# (12) UK Patent Application (19) GB (11) 2 431 250 (13) A

(43) Date of A Publication **18.04.2007**

(21) Application No: **0520602.4**

(22) Date of Filing: **11.10.2005**

(71) Applicant(s):
**Hewlett-Packard Development Company**
**L.P., 20555 S.H.249, Houston, Texas 77070,**
**United States of America**

(72) Inventor(s):
**Andrew Topham**
**Duncan Wakelin**
**John William Drew**

(74) Agent and/or Address for Service:
**Hewlett-Packard Limited**
**IP Section, Filton Road, Stoke Gifford,**
**BRISTOL, BS34 8QZ, United Kingdom**

(51) INT CL:
***G06F 12/14*** (2006.01) ***G06F 1/00*** (2006.01)
***G06F 3/06*** (2006.01) ***G06F 21/02*** (2006.01)
***G11B 20/00*** (2006.01)

(52) UK CL (Edition X ):
**G4A** AAP A23A
**G5R** RHB

(56) Documents Cited:
**US 6473861 B1** **US 6134660 A**
**US 5651064 A** **US 20050071591 A1**
**US 20040101140 A1** **US 20030074319 A1**

(58) Field of Search:
UK CL (Edition X ) **G4A, G5R, H4P**
INT CL **G06F, G11B, H04L**
Other: **WPI, EPODOC, INSPEC**

## (54) Abstract Title: **Data transfer system**

(57) A method of distributing a key to encrypt data for storing on a removable data storage item in a data transfer device library, the library comprising a controller 10 having a key associated therewith and being connected to a plurality of data transfer devices 2 each being operable to transfer data to a removable data storage item (not shown) and having a key store 29, the method comprising: providing the key for the library to the controller; the controller providing the key to the key store of each data transfer device connected to the controller. A data transfer device library is also disclosed.
The main embodiment relates to the library being a tape drive library, the data transfer devices being tape drives and the data storage items being tape cartridges.

