



(51) International Patent Classification:
G06F 21/02 (2006.01)

(21) International Application Number:
PCT/EP2009/058987

(22) International Filing Date:
14 July 2009 (14.07.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **NEC EUROPE LTD.** [DE/DE]; NEC Laboratories Europe, Rathausallee 10, 53757 Sankt Augustin (DE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **RIPKE, Andreas** [DE/DE]; NEC Europe Ltd., NEC Laboratories Europe, Rathausallee 10, 53757 Sankt Augustin (DE). **KLAAS, Jens** [DE/DE]; NEC Europe Ltd., NEC Laboratories Europe, Rathausallee 10, 53757 Sankt Augustin (DE).

(74) Agent: **VOSSIUS & PARTNER**; Siebertstrasse 4, 81675 München (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: STACKABLE CRYPTOGRAPHIC ADAPTER

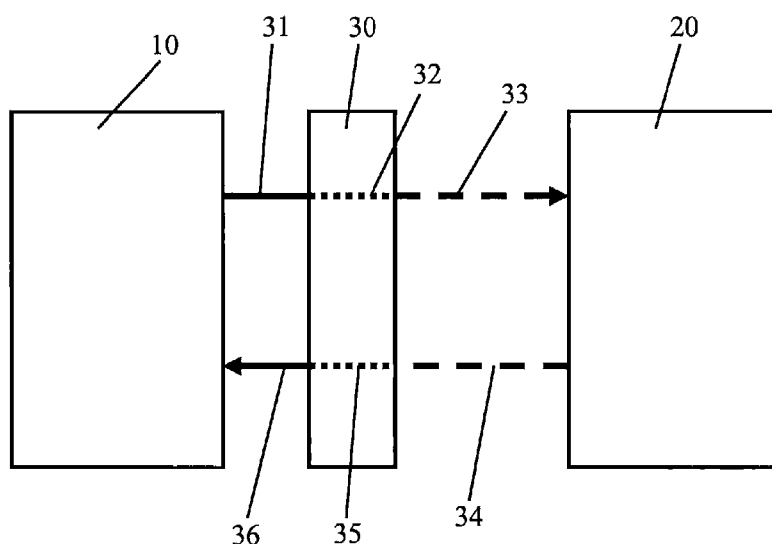


FIG. 1

(57) Abstract: The invention provides for an adapter for a computer system. The adapter is configured to provide encryption and decryption of data to be transmitted to or received from a data storage device. The data storage device is connected via the adapter to the computer system. Further, the invention provides for an adapter kit comprising at least two of the adapter as discussed above. In particular, the plug of the second adapter is connectable to the receptacle of the first adapter. Furthermore, the invention provides a method for encrypting and decrypting data to be transmitted to or received from a data storage device. The method comprises the steps of (a) connecting the data storage device via an adapter or adapter kit to a computer system; (b') encrypting the data to be transmitted to the data storage device upon initiating a USB write command; and/or (b'') decrypting the data received from a data storage device upon initiating a USB read command.

Stackable cryptographic adapter

5 The invention relates to an adapter for a computer system to encrypt and decrypt data. Further, the invention is directed to an adapter kit comprising two or more adapters to encrypt and decrypt data. Furthermore, a method for encrypting and decrypting data is provided. In one embodiment, the data to be encrypted or decrypted is data to be transmitted to or received from a data storage device.

10

A data storage device may be a removable media to store data separately from a computer system. For example, the storage media may contain sensitive or confidential data so that high levels of security are needed to avoid public access.

15 In order to allow access to the data, usually the storage device is connected to a computer system and then a software is used to decrypt the ciphered data received from the storage device. Alternatively, the same or another software is used to cipher data from the computer system before they are transmitted to the storage device.

20 Usually the encryption and decryption steps each require a particular password/keyfile or a encryption key: without using the correct password, the data stored on the storage device cannot be read or the data to be transmitted to the storage device cannot become encrypted.

However, the use of a software as the cryptographic key for encryption and/or decryption
25 of, for example, confidential data has several drawbacks: for example, the software can be easily duplicated or manipulated so that this kind of software keys bears the risk that unauthorized persons may read the confidential data or may hinder originally authorized users to obtain access to the data. Further, the requirement of a password also bears the risk of easy duplication of the password by unauthorized persons. The duplication of the

software and/or the password is often not recognized by the authorized user so that necessary steps to avert any violation are usually taken to late.

