Title: CENTRALLY CONTROLLED BACKUP FUNCTIONALITY

Abstract: A method and mobile device are presented for centrally controlling backup functionality, so that parties such as backup devices will efficiently be informed how data content should be backed up from or restored to the mobile device. The mobile device exposes a party to rules for backing up or restoring data content, and those rules are not just for the party, but are also for other parties including the mobile device itself. The rules are contained in a list formatted in extensible markup language (XML). If the party is an external party, the mobile device provides an object exchange protocol (OBEX) capability object in response to the party fetching that object. The OBEX capability object describes capabilities of the mobile device, and is for use by the external party in order to access the list of rules via the mobile device exposing those rules to the external party.
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.
CENTRALLY CONTROLLED BACKUP FUNCTIONALITY

Field of the Invention

The invention relates to backing up data, and more particularly to backing up data from a mobile communication device.

Background of the Invention

The importance of users’ data in mobile telephone devices is becoming a great concern of the telecommunications industry, because wireless phones are increasingly being used not just for communication but also for managing personal data. Therefore, backing up this data is an important issue, in order to protect against data loss. Some of this data can be backed up in synchronization with a local personal computer (PC), or remotely backed up with a synchronisation server located in a network. In case the device is lost or broken, or in case of a hardware (HW) crash, one-way synchronization from the server (or PC) to the phone can be established in order to restore the data. However, data such as documents, or photos taken by a phone’s built-in camera, may not be part of a typical synchronization procedure, and they may require traditional backup to be done manually, instead of in a regular and synchronized way. Different types of data need to be backed up at different intervals, and also may require different storage capacities, and therefore a need exists for an efficient system of backing up different types of data to different locations.

Recently, PC “suites” have been developed, in order to provide a package of applications that allow a user to synchronize, edit, and back up many of a phone’s files on a compatible PC through a wireless or cable connection. See, for example, Nokia PC Suite: Description, at http://www.nokia.com/nokia/0,,54691,00.html. Since PC suite development has moved application development from a “separate release for each phone” towards a “unified” operation mode, it is now increasingly important to minimize phone-dependent differences. This need for unified functionality includes backup and restore functionality, because there are many
variations of locations, amounts, and types of data to be backed up. There also are a number of variations of phone devices having different sets of applications and features (e.g. camera included or not included, differing multimedia capabilities, etcetera), and therefore data content needs to be copied to and from different locations and by following different rules.

Additionally, it is also important to consider a device’s ability to be backed up by a removable medium such as a multi media card (MMC). The same backup rules are needed in this MMC case in order to ensure a good user experience. It is not acceptable or efficient for backup instructions to have a different meaning if the device’s removable backup/restore application is used instead of a corresponding application on the PC side performing the same backup function.

Traditional device side backups, and also backups taken from the PC side, have not had any coordination with each other, and no coordinated rules about which content to respectively manage, and how to manage content jointly. Instead, each side has had its own “exclude” lists used for blocking out unnecessary content from backup, and this has unfortunately led to the present difficult situation where backups are not necessarily consistent with each other.

It is known in the art to use an Object Exchange Protocol in order to provide a server with synchronization and backup services. See Infrared Data Association (IrDA) Object Exchange Protocol, OBEX, Version 1.3 dated January 3, 2003, Section 8.3. However, no way has heretofore been found to use OBEX so as to allow consistent backups to a plurality of backup repositories which respectively back up different categories of data.

Summary of the Invention

The present invention enables a device to expose rules regarding how the device should be backed up and restored, and these exposed rules are for use by all parties including the device itself. These rules are valid not only for the device’s own (e.g. MMC) backup application, but additionally for the PC side backup used via local communication media such as a universal serial bus (USB), Bluetooth.
(BT), wireless local area network (WLAN), or infrared link (in accordance with the Infrared Data Association IrDA). These rules can additionally be valid for a backup application employing a synchronisation server located in a network.

The device of the present invention contains a structured list in extensible markup language (XML), including strict rules about how a particular main category of data content should be handled. An external party such as a PC can obtain access to the structured list by fetching a first object that describes capabilities of the device.

