receiving authorisation from said remote location to commence normal operation of the device.

The present invention provides that the operation of the electronic device is symbiotically linked to the presence of the transponder and to an external database which is able to verify the validity of the device to transponder relationship. The database is able to communicate with the device and can modify the functional ability of the device, which is to say that the database may instruct the device to provide only certain functions to the holder of the transponder. While specific reference is made to an electronic communications device, it will be appreciated that the present invention may be used in conjunction with other types of electronic device.

Communication between the device and the database is made via communications means within the device, Communication between the database and the device may be conducted through communication channels such, for example, GSM or GPRS systems, or via the Internet.

The step of initiating the activation sequence of the electronic device may include the step of manually entering an activation code into the device. The activation code may comprise a string of characters which can be inputted into the device via an input means of the device. The input means may comprise a keyboard or keypad of the device. The activation code may be supplied to a user with the transponder. For example, the activation code may be provided on the transponder in the form of a sticker or printed text. Alternatively the activation code may be supplied on a card which accompanies the transponder.

The step of initiating the activation sequence comprises the steps of inputting a plurality of activation codes into the device. The use of more than one activation code may be employed in situations where security is paramount For example, the device may require an initial activation code to cause the device to activate, and a subsequent activation code to cause the device to correspond with the transponder and then communicate with the remote location. The subsequent activation code may be referred to as a relationship identity code which initiates communication between the device and the transponder.

The relationship identity code or RID is preferably supplied to the user in a secure manner and separately from the device and transponder. For example, the RID may be sent to the user via a secure email communication.

The remote location with which the device communicates includes a database arranged to verify the identity and status of the device and the transponder. The database includes a register which contains information relating to the identity of the transponder and device such as, for example, a unique identity code. The database can verify that the correct transponder is being paired with the electronic device and that neither the device nor the transponder are listed as being lost or stolen. The authorisation subsequently sent to the electronic device may permit the user to use all of the functions of the device or merely a selection thereof.

The method may include the additional step of causing the electronic device to correspond periodically with the database to verify the identity of the device and transponder. If the device and or transponder are lost, stolen or otherwise separated from the user, then the user can inform the database accordingly. When the device next corresponds with the database an update can be sent to the device to alter the operational profile of the device. The provision of this feature enables the use of the device to be restricted in the event that both the transponder and device are separated from the user but are still in symbiotic contact with one another.

The database may be configured to correspond with the electronic device and alter the operational parameters of the electronic device in response to the database being informed of a change of status of the electronic device and/or transponder. This alteration may be due to the user informing the database of the loss or theft of the device as noted above. Alternatively, the alteration may be due to the user of the device switching to a different service plan. In certain circumstance the database may alter the operational profile of he device to prevent the use of the electronic device. The database may instruct the device to erase information contained within the electronic device. The information may be contained within a memory of the device or on a removable data carrier of the device. The database may comprise more than one

database element. For example, the database may comprise an authorisation and control database element, and an authentication database element.

In the embodiment described, the step of receiving information from the transponder comprises the steps of the integral controller sending an interrogation signal and the transponder in response thereto sending a reply signal. The controller may send the interrogation signal either continually, periodically or intermittently.

The step of restricting the normal operation of the electronic device may comprise the controller within the device placing the device in one of a temporary dormant state and a permanent dormant state. The device may be placed in to the temporary dormant state in the event that the controller fails to receive a reply signal from the transponder in reply to the interrogation signal. The failure to receive a reply signal may be caused by a number of factors, for example the transponder being moved out of range of the device. While in the temporary dormant state the controller continues to send the interrogation signal. Upon entering the temporary dormant state the normal operation of the device may be either partially or wholly restricted. The device may be removed from the temporary dormant state in the event that the controller receives a reply signal from the transponder within a predetermined time limit since the receipt of a prior reply signal. In such an event the controller removes the restrictions placed upon the normal operation of the device. The temporary dormant advantageously prevents third parties from accessing specific user or device data from the device in the event that the device is obtained from the authorised user without their consent.