Hence, a need exists to provide secure means enabling data transmission to or from a storage device, wherein the data is ciphered, but readable for an authorized user, or is to be ciphered before storage.

The above objects may be achieved with the features of the claims.

10 In particular, the present invention is directed to an adapter for a computer system. A data storage device connected to the computer system via the adapter may contain ciphered data which have to be decrypted by the adapter before any reading by a user. Further, data from the computer system may be transmitted to the storage device and is encrypted by the adapter before storage. Additionally, an adapter kit is provided, comprising two or more
15 adapters as discussed above. Furthermore, the invention is also related to a method for encrypting and decrypting data by using the above adapter and/or adapter kit.

According to the present invention, an adapter for a computer system is provided. The adapter is configured to provide encryption and decryption of data to be transmitted to or
20 received from a data storage device. The data storage device is connected via the adapter to the computer system.

The adapter may be any kind of connecting piece removably attachable/connectable to the computer system and removably attachable/connectable to the data storage media. For
25 example, the adapter may be an adapter providing at least two USB ports for connecting the storage device indirectly to the computer system. According to the present invention the connection between the storage device and the computer system is indirect in contrast to (direct) connections between the storage device and the computer system without using any removable connecting piece.

The (data) storage device may be any media for storing data, for example, a mass storage device or a flash device. The storage device may be a removable/external storage media adapted to be connected to further devices or systems via one or more ports. In a particular embodiment, the storage device is a USB storage media. For instance, the storage media
5 may be connected/attached to the adapter via a particular port, for example, via an external port (provided at the casing of the storage device, and not provided inside the casing), for example, a USB port/plug. A USB port/plug of a storage device is usually applied to connect peripheral devices to computer system and, in the present invention, for example, to an adapter.

10

For example, Universal Serial Bus (USB) storage media may be used as storage media and may also be referred to as “USB stick” or “USB drive”. These storage media may be removable storage media, in particular, removable USB storage media. Removable media are meant herein to be configured for being attached/connected to an external port of the
15 computer system.

For example, due to the decryption of (ciphered) data, the confidential data may be readable only by the user to which the adapter belongs. Further, due to the encryption of the data, these ciphered data may be securely stored in the storage device.

20

In a particular embodiment, the adapter may contain a firmware enabling the encryption and decryption.

Firmware is a program to internally control the functionality of electronic devices, for
25 example, of an adapter. The expression “firmware” is contrasted with “hardware” and “software” which are well-known terms in this technical field. Firmware may be a microcode which cannot be manipulated or changed by a user. For example, in general terms, firmware denotes anything ROM-resident. In a particular embodiment, the functionality of the adapter cannot be manipulated or changed by a user.

30

The adapter containing a firmware enabling/initiating the functionality of the adapter (encryption/decryption of data) may fulfil the function of a cryptographic key and may thus be useful for making ciphered data readable to a user and/or ciphering data before storing them externally.

5

In a particular embodiment, the encryption is an on-the-fly encryption and the decryption is a on-the-fly decryption.

On-the-fly encryption/decryption means that data is automatically encrypted/decrypted right
10 before it is saved/loaded, without any user intervention.

Providing the encryption and decryption “on-the-fly” lets the need for any further access of an authorized user to the computer system become redundant and may thus avoid the possibility of any violation of the transmission of confidential data between the computer
15 system and the data storage device.

In a particular embodiment, the adapter comprises two USB ports.

Universal serial bus (USB) is a serial bus standard to connect devices to a host computer
20 and is well-known in the art of information technology. A USB port may provide a USB plug or may provide a USB socket/receptacle. USB may be used to connect a computer system to external devices, for example digital cameras, flash drives, and external hard drives.

25 In a particular embodiment, the first of the USB ports of the adapter provides a plug and the second USB port provides a socket/receptacle.

In this embodiment, the computer system may be connected to the adapter via the USB plug of the adapter, and the adapter may be connected to the data storage device via the
30 receptacle of the adapter. Particularly, the computer system provides a USB receptacle to

receive the adapter's USB plug, and the data storage device provides a USB plug to be plugged into the receptacle of the adapter.

Using USB may provide a plug-and-socket connection which is easy to handle and which
5 may easily be used with every common computer system and data storage devices.

In a particular embodiment, the adapter is configured to provide encryption upon a USB write command.