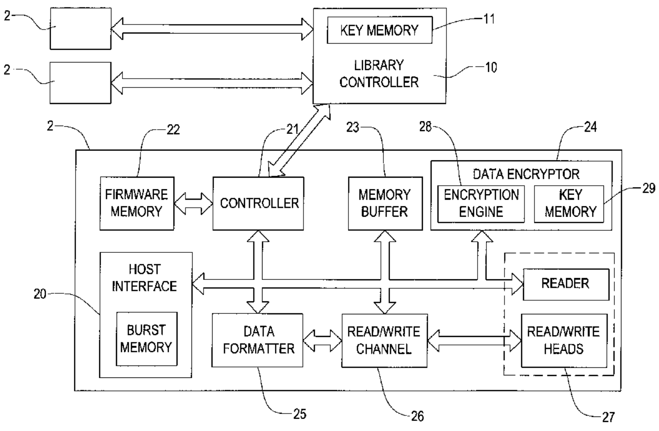


FIG. 2

GB 2 431 250 A

Original Printed on Recycled Paper

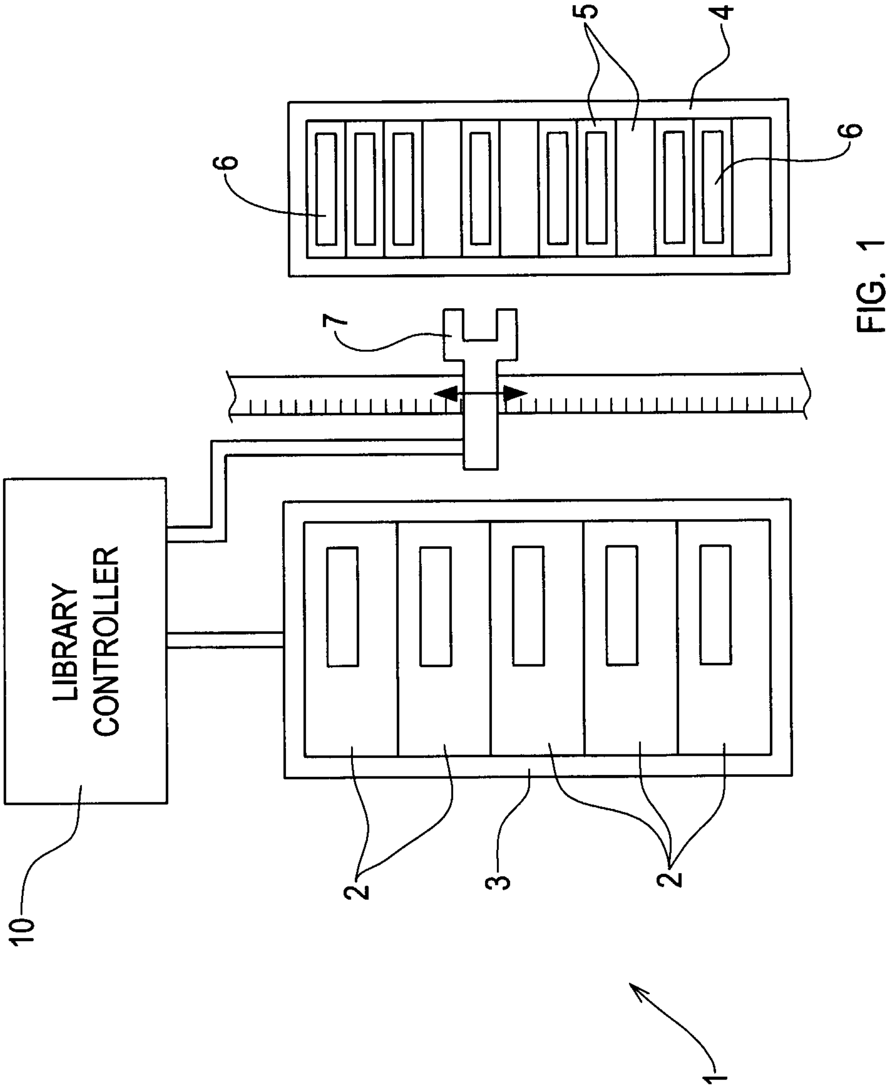


FIG. 1

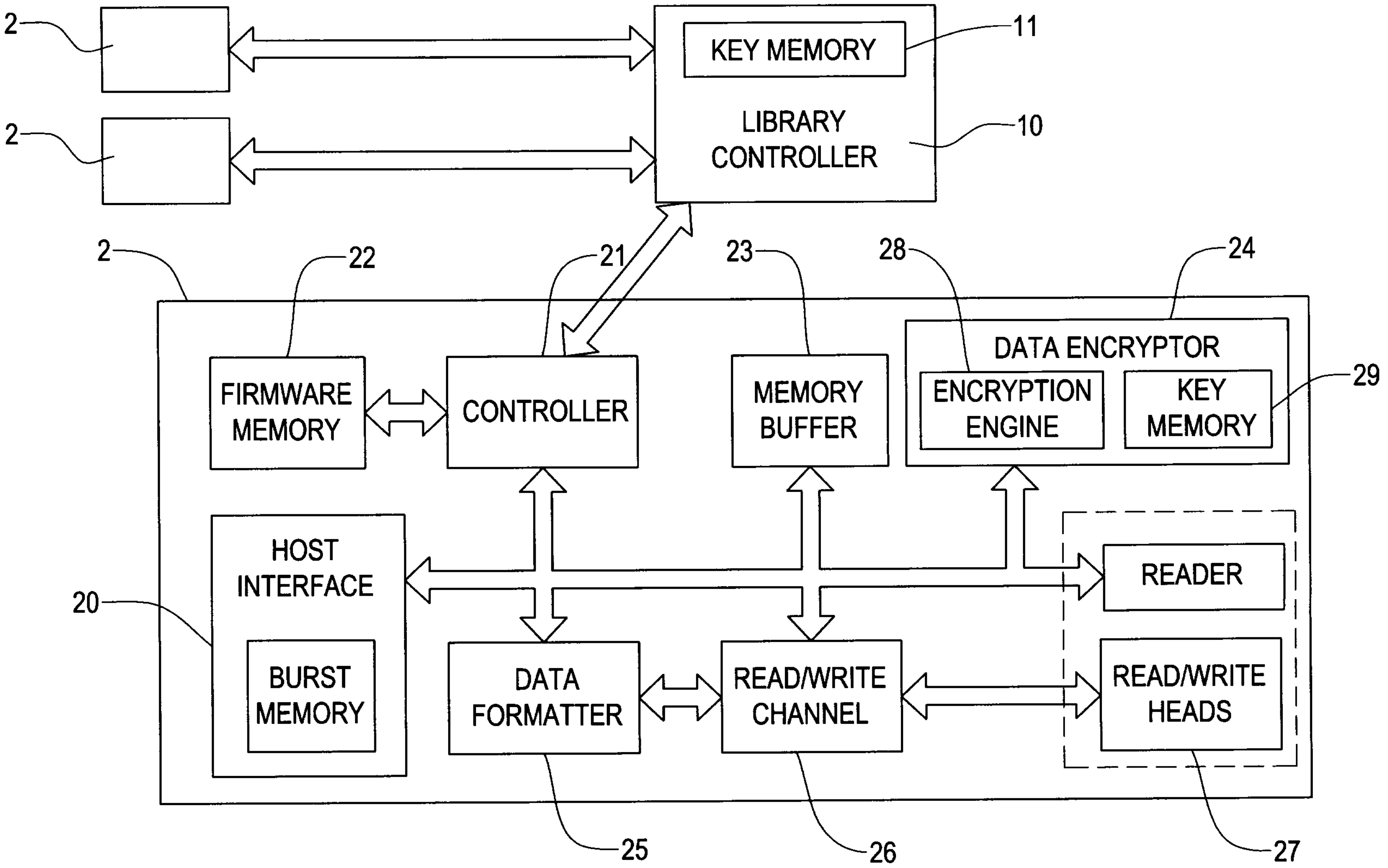
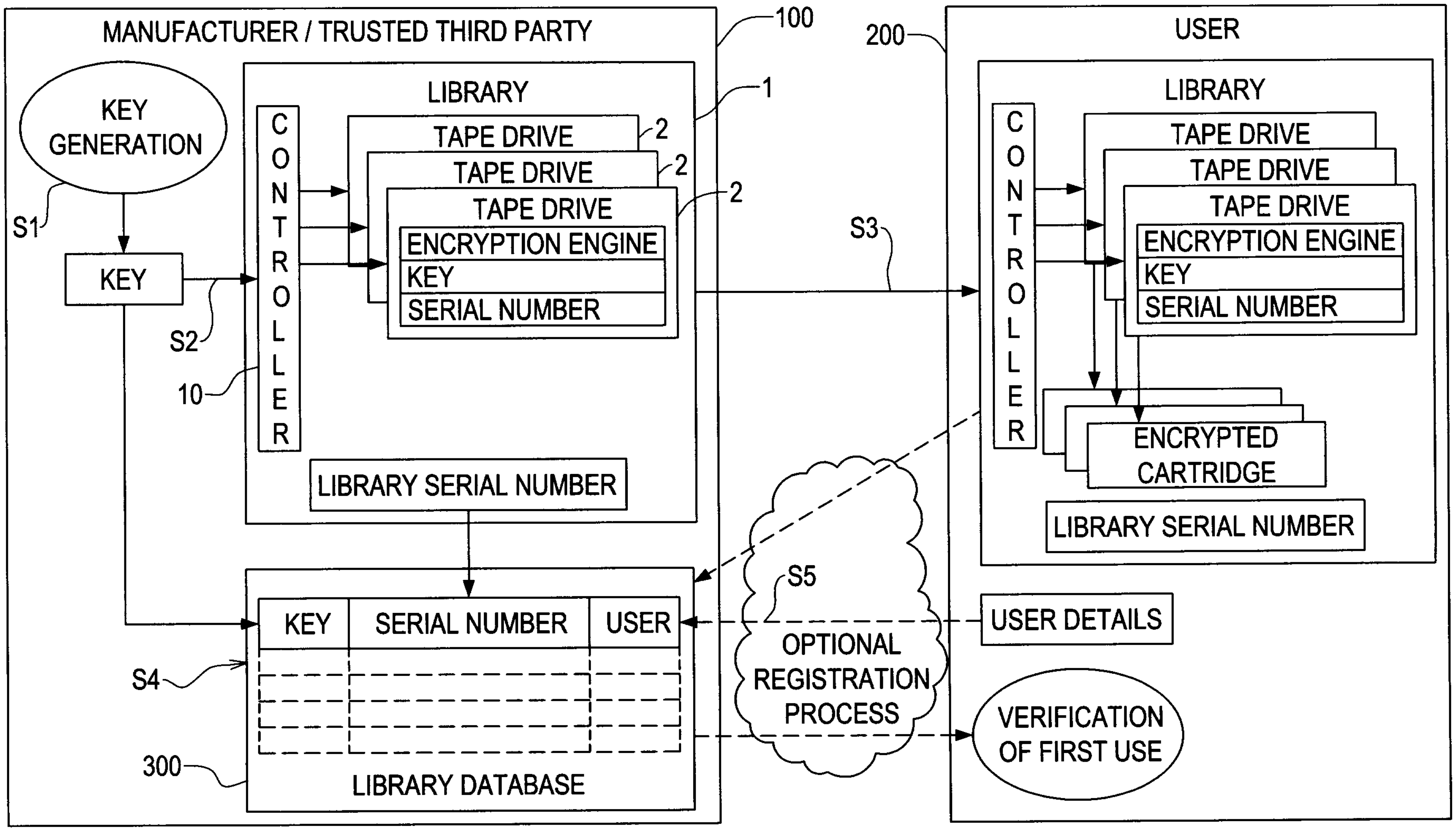

