(54) **Title:** PROCEDURE FOR STORING ALPHANUMERICAL INFORMATION SENT BY A MOBILE PHONE TO A STORAGE CENTRE CONNECTED TO THE NETWORK

(57) **Abstract:** The present invention relates a procedure for storing alphanumerical information, such as for example telephone numbers and names of a phonebook, to a storage centre connected to the network, and for the subsequent retrieval and storage of the same to the phone memory or to a SIM card inserted therein, where said storagecentre comprises at least one electronic computer provided with a memory divided in as many memory benches as the number of users enabled to use the data storage service, wherein the mobile phone implements an encryption algorithm whose key consists of a password that can be entered by the phone’s user, and where the information storage and retrieval procedures are based on an exchange of simple SMS mesages suitably encrypted.
Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
PROCEDURE FOR STORING ALPHANUMERICAL INFORMATION SENT BY A MOBILE PHONE TO A STORAGE CENTRE CONNECTED TO THE NETWORK

*** *** ***

DESCRIPTION

Field of application

The present invention relates to the mobile communications field. In particular, it relates to a procedure for storing alphanumerical information, such as for example telephone numbers and relevant names, sent by mobile phones, for example GSM phones, or by the cards contained therein (SIM), at a data storage centre accessible by the phone users via the transmission and reception of SMS messages.

Prior Art

As known, current mobile phones are provided with an electronic circuitry and with a memory space that allow storing a certain amount of alphanumerical information, thereby giving the users the possibility to create a digital phonebook integrated in the telephone, or in the SIM card inserted therein.

Such possibility of electronic storage of the information, however, exhibits the disadvantage in that if the mobile phone or the SIM card are damaged, all data stored are lost and cannot be retrieved or transferred to a new phone.

It is therefore advisable to always store and have a hard copy of
telephone numbers, data or other information stored in the mobile phone.

**Objects and summary of the invention**

Object of the present finding is to obviate the above disadvantage by providing mobile phone users with the possibility of storing their alphanumerical information, such as for example telephone numbers and associated names, at a special data storage centre connected to the network, and of retrieving said information, storing it to the phone memory and to the SIM card again every time the users wishes so, through the exchange of SMS messages with said storage centre.

Another object of the present invention is to provide a procedure for storing the phonebook of a mobile phone to a special storage centre in a confidential and safe manner, without any risk for the user data of being intercepted during transfer over the network or being read when stored to the data storage centre.

Such new function of mobile phones therefore allows the users to create a strictly confidential copy of their phonebook, or of any information in general, storing it to a memory area external to the phone, so that even when the user is forced to replace his mobile phone or the relevant SIM card, he can retrieve his information and store it again to the new phone or SIM card.

Such objects and resulting advantages are achieved by a
procedure for storing alphanumerical information sent by a mobile phone to a storage centre connected to the network according to at least claim 3, reported hereinafter.

**Brief description of the drawings**

Further features of the finding will appear more clearly with reference to the attached indicative and non-limiting drawings. In such drawings:

- Figure 1 shows a flow chart relating to the data storage request by the user;
- Figure 2 shows a flow chart relating to the data storage operation by the storage centre;
- Figure 3 shows a flow chart relating to the data retrieval request by the user;
- Figure 4 shows a flow chart relating to the data transmission operation from the storage centre to the requesting user.

**Detailed description of the invention**

The storage procedure under discussion uses the data computation and processing capabilities provided by mobile phones and requires a computer, provided with a wide memory area, performing the function of data storage centre. Such computer must be connected to the telephone network and can belong directly to the service provider, or to any board authorised by one or more providers.

In this way, any mobile phone supporting wireless connection to
the storage centre can send properly encrypted SMS messages to the centre containing the information to be stored, such as for example names and relevant phone numbers. The storage centre computer is configured to recognise messages and store their contents to a memory area reserved to the calling subscriber. The computer memory can therefore be divided in as many memory benches as the number of users enabled to use the data storage service provided by the service provider.

When the user needs to retrieve stored data, he sends a data request message to the storage data. The computer recognises the message and the sender, and generates a reply containing the requested information in an encrypted form. When the reply message reaches the user's mobile phone, it is decrypted and written to the phone memory or to the SIM card.

It should be noted that the user may request to retrieve both a single information as well as all data previously stored with a single request.