10 In this case, as soon as the write command is issued/initiated, the data to be transmitted to the data storage device are encrypted by the adapter. The issuance/initiation of the USB write command may be realized by a particular input of a user without any need for a password or particular key or may, alternatively, start automatically upon (physical) connection between the data storage device and the computer system via the adapter. For
15 example, before connection to the data storage device, the user may have chosen the particular data (in the computer system) to be transmitted to the data storage device, and upon connection to the data storage device via the adapter, the data are automatically encrypted before they are stored in the storage device.

20 Providing encryption upon a USB write command also avoids any intervention of a user, since inputting a password to encrypt the data to be transmitted to the storage device is not necessary anymore.

In a particular embodiment, the adapter is configured to provide decryption upon a USB
25 read command.

Similar to the above encryption, in this case, as soon as the read command is issued/initiated, the data received from the data storage device are decrypted by the adapter before the data is received by the computer system. The issuance/initiation of the USB read
30 command may be realized by a particular input of a user without any need for a password

or particular key or may, alternatively, start automatically upon (physical) connection between the data storage device and the computer system via the adapter. For example, as soon as the data storage device is connected via the adapter to the computer system, the (ciphered) data are automatically transmitted to the computer system via the adapter, and
5 the adapter decrypts these data “on-the-fly”, without any further intervention by a user.

In a particular embodiment, the data storage device is a USB RBC class device.

USB RBC class devices are storage devices that use the reduced block commands
10 (RBC)(subclass 0x01) protocol. The Reduced Block Commands standard defines a minimal command set for logical block addressable storage devices including removable media devices. The RBC set is designed to provide very efficient initiator-to-target operation of input/output logical units (disks, tapes, printers, etc.) by an operating system.

15 In a particular embodiment, the adapter and/or the computer system “understands” the RBC version, that means that they are RBC compatible.

According to the present invention, an adapter kit is provided, comprising at least two of the adapter as discussed above. In particular, the plug of the second adapter is connectable
20 to the receptacle of the first adapter.

The same definitions and particular embodiments as discussed above with reference to the adapter may also be applied to the adapter kit according to the present invention.

25 In a particular embodiment, the kit is adapted to have the data storage device connected to the computer system via the receptacle of the second adapter.

In particular, the two adapters are stacked, wherein the USB plug of the second adapter is plugged in the receptacle of the first adapter. In doing so, an adapter system is provided,
30 wherein the adapter system has two free USB ports, the plug of the first adapter and the

receptacle of the second adapter. In this case, the USB plug of a storage device may be connected to the receptacle of the adapter system, and the plug of the adapter system may be connected to the receptacle of the computer system to provide the (indirect) connection between computer system and data storage device.

5

In a particular embodiment, the adapters are configured to provide encryption and decryption due to their connection.

In this case, an encryption cannot take place without having all adapters of the kit stacked.

10 The storage device may be connected to the computer system via the kit of stacked adapters.

Using a kit of adapters to encrypt data to be transmitted to a storage device is advantageous, since all adapters of the kit are needed to encrypt the data. Theft or loss of any one of the
15 adapters of the kit would not enable the unauthorized person to get any access to the confidential data. Thus, additional security is provided.

In a particular embodiment, each of the adapters contains a firmware. The firmware of the first adapter and the firmware of the second adapter complement each other so as to enable
20 the encryption and decryption.

As defined above, firmware cannot be manipulated or changed by a user, and the firmware controls the functionality of the adapter.

25 In an alternative embodiment, each of the adapters contains a firmware, and each of the adapters may be configured to decrypt and encrypt data as discussed above.

For example, due to the connection between the adapters, the data from the computer system to the storage device is encrypted by the first adapter and then further encrypted by
30 the second adapter. In order to provide decryption, for example, the data from the storage

device has to be firstly transmitted to the second adapter (where a first decryption takes place) and then to the first adapter (where the second decryption takes place). Hence, in this example, the adapters of the adapter kit are connected to each other in a pre-defined order when the data is decrypted, depending on the order of the adapters of the adapter kit during
5 the encryption of the data.

To summarize, in the alternative embodiment, each adapter of the adapter kit is configured to provide encryption and decryption of the data, wherein the adapter kit is configured to provide decryption of the data if and only if the order of the adapters is identical during
10 decryption and encryption.

If the order of the adapters of the adapter kit during decryption is different from the order during encryption, no decryption of the data can take place in this particular embodiment.