The electronic device may be placed in the permanent dormant state in the event that no reply to the interrogation signal is received by the controller within a predetermined time period. Upon entering the permanent dormant state the controller ceases to send the interrogation signal.

The present invention seeks to improve the security of electronic devices, and in particularly mobile communication devices such as mobile telephones by providing an

activation and continued operation system which is resistant to unauthorised modification, alteration or fraudulent abuse. The present invention further provides a means of disabling and or restricting the functional aspects of an electronic device in the event of its theft or loss. The invention also provides a method of verifying the identity of a electronic device prior to the initial activation thereof.

An embodiment of the present invention will now be described with reference to the accompanying drawing in which there is shown a schematic representation of the invention. In the figure there is shown a mobile telephone handset generally designated 10. The handset 10 is of a conventional type having a keypad 12 and a display 14 and is able to make and receive voice calls and SMS messages in a conventional manner, and may further be able to transmit and receive data in the form of broadcast or distributed content and visuals, and permit peer to peer data and content interchange. Within the body of the handset 10 there is provided a SIM or USIM card (not shown) or equivalent which links the operation of the handset to a service provider and further allows information specific to the user to be stored therein. Such information may include, for example, a telephone number directory, contents scheduler, personal data, ring tones and text messages. Other information which may be stored includes banking and payment information, access registration information, personal identity information and closed user group data. Alternatively, the above mentioned information may be stored within an internal memory of the handset 10. The handset is provided with a security system according to the present invention.

Typically the handset 10 is supplied to an end user in a deactivated state and before use must be activated. The security system is also deactivated and must be activated prior to use. Activation of the handset 10 and security system may be achieved simultaneously by the inputting into the handset 10 via the keypad 12 a numerical activation code or string 16 which may, for example, be provided on a card 18 supplied with the handset 10. With the handset 10 activated the card 18 can be discarded, it is preferably be retained in the event that further re-activations and de-activations are required.

In an alternative embodiment activation of the handset 10 and security system may be achieved separately. For example, the handset 10 may be activated by the input of the activation code 10, while the security system may be activated by the input of an additional activation code, as will be described in greater detail below.

A typical GSM mobile telephone, once activated, communicates with the its network using two identification measures. The first of these is known as the International Mobile Equipment Identity or IMEI. This comprises a unique fifteen digit code which identifies the handset 10. As the IMEI is not portable it cannot subsequently be assigned to another piece of hardware. Furthermore the IMEI is assigned to the hardware in such a way that it cannot be altered. The second identification measure is known as the International Mobile Subscriber Identifier or IMSI. This comprises a code which is associated with the SIM or USIM card.

In the event of the handset being lost or stolen, commands specific to the IMEI and IMSI can be sent by either the network provider or agents of the network provider to bar both the handset 10 and the SIM card. If the SIM only is barred then the phone handset itself may still remain valuable as it can be used in conjunction with other non-barred SIM cards. If, on the other hand, the handset only is barred, for example by listing the IMEI in a table known as the Equipment Identification Register or EIR, then the SIM card may still be used to make calls in another non-barred handset. The barring of the SIM card and handset can be done relatively quickly, however this can only be done after the network provider has been informed of the loss or theft of the handset 10.

It will be appreciated that circumstance may lead to a significant time delay before the SIM or handset 10 are barred, for example when the user is not aware that the handset 10 is missing. This provides a window of opportunity when the handset 10 may be used without permission and/or be acted upon so as to be resistant to any subsequent network initiated disablement procedures.