This second option is especially useful and convenient when the user has to replace his phone or SIM card, since he can quickly store his phonebook to the new mobile phone.

As regards message encryption/decryption, i.e. the information confidentiality protection, current GSM mobile phones are provided with an electronic circuitry capable of implementing encryption algorithms, such as for example symmetric algorithms A3, A5 and
A8 currently used in GSM communication systems for all message authentication and masking procedures. As encryption key, the user is required to enter a password both before sending the messages containing the information to be stored, which must therefore be encrypted, and upon reception of the messages from the storage centre, which must be decrypted. The user can then choose whether each piece of information should be associated to a password, or the same password may be used for all information, as it is advisable.

Below is a description of a possible sequence of actions for implementing the data storage function under discussion.

INFORMATION STORAGE (USER SIDE)

Fig. 1

a) The user associates the information to be stored, for example a telephone number and an alphanumerical information, if any, such as a name associated to the number, to a memory position of the mobile phone or of the SIM card. Such position will then be used to indicate the information to be retrieved to the storage centre. If the information to be stored is also stored to the phone, the relevant position may be preceded by letter T. In addition, if the memory position is already occupied by a previously stored information, the user is warned. It should be noted that the information to be stored may be directly typed by the user, or retrieved from the phonebook or from incoming calls.
b) The user is required to select whether he wants to store the selected information.

c) If so, the user is required to enter a password to encrypt the information to be stored.

d) The mobile phone generates an SMS message consisting of the encrypted information, of a number in plain text denoting the relevant memory position, and of a control character of the message integrity, called CRC.

e) The SMS message is sent to the storage centre, which returns a confirmation message.

f) If the user receives the confirmation message within a fixed time, this means that the storage operation was successful, and a signal is displayed on the stored memory position to inform the user that the information associated to such memory position has already been stored.

INFORMATION STORAGE (STORAGE CENTRE SIDE)

Fig. 2

The storage centre activates every time it receives a message, and it performs the following operations:

g) Checks the sender's number: if it comes from a subscriber who is not up-to-date with payments, the message is automatically rejected and the procedure ends.

h) Checks the message type: if it is in plain text, it performs the information retrieval procedure (described hereinafter), while if it is
encrypted, it continues this procedure.

i) Analyses the control character of the message integrity (CRC): if the message is corrupted, storage is not performed.

j) Reads the memory position occupied by the information in the SIM or in the phone, as it is in plain text. In this latter case, the memory position may be preceded by a T.

k) Stores the encrypted portion of the message to the memory position corresponding to the subscriber. If the position is already taken, it is overwritten. A function is also provided to record all storage operations performed.

l) Generates an SMS message for confirmation, which is sent to the same number that has sent the storage request. The message contains the memory position and is composed so that the telephone may recognise it.

m) It is advisable to also provide for the user's reception notification, so as to be sure that the procedure was successful (and that the phone has reported the successful storage to the memory position).

INFORMATION RETRIEVAL (USER SIDE) – Fig. 3

The user decides which memory position he wants to retrieve. A request for retrieving all information is also possible, which will generate a request procedure with a jolly position number (indicated, for example, by "**") This causes the transmission of all information stored at the centre.
An information retrieval request message is therefore generated, containing the requested position number. If the user has changed telephone and telephone number, he must notify the change to the storage centre, proving his rights on the old telephone number. The message is in plain text since it does not contain confidential information and this makes it easy to distinguish it from messages containing storage information.

n. The user receives the message containing the retrieved information from the storage centre; such messages is composed as those sent by the telephone upon the storage request, and it contains a single phonebook position: for multiple retrievals, messages are received in a sequence. If the message received does not come from the backup centre, it is ignored by this procedure; if it comes from the centre but is corrupted, it is deleted and the user receives a notification.

o. The user enters the password to decrypt the retrieved information. For multiple retrievals and if the user has selected to associate a single password to all memory positions, the password of the previous position can be reconfirmed with a single key without having to retype it again.

p. The retrieved information is displayed as check: if the password is wrong, a senseless sequence of characters is displayed.

q. Once the user has checked that the information is correct, he authorises its storage to the memory (to the SIM card or to the
phone), or he cancels the operation and types in a new password.

r. The information is written to the original position. If the position is already taken, the user is prompted to confirm overwriting.

s. The phone records that the memory position contains an information with an already stored copy; this is necessary in the (very probable) event that the SIM card and/or the phone have been replaced.