15 The above discussed alternative embodiment further increases the safety of the data transmission, since even a loss of the whole adapter kit would not enable an unauthorized person to decrypt encrypted data without knowing the correct order of the adapters.

In a particular embodiment, the firmware of the adapters of the adapter kit are inter-
20 coordinated so that the encryption and decryption may only be provided (as a synergistic effect) if both adapters are stacked and (indirectly) connect the computer system to the storage device. If one of the adapters is not available, no encryption can take place.

In a particular embodiment, the encryption is an on-the-fly encryption and the decryption is
25 an on-the-fly decryption.

As defined above, on-the-fly encryption/decryption means that data is automatically encrypted/decrypted right before it is saved/loaded, without any user intervention.

Providing the encryption and decryption “on-the-fly” may avoid the possibility of any violation of the transmission of confidential data between the computer system and the data storage device and thus further enhances security of the data transmission via the adapter kit.

5

In a particular embodiment, the data storage device is a USB RBC class device.

In a particular embodiment, a system of at least two adapter kits is provided, wherein one of the adapter kits is an adapter kit as discussed above with reference to the particular
10 embodiment teaching that each of the adapters contains a firmware and that the firmware of the first adapter and the firmware of the second adapter complement each other so as to enable the encryption and decryption. The other adapter kit of the system is an adapter kit as discussed above with reference to an alternative embodiment teaching that each of the
15 adapters contains a firmware, and each of the adapters is configured to decrypt and encrypt data, and wherein the adapter kit is configured to provide decryption of the data if and only if the order of the adapters is identical during decryption and encryption.

According to the present invention, a method for encrypting and decrypting data to be transmitted to or received from a data storage device is provided. The method comprises
20 the steps of (a) connecting the data storage device via an adapter or adapter kit to a computer system; (b') encrypting the data to be transmitted to the data storage device upon initiating a USB write command; and/or (b'') decrypting the data received from a data storage device upon initiating a USB read command.

25 The same definitions and particular embodiments as discussed above with reference to the adapter and/or the adapter kit may also be applied to the above-recited method according to the present application.

In the following, the above and other aspects of the invention will be apparent from and
30 exemplified with reference to the embodiments described hereafter.

Fig. 1 schematically shows a computer system connected to a storage device via an adapter according to a particular embodiment of the present invention;

- 5 Fig. 2 schematically shows a computer system connected to a storage device via an adapter kit according to a particular embodiment of the present invention;

Fig. 3 schematically shows a computer system connected to a storage device via an adapter kit according to a particular embodiment of the present invention.

10

Fig. 1 shows a computer system 10 connected to a data storage device 20 via an adapter 30. In a first embodiment, data 31 to be transmitted from the computer system 10 to the storage device 20 is received by the adapter 30, where the data is being encrypted 32. The encrypted/ciphered data 33 is then transmitted to the storage device 20.

15

In a second embodiment, ciphered data 34 is received by the adapter 30 from the storage device 20. In the adapter 30, the data is being decrypted 35, and then the decrypted data 36 is transmitted to the computer system 10.

- 20 Fig. 2 shows a computer system 10 connected to a data storage device 20 via an adapter kit of two adapters 30, 40.

In a first embodiment, data 31 to be transmitted from the computer 10 to the storage device 20 is received by the adapter kit, where the data is being encrypted 42. The encryption takes only place if the two adapters 30, 40 of the kit are stacked. Otherwise the functionalities
25 (for example provided by a particular firmware) of the adapters 30, 40 cannot complement each other to provide the needed synergistic effect resulting in the encryption. After encryption, the ciphered data 43 is further transmitted to the storage device 20.

- In a second embodiment, ciphered data 34 is received by the adapter kit of two adapters 30,
30 40 from the storage device 20. In the adapter kit, the data is being decrypted 45, and then

the decrypted data 46 is further transmitted to the computer system 10. Similar to the first embodiment of Fig. 2, the decryption takes only place if the adapter kit is complete, that means that the adapters 30, 40 of the adapter kit are stacked. Only if the adapters 30, 40 are stacked, their functionality (for example, provided by a particular firmware) is able to
5 provide decryption as a synergistic effect.

Fig. 3 shows a computer system 10 connected to a data storage device 20 via an adapter kit of two adapters 30, 40. In this particular embodiment, each of the adapters 30, 40 of the adapter kit is configured to provide encryption and decryption of data.