In accordance with the present invention operation of the handset 10, once activated, is made dependent upon another electronic device. In the embodiment shown in the drawing, the card 18 bearing the activation code 16 is provided with an electronic transponder 20 which can be interrogated by the handset 10. Advantageously the transponder comprises a radio device which is energised or interrogated by, but not limited to, electromagnetic energy emanating from the handset 10. The transponder 20 is intended to be carried about the person of the user so that it is kept within a specified distance of the handset 10. The distance is not normally specified by the user but takes into account their intended use profile for the handset 10. For example the distance may be five to ten metres. Taking the example of the transponder 20 being incorporated into a card 18, the card 18 may be carried in a wallet of the user. Alternatively the transponder may, for example, be incorporated into an article which is worn by the user such as an item of jewellery.

In use, the handset 10 continually sends out a signal consisting of small periods of communication which is specific to the transponder 20. The signal interrogates the transponder 20 which sends a reply to the handset 10. Continued operation of the handset 10 is dependent upon receiving a reply from the transponder 20.

In the event that the handset 10 fails to receive a response, for example where the distance between the handset 10 and the transponder exceeds the above mentioned specific distance, then the handset 10 places itself into a temporary dormant state. In this temporary dormant state operation of the handset 10 is disabled, however the periodic transponder interrogation signal is continued. Should the handset 10 subsequently receive a response from the transponder 20 then the handset 10 removes itself from the temporary dormant state and is able to function normally. The degree to which the handset 10 is disabled may be specified by a number of parties such as the user, handset supplier network provider or, in the case of a business provider, the business operator.. For example the handset may be partially disabled yet it still may be able to receive calls but unable to make them.

Should the handset 10, when in the temporary dormant state, fail to receive a response from the from the transponder 20 within a specified time period, then the handset assumes a permanent dormant state. In the permanent dormant state the handset 10 remains disabled and further ceases to send the transponder interrogation signal. Once in the permanent dormant state the handset 10 can only be reactivated by the re-entry of the activation string 16 in the presence of the transponder 20 via the keypad 12. Further verification checks, discussed in greater detail below, may also be undertaken.

It will be appreciated that the provision of the temporary dormant state enables the handset 10 to be automatically reactivated once it re-establishes contact with the transponder 20. The duration of the temporary dormant state may be specified by the user, handset supplier, network provider or business operator and accommodates instances where the handset 10 is separated from the transponder unintentionally. Such a separation may occur when the handset 10 is left overnight in a car or office and recovered the following morning by the user.

Upon entering the permanent dormant state, the handset 10 may be configured so as to undertake additional functions over and above remaining inactive to a greater or lesser degree. For example data stored on the SIM card may be erased and or the Digital Signal Processor or DSP disabled thereby rendering the handset unusable. Such additional functions may also be instructed remotely by an authorised third party.

Initial activation of the handset 10 is conducted as follows. The handset 10 is supplied with a card 18 bearing an activation string 16 and an electronic transponder 20. For the sake of simplicity the transponder is shown incorporated in the card bearing the activation string, however it will be appreciated that the handset 10 may be supplied with the transponder 20 separate from the activation string 16. The transponder 20 supplied with the handset is known as the master transponder and is provided with a unique identification code or TID. Upon initial start-up of the handset 10, and after registering with a mobile network, the handset 10 looks for the presence of the master transponder 20 by sending out a generic signal which is not specific to any individual master transponder 20. The signal interrogates the transponder 20 which sends a

transponder specific reply to the handset 10. Upon receiving the reply the handset 10 may then prompt the user to input the activation string 16. If this manual input method is required then the handset 10 then checks that the activation string 16 correlates with the master transponder TID. In the event that the string 16 and TID do not match, then the handset 10 will fail to operate. Advantageously the handset 10 will communicate the mismatch to the user and allow them an opportunity to re-input the string in case the mismatch is due to an input error. The user may be permitted a limited number of attempts to input the correct string. Further proprietary security mechanisms may be incorporated into the transponder 20 and handset 10 to validate the authenticity of a the above referenced activation procedure.