This first object is part of the Object Exchange Protocol (OBEX) standard developed by the IrDA, and this first object is called an “OBEX capability object.” Various extensions to the OBEX capability object can be defined, including an extension that links to a location of a backup description XML object (backup.xml). This backup description XML object then provides the structured list explaining how data should be backed up from the device. It should be noted that the structure of the backup description XML object is given by a Document Type Definition (DTD). The purpose of a Document Type Definition is to define the allowed building blocks of an XML document; it defines the document structure with a list of allowed elements. Inside of this DTD there are possibilities for making additions for additional content or types of content. The structured list is thus accessible via normal file transfer.

The method and mobile device of the present invention thus make it feasible to centrally control backup functionality, so that backup devices will efficiently be informed how data content should be backed up from (and restored to) the mobile device. The device is equipped to provide an object exchange protocol (OBEX) capability object from the mobile device to the backup device. The device then exposes to the backup device a backup description extensible markup language (XML) object in response to a link from an extension of the OBEX capability object.
The present invention is for centrally controlling backup functionality, so that parties such as backup devices will efficiently learn how data content should be backed up from the mobile device, or restored to the mobile device. The mobile device exposes (i.e. shows) to a party various rules for backing up or restoring data content, and those rules are not only for the party, but also are for other parties including the mobile device itself, including all backup devices that interact with the mobile device. The rules are contained in a list formatted in extensible markup language (XML). If the party is an external party, the mobile device provides an object exchange protocol (OBEX) capability object in response to the party fetching that object. The OBEX capability object describes capabilities of the mobile device, and is also for use by the external party in order to access the list of rules via the mobile device exposing those rules to the external party, as discussed previously.

Brief Description of the Drawings

FIG. 1 shows subsystems and components needed for centralized backup handling.

FIG. 2 shows a method according to an embodiment of the present invention.

FIG. 3 shows a block diagram of an embodiment of the present invention.

Detailed Description of the Invention

A backup description XML object (backup.xml) containing a list of rules is available by linking from an OBEX capability object that is fetched from a mobile device by a PC, MMC, or network server. The syntax for the capability object is based on XML, and XML has been chosen because of its flexibility and ease with which elements can be categorized and their attributes collected. The capability object is flexible enough that individual manufacturers can selectively include objects, services and attributes that are of interest to them. It also permits the addition of user-defined elements for specific application or manufacturer needs.
The backup description XML object contains categories to be backed up, such as user documents, calendar, contacts, bookmarks, and the like. Categories can be added to the backup description by defining a new version of DTD that describes backup.xml. These categories contain rules to be followed in the respective backup case. These rules are, for example, tags such as "include" or "exclude" or "inclusiveatomic."

Each of these tags indicates folders and/or files belonging to the respective rule. Tags are of "file" type or "folder" type, meaning that the tag takes into account a single file or an entire folder structure, so that a single file or an entire folder is "included" in or "excluded" from the backup. The tag "inclusiveatomic" has a specific purpose: it is used in cases where a folder contains linked files requiring that some of the folder must be handled as whole. In case of restore (as opposed to backup), this "inclusiveatomic" tag means that the whole folder must be emptied before content can be replaced by the old version of the files (e.g. some of the emptied files will not be replaced).

Following is an example of information provided by the backup description XML object that is used for controlling backups.

```xml
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE BACKUP>
<!ELEMENT BACKUP (CALENDAR?, CONTACTS?, MESSAGES?, BOOKMARKS?, USER_DATA?, SETTINGS?, FULL?)>
<!ATTLIST BACKUP Version CDATA "1.0">
<!ELEMENT CALENDAR (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT CONTACTS (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT MESSAGES (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT BOOKMARKS (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT USER_DATA (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT SETTINGS (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT FULL (INCLUDE | INCLUDEATOMIC | EXCLUDE)+>
<!ELEMENT INCLUDE (FOLDER | FILE)+>
<!ELEMENT INCLUDEATOMIC (FOLDER | FILE)+>
<!ELEMENT EXCLUDE (FOLDER | FILE)+>
<!ELEMENT FOLDER (#PCDATA)>
```
<!ELEMENT FILE (#PCDATA)>
  ]>