10 In a first embodiment, data 31 to be transmitted from the computer 10 to the storage device 20 is received by the first adapter 30 of the adapter kit, where the data is being encrypted 42a. In a next step, the encrypted data 42a is transmitted to the second adapter 40, where the data 42a is further encrypted 42b. After the second encryption, the ciphered data 43 is further transmitted to the storage device 20.

15

In a second embodiment, the ciphered data 34 which was encrypted as explained above (by encryption 42a and 42b) is received by the adapter kit of two adapters 30, 40 from the storage device 20. In the adapter kit, the data is being decrypted 45b by the second adapter 40. After the first decryption, the data 45b is transmitted to the first adapter 30 to be further
20 decrypted 45a, and then the decrypted data 46 is further transmitted to the computer system 10. In this embodiment, the decryption takes only place if the adapter kit is complete and the two adapters 30, 40 are stacked/connected in the same order as during encryption.

In a particular embodiment, a system of at least two adapter kits is provided, wherein one of
25 the adapter kits is the adapter kit shown in Fig. 2 and the other adapter kit is the adapter kit shown in Fig. 3.

Due to the above discussed invention, it may be possible to provide a secure means, i.e. the adapter or the adapter kit, for encryption and decryption of data to be transmitted to or
30 received from a storage device connected to a computer system via the adapter/adapter kit.

Due to the physical possession of the device, additional security is provided to the authorized user, since a theft or a loss of the adapter would be recognized immediately. Hence measures necessary to avert any violation in regard to the confidential content of the storage device can also be taken immediately. Further, the use of the adapter/adapter kit to
5 encrypt and decrypt data does not require the need of inputting a password bearing several risks as discussed above.

Furthermore, by stacking two or more adapters belonging, for example, to different users, the firmware of the adapters may be configured to complement each other in order to
10 provide functionality of the adapter kit. In this case, the encryption/decryption only works if all necessary adapters are stacked so that the security of the encryption/decryption is further enhanced.

The present invention is advantageous for any safe handling of information in general, for
15 example, for providing a safe personal mobile health card.

While the invention has been illustrated and described in detail in the foregoing description, such illustration and description are to be considered illustrative or exemplary and non-restrictive; the invention is thus not limited to the disclosed embodiments. Features
20 mentioned in connection with one embodiment described herein may also be advantageous as features of another embodiment described herein without explicitly showing these features. Variations to the disclosed embodiments can be understood and effected by those skilled in the art and practicing the claimed invention, from a study of the disclosure and the appended claims. In the claims, the word “comprising” does not exclude other elements
25 or steps, and the indefinite article “a” or “an” does not exclude a plurality. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures can not be used to advantage.

CLAIMS

1. Adapter kit for a computer system comprising at least two adapters, wherein
 - each of the adapters comprises a first and a second USB port,
5
 - the first USB port of each adapter provides a plug and the second USB port of each adapter provides a receptacle,
10
 - wherein the plug of the second adapter is connectable to the receptacle of the first adapter, and
 - the adapter kit is configured to provide encryption and decryption of data to be transmitted to or received from a data storage device connected via the adapter kit to the computer system.
15
2. Adapter kit of claim 1, wherein the adapters are configured to provide encryption and decryption due to their connection.
3. Adapter kit of claim 1 or 2, wherein each of the adapters contains a firmware, and
20 wherein the firmware of the first adapter and the firmware of the second adapter complement each other so as to enable the encryption and decryption.
4. Adapter kit of claim 1 or 2 or 3, wherein the encryption is on-the-fly encryption and the decryption is on-the-fly decryption.
25
5. Adapter kit of any one of claims 1 – 4, wherein the data storage device is a USB RBC class device.

6. Adapter kit of any one of claims 1 – 5, wherein the kit is configured to provide encryption upon a USB write command and/or to provide decryption upon a USB read command.

5

7. System of at least two adapter kits, wherein one adapter kit is the adapter kit of claim 3 and the other adapter kit is the adapter of claim 1 with its adapters containing a firmware, and wherein the other adapter kit is configured to provide decryption of the data if and only if the order of the adapters is identical during decryption and encryption.

10

8. Adapter for a computer system configured to provide encryption and decryption of data to be transmitted to or received from a data storage device connected via the adapter to the computer system.