Assuming that that the activation string 16 and TID are correct, then the handset 10 communicates with a database or 3rd party authentication centre in order to authorise the subsequent operation of the handset 10. The handset 10 communicates with the database in an encrypted message format using, for example, SMS (Short Message Service) or MMS (Multimedia Message Service) formats. The handset 10 communicates to the authentication centre the TID of the master transponder 20 and the IMEI of the handset 10, and optionally the SIM or USIM IMSI and other information which may be deemed necessary. Such information may comprise details of the aforementioned proprietary security systems. The database checks that the TID and IMEI are both valid and authentic, and further verifies that the TID and IMEI are correct for each other. Upon confirming that all is in order, the database sends an activation instruction to the handset 10 which permits free operation thereof. The TID, IMEI and any further information supplied to the database is stored securely for possible future retrieval.

An additional layer of security relating to the initial start up and pairing of the transponder 20 with the handset 10 may be provided. Such a step may be utilised in high security and/or business applications of the present invention In order to commence the interrogation of the transponder 20 by the handset 10 and the subsequent communication of the handset 10 with the remote database the input of a further activation code may be required. This further code may be referred to as the

relationship identification code or RID. The RID is preferably supplied to the user in a secure manner, for example by email to a secure address which has been provided by the intended user of the handset 10.

Once the handset 10 has undergone initial activation by the input of the activation code 16, the handset 10 may be instructed to remain operational in the presence of one or more additional transponders 22. The additional transponders 22 are hereinafter referred to as slave transponders as they can only be associated with a handset 10 after it has been activated by the master transponder 20. The slave transponders 22 may not need to be authorised by the authentication centre before being associated with handset 10, however the slave transponders 22 on their own cannot be used for initial activation of the handset 10.

For example, the handset 10 may be intended to be shared between a number of users and hence each is provided with their own transponder 22. The linking of the handset 10 to the additional transponders 22 may be effected by the input of additional activation codes 24. In an alternative embodiment, a user may be provided with a number of slave transponders 22 which may be secreted about their person or property to enable use of the handset 10. Slave transponders 22 may be placed in or about the user's home and working environment, transport means and items of personal property such as apparel, handbags, wallets and the like. A user would be supplied with sufficient slave transponders 22 to ensure that one or more is always in the vicinity of the handset 10 when it is in their possession. The master transponder 20 and activation string 26 can then be kept in a safe place in case they are subsequently needed to remove the handset 10 from the dormant state described above.

While the above described embodiment relates to mobile telephone handsets, the invention is applicable to the security of other types of electronic device. For example, the operation of high value domestic appliances such as televisions, computers, multimedia devices such as DVD players and the like may be dependent upon them receiving a response from a transponder in their vicinity. The transponder may be carried on the person of a homeowner with the result that the electrical appliances can

only function when the homeowner is present within their home. Alternatively the transponder may be hidden somewhere within the home with the result that devices removed from the home, for example by a burglar, are rendered inoperative.

## Claims

1. A method of authorising the operation an electronic communications device comprising the steps of:

providing an electronic device having an integral controller;

providing a transponder remote from and separate to the electronic device, the transponder being arranged to correspond with the controller; and

configuring the controller to permit normal operation of the electronic device in response to information received from the transponder and to restrict normal operation of the device in the absence of information received from the transponder, wherein initial start up of the device comprises the steps of:

placing the electronic device within range of the transponder,

initiating an activation sequence of the electronic device, wherein the electronic device sends an interrogation signal to the transponder, which in turn sends a replies to the electronic device,

the electronic device relaying information relating to both the identity of the device and the transponder to a remote location and receiving authorisation from said remote location to commence normal operation of the device.

2. A method as claimed in claim 1 wherein the step of initiating the activation sequence of the electronic device includes the step of manually entering an activation code into the device.

3. A method as claimed in claim 2 wherein the step of initiating the activation sequence comprises the steps of inputting a plurality of activation codes into the device.