2
2
KEY MEMORY
11
LIBRARY CONTROLLER
10
2
22
21
23
28
24
DATA ENCRYPTOR
29
FIRMWARE MEMORY
CONTROLLER
MEMORY BUFFER
ENCRYPTION ENGINE
KEY MEMORY
HOST INTERFACE
READER
20
BURST MEMORY
DATA FORMATTER
READ/WRITE CHANNEL
READ/WRITE HEADS
25
26
27

FIG. 2



MANUFACTURER / TRUSTED THIRD PARTY
100
KEY GENERATION
S1
KEY
S2
LIBRARY
1
CONTROLLER
10
TAPE DRIVE
2
TAPE DRIVE
2
TAPE DRIVE
2
ENCRYPTION ENGINE
KEY
SERIAL NUMBER
LIBRARY SERIAL NUMBER
KEY
SERIAL NUMBER
USER
S4
300
LIBRARY DATABASE
S3
200
USER
LIBRARY
CONTROLLER
TAPE DRIVE
TAPE DRIVE
TAPE DRIVE
ENCRYPTION ENGINE
KEY
SERIAL NUMBER
ENCRYPTED CARTRIDGE
LIBRARY SERIAL NUMBER
S5
OPTIONAL REGISTRATION PROCESS
USER DETAILS
VERIFICATION OF FIRST USE

FIG. 3

# DATA TRANSFER DEVICE LIBRARY AND KEY DISTRIBUTION

## FIELD OF THE INVENTION

This invention relates to a data transfer device library and a method of key distribution.

## BACKGROUND OF THE INVENTION

Many institutions and corporations back up their data and use removable data storage items such as tape cartridges for storage. Data are usually backed up in a secure location such as an off-site library from where data can be restored in the event of disaster recovery. There have been instances of company data potentially losing its confidentiality due to the loss of backup tape cartridges. In the event that the data on a lost tape cartridge has not been encrypted, that data would be relatively easy for a non-authorised user to read. That situation is undesirable.

Where the backed up data are extremely sensitive, a need is perceived to encrypt the data and thereby improve security. Encryption technology exists that can make the data on tape cartridges unreadable to any person without a correct decryption key. There may be a separate encryption/decryption key. It is difficult to manage the availability of encryption, decryption and encryption/decryption keys, especially keys in an environment with multiple tape drives such as a tape library.

Current encryption solutions concentrate on encrypting the data either at source or on the wire.

The encryption at source solutions use software encryption running on the computer to which the backup devices are attached. This has the advantage of avoiding sending un-encrypted data over a network. However, such software-based encryption is typically slow and can impact backup performance. Also, the software must have some form of associated key management so one does not escape the problem of key management.

Encryption on the wire involves breaking the direct connection between the writing computer and the backup device and inserting an encrypting appliance into the break. This is generally a very expensive solution since such encrypting appliances are expensive. There is also again the key management issue.

SUMMARY OF THE INVENTION

The invention seeks to provide encryption in a multiple data transfer device environment without the user needing to become involved in the complexities of key management.