15 9. Adapter of claim 8, wherein the adapter contains a firmware enabling the encryption and decryption.

10. Adapter of claim 8 or 9, wherein the encryption is on-the-fly encryption and the decryption is on-the-fly decryption.

20

11. Adapter of claim 8 or 9 or 10, wherein the adapter comprises two USB ports.

12. Adapter of claim 11, wherein the first of the USB ports provides a plug and the second USB port provides a receptacle.

25

13. Adapter of any one of claims 8 – 12, wherein the adapter is configured to provide encryption upon a USB write command.

14. Adapter of any one claims 8 – 13, wherein the adapter is configured to provide decryption upon a USB read command.

5 15. Adapter of any one of claims 8 – 14, wherein the data storage device is a USB RBC class device.

16. Method for encrypting and decrypting data to be transmitted to or received from a data storage device, comprising the steps of:

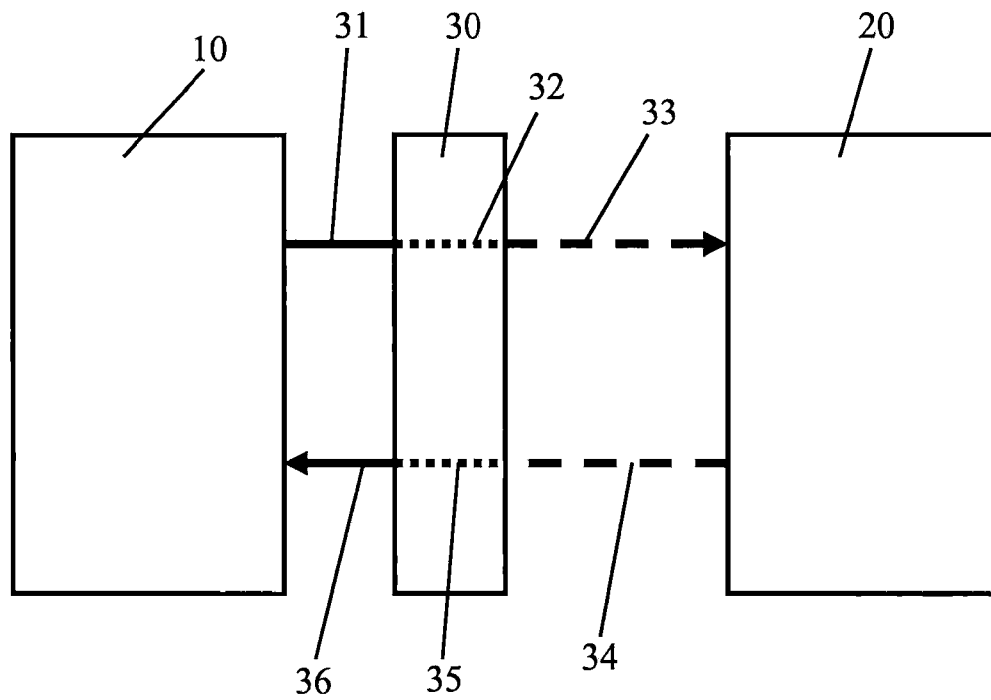
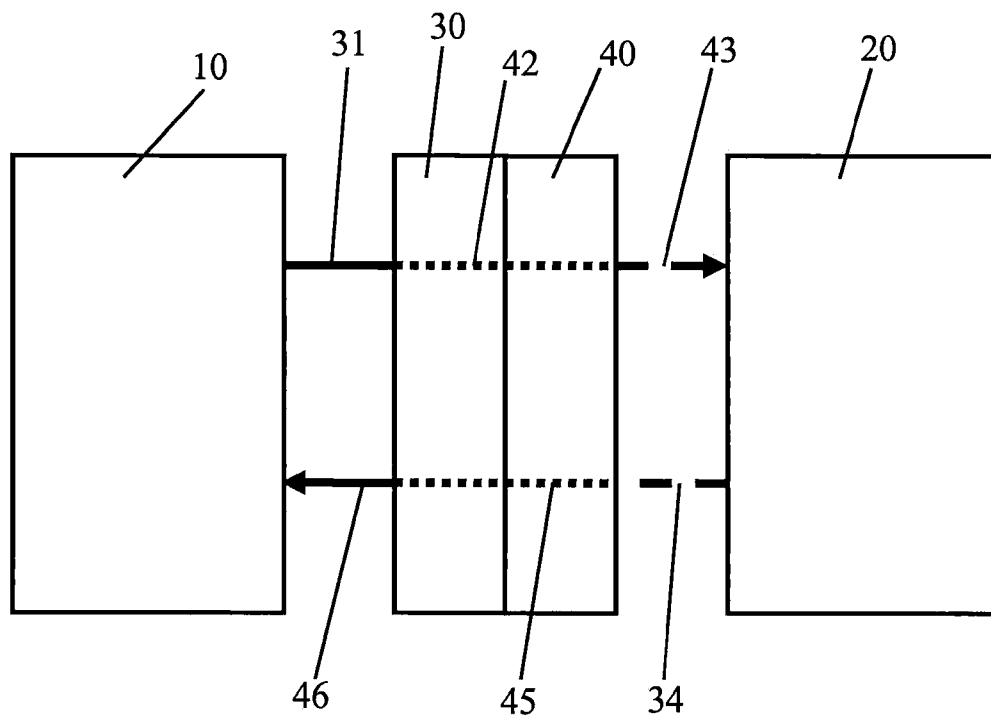
10