INFORMATION RETRIEVAL (STORAGE CENTRE SIDE) – Fig. 4

The procedure starts any time the storage centre receives a message in plain text from a regular user; preliminary checks have already been performed by the storage procedure.

t. The storage centre reads the requested memory position from the SIM or from the telephone. In this latter case the memory position may be preceded by a T. If a jolly character ("*"") is read in place of the position number, the procedure generates a sequence of messages equal to the number of positions stored. On the other hand, if a single position is requested, a single message is generated.

u. The information retrieval SMS message is therefore generated and sent to the same number that has transmitted the request. Besides the information requested, the message also contains the memory position and is composed exactly as the storage request messages received. A specific function records all operations performed.
v. It is advisable to handle the user's reception notification so as to be sure that the procedure was successful and that the phone has received and stored the requested information (and that the indication that the retrieved information has a copy at the storage centre has been set).

w. A specific function will report any transmission errors for the relevant manual checks.

x. If further memory positions have to be transmitted (multiple retrieval request) the procedure continues, otherwise it ends.

It should be noted that, without departing from the scope of the finding, the connection between mobile phone and storage centre, besides by SMS messages, may be implemented by a data transmission connection or over the Internet, making use of WAP and GPRS protocols on current GSM telephones, and UMTS protocols on future new-generations telephones.
Claims

1. Procedure for storing alphanumerical information sent by a mobile phone to a storage centre connected to the network and for retrieving and storing the same to the phone memory or to a SIM card inserted therein, where said storage centre contains at least one electronic computer provided with a memory consisting of as many memory benches as the number of users enabled to use the data storage service, and where the mobile phone implements an encryption algorithm whose key consists of a password that can be
entered by the phone's user, characterised in that for the mobile phone's user, the storage procedure comprises the following steps:
a) selecting the information to be stored, either by direct typing or by retrieving it from the phonebook or from the calls received;
b) associating the selected information to a memory position of the phone or of the relevant SIM card;
c) typing the password to encrypt the information to be stored;
d) sending the resulting SMS message to the storage centre;
and for the storage centre, the following steps:
e) checking the correct source and type of message; if the source is correct, and it is an encrypted message, continuing the storage procedure; if the source is correct and the message is in plain text, performing the data retrieval and transmission to the calling phone;
if the source is not correct, rejecting the message;
f) reading the memory position associated to the information to be stored and storing the encrypted portion of the message to the corresponding memory position reserved to the calling user;
g) sending a storage confirmation message to the user;
and in that the data retrieval and storage procedure to the mobile phone or to the relevant SIM card comprises, for the mobile phone's user, the following steps:
h) generating a request message for retrieving one, multiple of all information previously stored, the message containing the memory position(s) associated to the information to be retrieved;
i) sending the generated message to the data storage centre, confirming the transmission and waiting for the reply message, or messages, in the event of multiple information retrieval;

l) upon the reception of each message, entering the password for decryption;

m) if the retrieved information is that requested, storing it to the phone or to the relevant SIM card;

and, as regards the storage centre, the following steps:

n) checking the correct source and type of message; if the source is correct, and it is an encrypted message, performing the storage procedure; if the source is correct and the message is in plain text, continuing the data retrieval and transmission procedure to the calling phone; if the source is not correct, rejecting the message;

o) reading the requested memory position(s); and

p) sending a message for each information to the same phone number that has sent the retrieval request.

2. Procedure according to claim 1, wherein the message sent by the user containing the information to be stored also contains a control character for the integrity of the entire message (CRC), and wherein at step e), the storage centre analyses said control character and proceeds to storing the information only if the message is integral.

3. Procedure according to claim 1 or 2, wherein at the end of the storage operation corresponding to steps a)-g), the memory
position of the phone or of the SIM card whose information has been stored is marked by an indicator.

4. Procedure according to any one of the previous claims, wherein at the end of the information retrieval operation corresponding to steps h)-p), the memory position of the phone or of the relevant SIM card containing the retrieved information is marked by an indicator.

5. Procedure according to any one of the previous claims, wherein at step f) of the storage operation, if the memory position where the information should be stored is already occupied by another information, the latter is overwritten.