4. A method as claimed in claim 3 wherein one of said activation codes is a relationship identify code which initiates communication between the device and the transponder.

5. A method as claimed in claim 4 wherein the relationship identity code is supplied to the user in a secure manner.

6. A method as claimed in any preceding claim wherein said remote location includes a database arranged to verify the identity and status of the device and the transponder.

7. A method as claimed in claim 6 and including the step of causing the electronic device to correspond periodically with the database to verify the identity of the device and transponder.

8. A method as claimed in claim 7 wherein the database is configured to correspond with the electronic device and alter the operational parameters of the electronic device in response to the database being informed of a change of status of the electronic device and/or transponder.

9. A method as claimed in claim 8 wherein the database is configured to prevent the use of the electronic device.

10. A method as claimed in claim 8 or claim 9 wherein the database is configured to erase information contained within the electronic device.

11. A method as claimed in any of claims 6 to 10 wherein said database comprises an authorisation and control database, and an authentication database.

12. A method as claimed in any preceding claim wherein the step of the electronic device receiving information from the transponder comprises the steps of the controller sending an interrogation signal and the transponder in response thereto sending a reply signal.

13. A method as claimed in claim 12 wherein the controller is operable to send the interrogation signal either continually, periodically or intermittently.

14. A method as claimed in any preceding claim wherein the step of restricting the normal operation of the electronic device comprises the controller placing the device in one of a temporary dormant state and a permanent dormant state in the absence of receiving a response from the transponder.

15. A method as claimed in claim 14 wherein the step of placing the device in the temporary dormant state occurs in the event that the controller fails to receive a reply signal from the transponder in reply to the interrogation signal.

16. A method as claimed in claim 14 or claim 15, wherein the controller continues to send the interrogation signal while the device is in the temporary dormant state.

17. A method as claimed in any of claims 14 to 16 wherein upon entering the temporary dormant state the normal operation of the device is one of partially or wholly restricted.

18. A method as claimed in any of claims 14 to 17 wherein the device is removed from the temporary dormant state in the event that the controller receives a reply signal from the transponder within a predetermined time limit since the receipt of a prior reply signal.

19. A method as claimed in any of claims 14 to 18 wherein the device is arranged to sound an alarm to indicate that it is in the temporary dormant state.

20. A method as claimed in any of claims 14 to 19 wherein the device is placed in the permanent dormant state in the event that the no reply to the interrogation signal is received by the controller within a predetermined time period.

21. A method as claimed in claim 20 wherein upon entering the permanent dormant state the controller ceases to send the interrogation signal.

22. A method as claimed in any preceding claim wherein once normal operation of the device has been authorised, the device may be instructed to operate in response to a reply signal received from an additional transponder.

23. A method as claimed in claim 22 wherein the device may be instructed to operate in response to reply signals received from one or more additional transponders.

The Patent Office

INVESTOR IN PEOPLE

**Application No:** GB0509660.7 16 **Examiner:** Riz Mohammad

**Claims searched:** All **Date of search:** 7 September 2005

## Patents Act 1977: Search Report under Section 17

**Documents considered to be relevant:**

| Category | Relevant to claims | Identity of document and passage or figure of particular relevance |
|---|---|---|
| X | 1 at least | US2001/021950 A1 [HAWLEY et al]; Entire document. |
| X | 1 at least | WO99/24894 A1 [STOBBE et al]; Entire document. |
| X | 1 at least | WO97/32284 A1 [THORP]; Entire document. |
| X | 1 at least | US2002/005774 A1 [RUDOLPH & KIRKHAM]; Entire document. |
| A,E | N.A. | WO2004/089016 A1 [WAKIM et al] |

Categories:

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |

**Field of Search:**

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

H4L

Worldwide search of patent documents classified in the following areas of the IPC[07]

G06F; G07C; H04M; H04Q

The following online and other databases have been used in the preparation of this search report

Online databases: EPODOC & WPI.