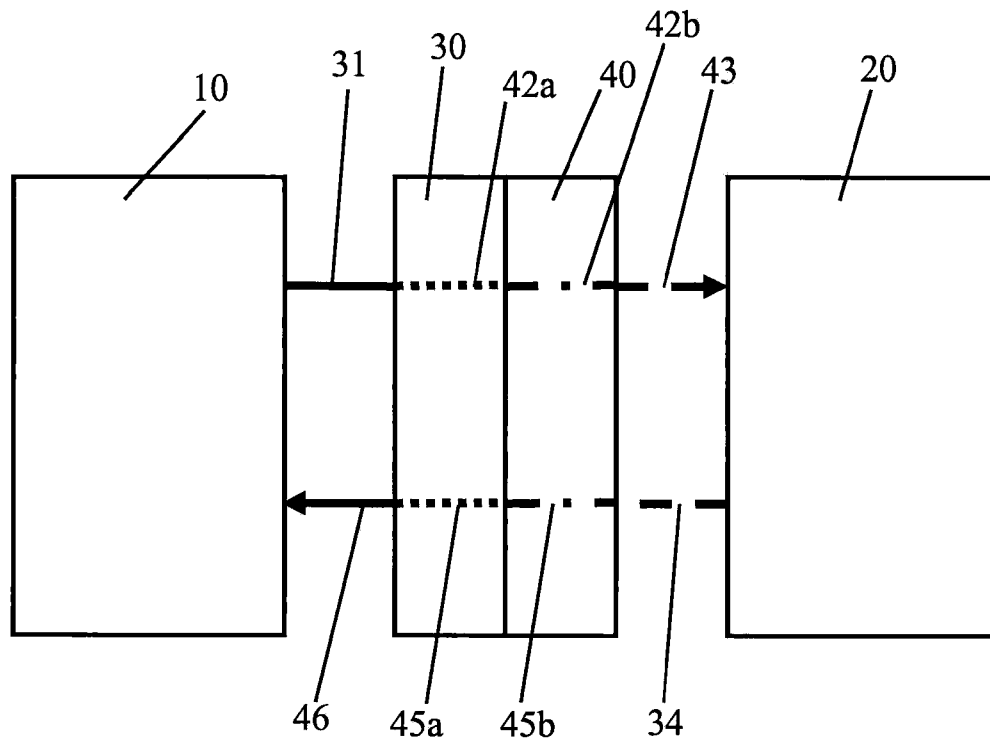
connecting the data storage device via an adapter or adapter kit to a computer system;

encrypting the data to be transmitted to the data storage device upon initiating a USB write command; and/or

15

decrypting the data received from a data storage device upon initiating a USB read command.

**FIG. 1****FIG. 2**

**FIG. 3**

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/058987

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/02

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)
G06F

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, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/033320 A1 (WU VICTOR C [US] ET AL) 8 February 2007 (2007-02-08) figure 3 paragraph [0026] paragraph [0033] -----	1-16

☐ 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 document 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.
- *g* document member of the same patent family

Date of the actual completion of the international search

30 October 2009

Date of mailing of the international search report

09/11/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

van Praagh, Kay

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/058987

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007033320 A1	08-02-2007	CN TW	13-12-2006 11-05-2006