6. Procedure according to any one of the previous claims, wherein at step m) of the information retrieval operation if the memory position where the information should be stored is already occupied by another information, the latter is overwritten after confirmation by the user.
START

Storing of a (new) number
(choice of a memory pos.)

Writing on SIM

Back-up request

END NO

Does the user want back-up?

YES

Password request

SMS encryption (Ax)

Sending SMS to back-up center

Sending OK?

YES

NO

Time-out?

WAITING FOR CONFIRMATION

Conf. OK?

YES

NO

User warning "Back-up OK"

Flag on mem. pos.

END

User warning "Back-up failed"
START

Storing of a (new) number (choice of a memory pos.)

Writing on SIM

Back-up request

END

Does the user want back-up?

YES

Password request

SMS encryption (Ax)

Sending SMS to back-up center

NO

Sending OK?

NO

Time-out?

YES

NO

Waiting for confirmation

Conf. OK?

NO

Time-out?

NO

YES

User warning "Back-up OK"

Flag on mem. pos.

END

User warning "Back-up failed"
Fig. 3

START

Restore request (mem. pos. choice)

SMS generation

Sending SMS to back-up center

Sending OK?

Time-out?

NO

User warning "Restore failed"

END

YES

Waiting for restore SMS

Time-out?

NO

SMS OK?

NO

Password request

SMS decryption

Data display

Confirmation request

Conf. OK?

NO

YES

Memory writing

Flag on mem. pos.

SMS deletion

END

User warning "Restore ended"
# INTERNATIONAL SEARCH REPORT

**A. CLASSIFICATION OF SUBJECT MATTER**

| IPC   | H04Q7/32 |

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 |

**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>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>WO 99 27730 A (BOUQUET HANSPETER ; RITTER RUDOLF (CH); SWISSCOM AG (CH); HEUTSCHI) 3 June 1999 (1999-06-03) page 2, line 1-24 page 4, line 11 - page 6, line 11 page 8, line 9 - line 32 page 10, line 7 - page 11, line 3 abstract</td>
</tr>
<tr>
<td>A</td>
<td>WO 01 62029 A (SARKOG JOHAN) 23 August 2001 (2001-08-23) the whole document</td>
</tr>
<tr>
<td>A</td>
<td>WO 00 45612 A (AHONEN PASI MATTI KALEVI ; ERICSSON TELEFON AB L M (SE)) 3 August 2000 (2000-08-03) abstract</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 art which is not considered to be of particular relevance
  - *E* earlier document 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

- *I* 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
- *Z* document member of the same patent family

**Date of the actual completion of the international search**

28 February 2003

**Date of mailing of the international search report**

06/03/2003

**Name and mailing address of the ISA**

European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk
Tel. (+31-70) 940-2040, Tx. 31 651 epo nl, Fax: (+31-70) 940-3016

**Authorized officer**

Coppeters, S
<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>
</table>
| P,X      | GB 2 373 139 A (MATCHTIP LTD)  
11 September 2002 (2002-09-11)  
page 28, line 6 - page 30, line 4  
page 33, line 1 - page 35, line 22  
abstract; claims 1-30; figures 9-12, 18-20 | 1-5                  |
<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>AT 230197 T</td>
<td>15-01-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 1139599 A</td>
<td>15-06-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5979798 A</td>
<td>15-06-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9927730 A1</td>
<td>03-06-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9927721 A1</td>
<td>03-06-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 59800948 D1</td>
<td>02-08-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 59806763 D1</td>
<td>30-01-2003</td>
</tr>
<tr>
<td>WO 0162029 A</td>
<td>23-08-2001</td>
<td>AU 3257901 A</td>
<td>27-08-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 0000478 A</td>
<td>16-08-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0162029 A1</td>
<td>23-08-2001</td>
</tr>
<tr>
<td>WO 0045612 A</td>
<td>03-08-2000</td>
<td>FI 990168 A</td>
<td>30-07-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 1986200 A</td>
<td>18-08-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1145579 A1</td>
<td>17-10-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0045612 A1</td>
<td>03-08-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2002536737 T</td>
<td>29-10-2002</td>
</tr>
<tr>
<td>GB 2373139 A</td>
<td>11-09-2002</td>
<td>WO 02071219 A2</td>
<td>12-09-2002</td>
</tr>
</tbody>
</table>