<BACKUP Version="1.0">
  <CALENDAR>
    <INCLUDE>
      <FILE>C:\System\Data\Calendar</FILE>
    </INCLUDE>
  </CALENDAR>
  <CONTACTS>
    <INCLUDE>
      <FILE>C:\System\Data\Contacts.cdb</FILE>
    </INCLUDE>
  </CONTACTS>
  <MESSAGES>
    <INCLUDEATOMIC>
      <FOLDER>C:\System\Mail\</FOLDER>
    </INCLUDEATOMIC>
  </MESSAGES>
  <BOOKMARKS>
    <INCLUDE>
      <FILE>C:\System\Data\Bookmarks1.db</FILE>
    </INCLUDE>
  </BOOKMARKS>
  <USER_DATA>
    <INCLUDE>
      <FOLDER>C:\Nokia\</FOLDER>
      <FOLDER>E:\</FOLDER>
    </INCLUDE>
    <EXCLUDE>
      <FOLDER>E:\System\</FOLDER>
    </EXCLUDE>
  </USER_DATA>
  <SETTINGS>
    <INCLUDE>
      <FOLDER>C:\System\Data\Profiles\</FOLDER>
      <FILE>C:\System\Data\Cdbv3.dat</FILE>
    </INCLUDE>
  </SETTINGS>
  <FULL>

6
<INCLUDE>
  <FOLDER>C:\</FOLDER>
  <FOLDER>E:\</FOLDER>
</INCLUDE>

<EXCLUDE>
  <FOLDER>D:\</FOLDER>
  <FOLDER>C:\System\temp\</FOLDER>
  <FOLDER>E:\System\temp\</FOLDER>
  <FOLDER>C:\System\midp\</FOLDER>
  <FOLDER>E:\System\midp\</FOLDER>
  <FOLDER>C:\System\sounds\digital\</FOLDER>
  <FOLDER>E:\System\sounds\digital\</FOLDER>
  <FOLDER>C:\System\sounds\simple\</FOLDER>
  <FOLDER>E:\System\sounds\simple\</FOLDER>
  <FOLDER>C:\System\apps\phone\oplogo\</FOLDER>
  <FOLDER>E:\System\apps\phone\oplogo\</FOLDER>
  <FILE>C:\System\shareddata\reserve.bin</FILE>
  <FOLDER>C:\System\data\voucherdb\</FOLDER>
  <FOLDER>E:\System\data\voucherdb\</FOLDER>
  <FOLDER>C:\System\data\backupvdb\</FOLDER>
  <FOLDER>E:\System\data\backupvdb\</FOLDER>
  <FOLDER>E:\Images_temp</FOLDER>
</EXCLUDE>
</FULL>
</BACKUP>

This approach to backing up mobile device data has the big advantage of having consistent functionality. This XML object can either be preprogrammed, or it can modified by a user. In either case, the user experience will be enhanced by ensuring reliable backups of user data, with the user data being backed up to a plurality of external backup areas in a coordinated fashion.

Implementation of this embodiment of the invention can be better appreciated by referring to FIG 1, which shows subsystems and components of a centralized
backup 100. A user 109 has access to an external device 105 such as a personal computer (PC), and also has access to a phone device 107.

The external device 105 includes a subsystem application 110 which contains applications running in the external device 105. A backup application receives static information regarding a connected phone 107 that is unavailable in the backup.xml list of rules 180 or in the OBEX capability object. The subsystem platform 120 implements connectivity and protocol-specific parts. A subsystem data handling layer 130 is an abstraction layer of the application data; it communicates to the phone 107 via the subsystem platform 120 using protocols that the platform 120 implements. A file system 140 provides mass memory that is used for file storage.

The external backup application 150 contains logic for decoding backup rules that are exposed by the phone device 107. This external backup application 150 has a human interface enabling the user 109 to control backup/restore functionality, and the external backup application 150 uses the file storage provided by the file system 140.

Turning now to the phone device 107, this entity includes a connectivity subsystem 160 that is substantially similar to the subsystem platform 120 on the external side. Likewise, a device file system 170 in the phone device is substantially similar to the file system 140 on the external (e.g. PC) side. The backup.xml 180 is an object containing rules in XML form. The MMC 190 is a multi media card that provides removable mass memory, and extends the device file system 140. Finally, the device backup application 195 corresponds to the external backup application 150 on the external side, and it stores backup on the MMC 190.