In accordance with the invention there is provided a method as claimed in claim 1.

In accordance with a further aspect of the invention, there is provided a data transfer device library as claimed in claim 6.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the present invention may be more readily understood, embodiments thereof will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of a data transfer device library embodying the present invention;

Figure 2 is a schematic block diagram of a controller and tape drives of the library of Figure 1; and

Figure 3 is a diagram illustrating a method embodying the present invention.

DETAILED DESCRIPTION

Referring to Figure 1, a library 1 comprises a plurality of data transfer devices 2 which are stacked in a rack 3 or otherwise physically arranged with respect to an array 4 of storage bays 5 which contain removable data storage items 6. There is in this example a controlled robot picker 7 operable to select a data storage item, insert that item in a data transfer device to read from or written to and to replace the item in a bay. A library controller 10 is operable to coordinate operations within the library and may also be the mechanism which controls the picker, although the operations performed by the picker may also be performed manually. The library controller 10 has a key memory 11 to store an encryption/decryption key together with the serial number of the library 1 (or some other unique identifier of the library). The library key memory 11 is non-volatile.

Referring now to Figure 2, each tape drive 2 in the library 1 comprises a host interface 20, a controller 21, firmware memory 22, a memory buffer 23, a data encryptor 24, a data formatter 25, a read/write channel 26, and magnetic read/write heads 27.

With the exception of the data encryptor 24 and the software stored in the firmware memory 22, the components of the tape drive 2 are identical to those employed in conventional tape drives.

The controller 21 of the tape drive 2 comprises a microprocessor and executes instructions stored in the firmware memory 22 to control the operation of the tape drive 2. In particular, the controller 21 responds to control commands received from the library controller 10.

As previously mentioned, the drive 2 contains a data encryptor 24 comprising an encryption engine 28 and a drive key memory 29 which are incorporated into the chipset of the tape drive. The encryption engine 28 is operable to encrypt data incoming to the tape drive with the key stored in the drive key memory 29 before writing the then encrypted data to the tape cartridge via the read/write channel 26 and the read/write heads 27. Conversely, the encryption engine 28 is operable to decrypt data read from the tape cartridge with the key stored in the drive key memory 29 before passing decrypted data to a host computer by the host interface 20. The encryption engine 28 in each tape drive 2 relies on being supplied with the encryption key. This key is supplied by the library controller 10.

The library controller 10 is the controller that is also used to control the movement of the tape cartridges 6 by the robotic picker 7. There could, however, be an incorporated or distinct other controller in the library that is either dedicated to the task of supplying keys or provides other functionality such as management of the library. Any existing communication path between the tape drive and the library controller 10 may be used to pass the key to the tape drive 2. The communication path should not, however, involve the host interface 20 of the tape drive 2 so as to provide no opportunity for snooping the key via that route.

The method of key distribution is as follows and as illustrated in Figure 3. Initially, the manufacturer 100 or a trusted third party (hereinafter manufacturer) generates S1 a unique encryption key suitable for use in an encryption engine of a tape drive to encrypt data for transfer to a tape. The generated key is pre-programmed S2 into the library key memory 11 which lies in the library controller. Each of these keys is unique to that particular library 1 and is stored in the library controller key memory 11 along with the library serial number or other unique library identifier for that library 1.

Each library 1, comprising at least of a library controller 10 and plurality of tape drives 2, is shipped S3 by the manufacturer 100 with the key pre-programmed into the library key memory 11 to a user 200, usually a corporate entity.

The library manufacturer 100 or trusted third party maintains S4 a library database 300 that matches the serial number of each library 1 to the pre-programmed key associated with that library 1. In the optional event that the user 200 registers their library 1 with the library database, user information will also be appended S5 to the record for that library. User information may be maintained in the record by the manufacturer 100 who is usually aware of the identity of the end user. This provides a recovery solution in the case of a disaster with the library 1. In that case, the manufacturer 100 is able to supply S3 a replacement library 1 to the user 200 pre-programmed with the same key for recovering the user's data. This replacement key will thus be the same as the key used to encrypt the data on the user's tape cartridges.

Registration of the library 1 by the user 200 is optional but there are benefits in that the manufacturer 100 can maintain the library database 300 and cross-check the record for that library with information derived from the user 200 – that being library serial number and user information – and flag any discrepancies. Upon registration of a library with the library database 300, the manufacturer 100 may also provide acknowledgement and verification of first use of the library 1 so as to confirm that the single key is being used to encrypt data for that library's tape cartridges.

The step of programming S2 the key into the library 1 and maintaining the library database 300 could be moved to a trusted third party if it was desired to prevent the original manufacturer having access to the keys.

As a part of the normal initialisation sequence of each library (which may take place when the library 1 is in the care of the manufacturer 100 or the user 200), the library controller 10 embodying the invention also writes the key stored in the library key memory 11 into the drive key memory 29 of each of the tape drives 2 in the library 1. This ensures that all cartridges that are written in that library are encrypted with the same key and so may be read by any tape drive in that library. Since the drive key memory 29 can be repopulated with the key from the non-volatile library key memory 11, it is not essential for the drive key memory 29 to be non-volatile.

Because such a large volume of data (all the tape cartridges in a library) are encrypted using the same encryption key, it is prudent to use a block encryption technique in which each block of data is encrypted using the same encryption key but different counter values, for example, using Gallois Counter Mode encryption. By ensuring that all tape cartridges still maintain unique key and counter combinations, the confidentiality of the data is not compromised even though so many cartridges are written using the same key.

Further, by providing software access to the key memory 11 in the tape library, the key can be updated as needed. The updated key would be distributed by the library 1 to all the tape drives 2 in the library 1. Clearly the library database 300 maintaining records of the library serial number and encryption key would also need to be updated if the key is changed.

The main advantage of this arrangement is that lack of any key management tasks for the user. A user may use a library using this invention in the same way as they use a similar library with no encryption. As long as any restoring of data is done with this library, then there is no change to existing processes. Thus, this appeals to users who recognise the need for encryption but are not prepared to put any effort into managing the process.

A further advantage of the present invention is that in the event that encrypted data need to be recovered from the tape cartridges of a single library, then only the one key for that entire library needs to be sent securely to the library to recover the data.

The very simple key management also lessens the likelihood of creating problems matching the appropriate key to each cartridge.

Although embodiments of the present invention have been described with reference to a tape drive 3, it will be appreciated that the present invention is equally applicable to other types of data transfer devices, such as optical drives, in which data are stored to removable data storage items (e.g. CDs, DVDs).

When used in this specification and claims, the terms "comprises" and "comprising" and variations thereof mean that the specified features, steps or integers are included. The terms are not to be interpreted to exclude the presence of other features, steps or components.

The features disclosed in the foregoing description, or the following claims, or the accompanying drawings, expressed in their specific forms or in terms of a means for performing the disclosed function, or a method or process for attaining the disclosed result, as appropriate, may, separately, or in any combination of such features, be utilised for realising the invention in diverse forms thereof.

CLAIMS:

1. A method of distributing a key to encrypt data for storing on a removable data storage item in a data transfer device library, the library comprising a controller having a key associated therewith and being connected to a plurality of data transfer devices each being operable to transfer data to a removable data storage item and having a key store, the method comprising:
providing the key for the library to the controller;
the controller providing the key to the key store of each data transfer device connected to the controller.

2. A method according to Claim 1, wherein the controller, upon initialisation of the library, provides the key to the key store of each data transfer device connected to the controller.

3. A method according to Claim 1 or 2, wherein all the data written to the removable data storage items by the data transfer devices in the library are encrypted with the key in the key store of each data transfer device, the keys being the same.

4. A method according to any preceding claim, wherein data are encrypted using a block encryption technique in which each block of data is encrypted using the key and a respective counter value.

5. A method according to any preceding claim further comprising maintaining a library database containing records of respective libraries and the key associated with a respective library.

6. A data transfer device library comprising a plurality of data transfer devices connected to a controller having a key associated therewith, each data

transfer device being operable to transfer data to a removable data storage item and having a key store to receive the key associated with the controller and to encrypt data with the key.

7. A library according to Claim 6, wherein the controller is a library controller and has a library key store pre-programmed with the key.

8. A library according to Claim 6, wherein the controller is distinct from a library controller and has a library key store pre-programmed with the key.