FIG. 2 is a flow chart showing a method 200 according to the present invention. First, it is determined 210 if the backup device is external to the mobile terminal (i.e. outside the mobile device). If not, then the mobile device directly exposes 250 the list of backup rules to the backup device within the mobile terminal. This single list is also to be exposed to external backup devices. Of course, although this is a single list, the different backup devices can utilize different parts of the list, given the different requirements and capabilities of each backup device.
If the question 210 is answered positively, then the backup device will go fetch 220 the OBEX capability object from the mobile device. Then, the mobile device will provide 230 the OBEX capability object. The backup device will then, in this embodiment, activate 240 a link in an extension of the OBEX capability object, and this will cause the mobile device to expose 250 the list of backup and/or restore rules to the backup device.

FIG. 3 shows system 300 corresponding to part of the method just described. The external backup device 310 will send a fetch signal 330 to the mobile device 320, and in particular this signal will be received by a means 340 for providing an OBEX capability object. This means 340 will respond by providing on a line 350 the OBEX capability object 360. The external backup device 310 will then activate a link located in an extension 370 of the OBEX capability object 360, and the extension 370 will consequently send an expose request signal 380 to the mobile device 320, and in particular to a means 390 for exposing to any backup device a list of backup rules. In response, the means 390 will then send an expose signal 395 to the external backup device in order to provide the uniform centralized backup rules to the backup device 310.

It is to be understood that the present figures, and the accompanying narrative discussions of best mode embodiments, are illustrative of the present invention, and are not purport to be completely rigorous treatments of the invention under consideration. A person skilled in the art will understand that the steps and signals of the present application represent general cause-and-effect relationships that do not exclude intermediate interactions of various types, and will further understand that the various steps and structures described in this application can be implemented by a variety of different combinations of hardware and software, in various configurations and sequences, consistent with the spirit and scope of the present invention, and need not be further detailed herein.
WHAT IS CLAIMED IS:

1. A method for a mobile device to describe to a party how data content should be backed up from the mobile device or restored to the mobile device, comprising:
   exposing to the party rules for backing up or restoring the data content, wherein the rules are for the party and for other parties including the mobile device itself, and wherein the rules are contained in a list formatted in extensible markup language (XML); and
   providing an object exchange protocol (OBEX) capability object from the mobile device to the party if the party is an external party that has fetched the OBEX capability object, wherein the OBEX capability object describes capabilities of the mobile device, and wherein the OBEX capability object is for use by the external party in order to access the list via the exposing step.

2. The method of claim 1, wherein the exposing step is in response to a link from an extension of the OBEX capability object.

3. The method of claim 1, wherein the party is a backup device, and the other party is another backup device.

4. The method of claim 1, wherein the list exposed to the party is substantially identical for a removable backup device that is removable from the mobile device.

5. The method of claim 1, wherein the OBEX capability object provided by the mobile device is substantially identical for at least one other party.

6. The method of claim 1, wherein the party is a medium removable from the mobile device, or is a personal computer, or is a synchronization server in a network.
7. The method of claim 5, wherein the OBEX capability object provided by the mobile device is substantially identical for every other party.

8. The method of claim 6, wherein the medium is a multi media card (MMC).

9. The method of claim 6, wherein if the party is the personal computer, then the backup occurs via a local communication medium.

10. The method of claim 1, wherein the list has a document type definition (DTD) structure that includes a plurality of categories of the data content, and that also accommodates additions for additional categories of the data content.

11. The method of claim 10, wherein the list provides backup rules to be followed in each of the categories respectively.

12. The method of claim 9, wherein the local communication medium is a universal serial bus, bluetooth, wireless local area network, or infrared link.

13. A computer readable medium encoded with a software data structure for performing the method of claim 1.

14. A mobile device for describing to a party how data content should be backed up from the mobile device or restored to the mobile device, comprising:

   means for exposing to the party rules for backing up or restoring the data content, wherein the rules are for the party and for other parties including the mobile device itself, and wherein the rules are contained in a list formatted in extensible markup language (XML); and

   means for providing an object exchange protocol (OBEX) capability object from the mobile device to the party if the party is an external party that has fetched the OBEX capability object, wherein the OBEX capability object describes capabilities of the mobile device, and wherein the OBEX capability object is for use
by the external party in order to access the list from the exposing means.

15. The mobile device of claim 14, wherein the exposing means is responsive to a link from an extension of the OBEX capability object.

16. The mobile device of claim 14, wherein the party is a backup device, and the other party is another backup device.

17. The mobile device of claim 14, wherein the list exposed to the party is substantially identical for a removable backup device that is removable from the mobile device.