9. A library according to any one of Claims 6 to 8, wherein the controller has a non-volatile memory in which the key is writable.

10. A library according to any one of Claims 6 to 9, wherein each data transfer device includes an encryption engine to encrypt data using the key from the controller.

11. A library according to any one of Claims 6 to 10, wherein: the library is a tape drive library; the data transfer devices are tape drives; and the data storage items are tape cartridges.

12. A method of distributing a key to encrypt data for storing on a removable data storage item in a data transfer device library substantially as hereinbefore described with reference to and as shown in the accompanying figures.

13. A data transfer device library substantially as hereinbefore described with reference to and as shown in the accompanying figures.

Amendments to the claims have been filed as follows

1. A method of distributing a key to encrypt data for storing on a removable data storage item ın a data transfer device library, the library comprising a controller having a key associated therewith and being connected to a plurality of data transfer devices each being operable to transfer data to a removable data storage item and having a key store, the method comprising:

providing the key for the library to the controller;

the controller providing the key to the key store of each data transfer device connected to the controller.

2. A method according to Claim 1, wherein the controller, upon initialisation of the library, provides the key to the key store of each data transfer device connected to the controller.

3. A method according to Claim 1 or 2, wherein all the data written to the removable data storage items by the data transfer devices in the library are encrypted with the key in the key store of each data transfer device, the keys being the same.

4. A method according to any preceding claim, wherein data are encrypted using a block encryption technique in which each block of data is encrypted using the key and a respective counter value.

5. A method according to any preceding claim further comprising maintaining a library database containing records of respective libraries and the key associated with a respective library.

6. A data transfer device library comprising a plurality of data transfer devices connected to a controller having a key associated therewith, each data transfer device being operable to transfer data to a removable data storage

item and having a key store to receive the key associated with the controller and to encrypt data with the key, and the controller is operable to provide the key associated therewith to the key store of each data transfer device.

7. A library according to Claim 6, wherein the controller is a library controller and has a library key store pre-programmed with the key.

8. A library according to Claim 6, wherein the controller is distinct from a library controller and has a library key store pre-programmed with the key.

9. A library according to any one of Claims 6 to 8, wherein the controller has a non-volatile memory in which the key is writable.

10. A library according to any one of Claims 6 to 9, wherein each data transfer device includes an encryption engine to encrypt data using the key from the controller.

11. A library according to any one of Claims 6 to 10, wherein the controller is operable to write the key to the key store of each data transfer device in response to initialisation of the library.

12. A library according to any one of Claims 6 to 11, wherein the controller is operable to receive a new key and to distribute the new key to each of the data transfer devices.

13. A library according to any one of Claims 6 to 12, wherein: the library is a tape drive library; the data transfer devices are tape drives; and the data storage items are tape cartridges.

14. A method of distributing a key to encrypt data for storing on a removable data storage item in a data transfer device library substantially as hereinbefore described with reference to and as shown in the accompanying figures.

15. A data transfer device library substantially as hereinbefore described with reference to and as shown in the accompanying figures.

|  |  |  |  |
|---|---|---|---|
| **Application No:** | GB0520602.4 | **Examiner:** | Mr Adam Tucker |
| **Claims searched:** | 1-11 | **Date of search:** | 22 February 2006 |

## 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,Y | X: 1-11;<br>Y: 1-11 | US2003/0074319 A1<br>(Jaquette) See the whole document and in particular paragraphs 5-7, 49, 64, 65, 71-78, 83, 94 & 105 |
| Y | 1-11 | US2005/0071591 A1<br>(Goodman et al.) See the whole document and in particular paragraphs 55 & 56 |
| Y | 1-11 | US5651064 A<br>(Newell) See the whole document and in particular col 2 line 65-col 4 line 2 and col 4 lines 51-62 |
| A | - | US6473861 B1<br>(Stokes) See the whole document and in particular the second embodiment in Fig. 3 |
| A | - | US2004/0101140 A1<br>(Abe) See in particular the abstract and paragraphs 31, 35-37 and Fig. 4 |
| A | - | US6134660 A<br>(Boneh et al.) See the whole document |

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$^X$ :

G4A; G5R; H4P

Worldwide search of patent documents classified in the following areas of the IPC

G06F; G11B; H04L

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

WPI, EPODOC, INSPEC