18. The mobile device of claim 14, wherein the OBEX capability object provided by the mobile device is substantially identical for at least one other party.

19. The mobile device of claim 14, wherein the party is a medium removable from the mobile device, or is a personal computer, or is a synchronization server in a network.

20. The mobile device of claim 18, wherein the OBEX capability object provided by the mobile device is substantially identical for every other party.

21. The mobile device of claim 19, wherein the medium is a multi media card (MMC).

22. The mobile device of claim 19, wherein if the party is the personal computer, then the backup occurs via a local communication medium.

23. The mobile device of claim 14, wherein the list has a document type definition (DTD) structure that includes a plurality of categories of the data content,
and that also accommodates additions for additional categories of the data content.

24. The mobile device of claim 23, wherein the list provides backup rules to be followed in each of the categories respectively.

25. The mobile device of claim 22, wherein the local communication medium is a universal serial bus, bluetooth, wireless local area network, or infrared link.

26. A system for describing how data content should be backed up from a mobile device or restored to the mobile device, comprising:

   the mobile device; and

   an external device, for providing a fetch signal, and also for providing an expose request signal responsive to receipt of an OBEX capability object;

   wherein the mobile device includes

   means for providing to the external device an object exchange protocol (OBEX) capability object, responsive to the fetch signal; and

   means for exposing to the external device rules for backing up or restoring the data content, responsive to the expose request signal;

   wherein the OBEX capability object describes capabilities of the mobile device.
FIG 2

START

Is the backup device external to the mobile terminal?

YES

Backup Device Goes to Fetch OBEX Capability Object

NO

Mobile Device Provides OBEX Capability Object to Backup Device

Backup Device Activates a Link in an Extension of the OBEX Capability Object

Mobile Device Exposes to the Backup Device a Single List of Rules for Backing Up Data Content, the List Being an XML Object
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/32, H04L 29/08
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)

IPC7: H04L, H04M, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

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>A</td>
<td>EP 1271885 A2 (NOKIA CORPORATION), 2 January 2003 (02.01.2003), paragraph [0046]-[0049], abstract</td>
<td>1-26</td>
</tr>
<tr>
<td>A</td>
<td>US 6493758 B1 (JAY F. MCLAIN), 10 December 2002 (10.12.2002), column 2, line 64 - column 4, line 11</td>
<td>1,6,9,12,14, 19,22,25</td>
</tr>
<tr>
<td>A</td>
<td>WO 03037015 A1 (IAN, CAREL, VAN REENEN), 1 May 2003 (01.05.2003), see whole</td>
<td>1,6,8,9, 12-14,19,21, 22,25</td>
</tr>
<tr>
<td>A</td>
<td>GB 2350973 A (NOKIA MOBILE PHONES LIMITED), 13 December 2000 (13.12.2000), see whole</td>
<td>1-26</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents
  *A* document defining the general state of the art which is not considered to be of particular relevance
  *E* earlier application or patent but published on or after the international filing date
  *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  *O* document referring to an oral disclosure, use, exhibition or other means
  *P* document published prior to the international filing date but later than the priority date claimed

**T** later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

**X** document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

**Y** document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

**&** document member of the same patent family

Date of the actual completion of the international search: 26 October 2005

Date of mailing of the international search report: 28-10-2005

Name and mailing address of the ISA/Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86

Authorized officer
Bo Gustavsson /itw
Telephone No. +46 8 782 25 00
<table>
<thead>
<tr>
<th>Country</th>
<th>Application No.</th>
<th>Date</th>
<th>Filing Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP</td>
<td>1271885 A2</td>
<td>02/01/2003</td>
<td>AT 302520 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CN 1407775 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DE 60205542 D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 2003101561 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>US 2003002504 A</td>
</tr>
<tr>
<td>US</td>
<td>6493758 B1</td>
<td>10/12/2002</td>
<td>NONE</td>
</tr>
<tr>
<td>WO</td>
<td>03037015 A1</td>
<td>01/05/2003</td>
<td>EP 1498002 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GB 0125451 D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>US 20050107122 A</td>
</tr>
<tr>
<td>GB</td>
<td>2350973 A</td>
<td>13/12/2000</td>
<td>AU 5240500 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BR 0011409 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CN 1369164 A,T</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EP 1192778 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GB 9913678 D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 2003502914 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX PA01012634 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WO 0078010 A</td>
</tr>
</tbody>
</table>