(12) UK Patent Application (19) GB (11) 2 434 887 (13) A

(43) Date of A Publication 08.08.2007

(21) Application No: 0600700.9

(22) Date of Filing: 13.01.2006

(71) Applicant(s):
Deepnet Technologies Ltd
(Incorporated in the United Kingdom)
The Maples Business Centre,
144 Liverpool Road, LONDON, N1 1LA,
United Kingdom

(72) Inventor(s):
Yurong Lin

(74) Agent and/or Address for Service:
Deepnet Security Limited
The Maples Business Centre,
144 Liverpool Road, LONDON, N1 1LA,
United Kingdom

(51) INT CL:
G06F 12/14 (2006.01) ***G06F 21/00*** (2006.01)

(52) UK CL (Edition X):
G4A AAP A23A

(56) Documents Cited:
US 6968459 B1 **US 6785810 B1**
US 20030221113 A1

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

(54) Abstract Title: **Access control by encrypting stored data with a key based on a "fingerprint" of the device storing the data**

(57) The invention provides a method for controlling access to data stored in a digital format on a device. The method comprises securely storing the data on the device by encrypting the data using a device key. The stored data is only accessible by using the device key to decrypt the encrypted data thereby controlling access to the data. The device key is based at least in part on a device "fingerprint" for the device on which the data is stored. The fingerprint may be based on e.g. hardware identifiers or serial numbers storage capacity etc. The data may further be double-encrypted with a user key. If any of the components in the device are changed, the fingerprint may be re-calculated. This may be carried out if the number of replaced components falls below a threshold value, with a user password being required for re-calculation to be done otherwise.

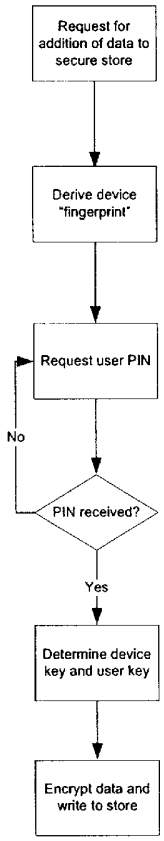

Fig. 2

GB 2 434 887 A

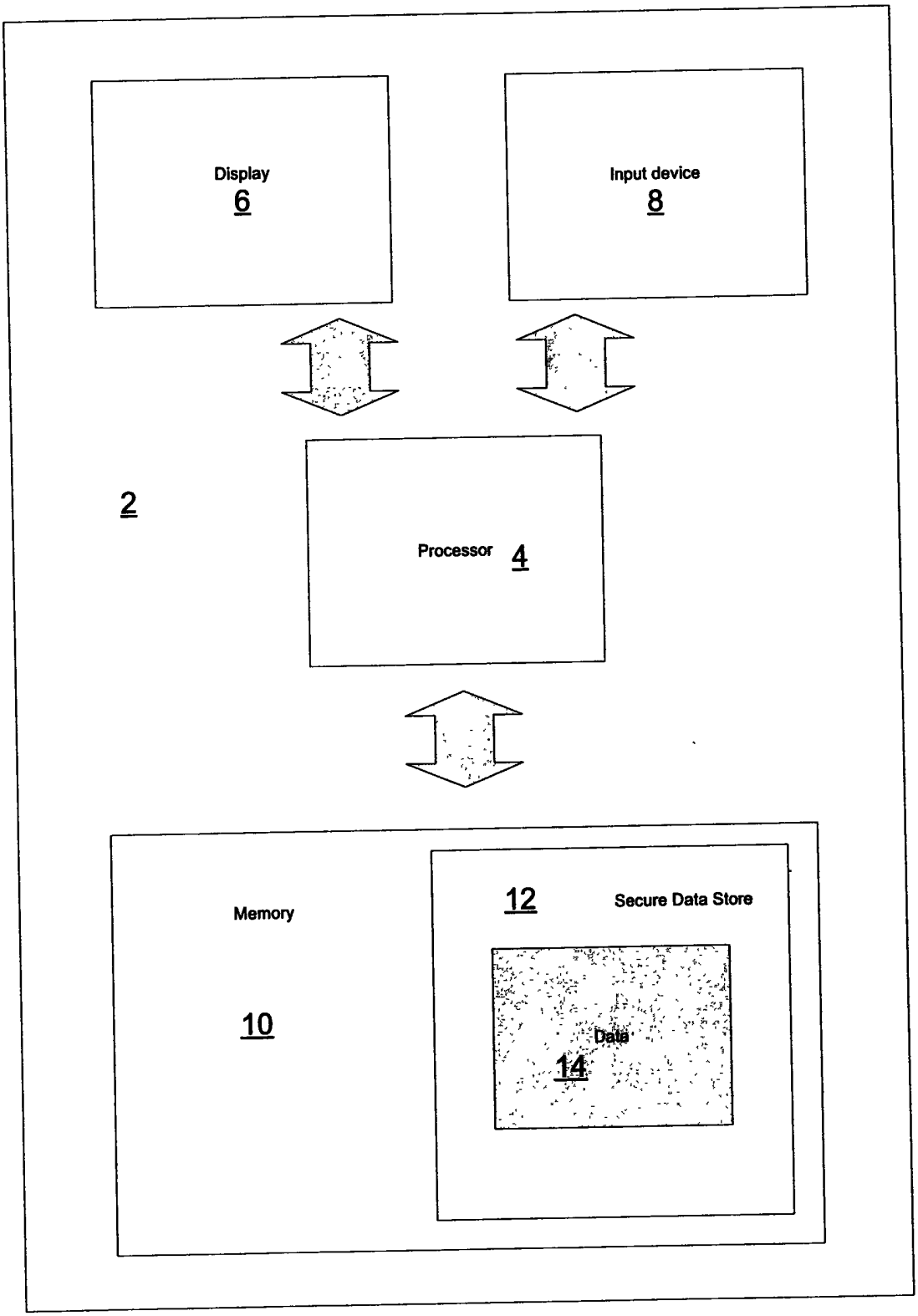
Display
6
Input device
8
2
Processor 4
Memory
10
12
Secure Data Store
Data
14

Fig. 1

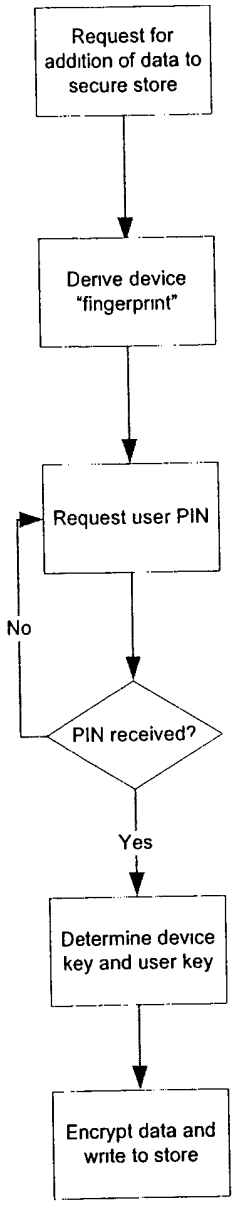

Fig. 2

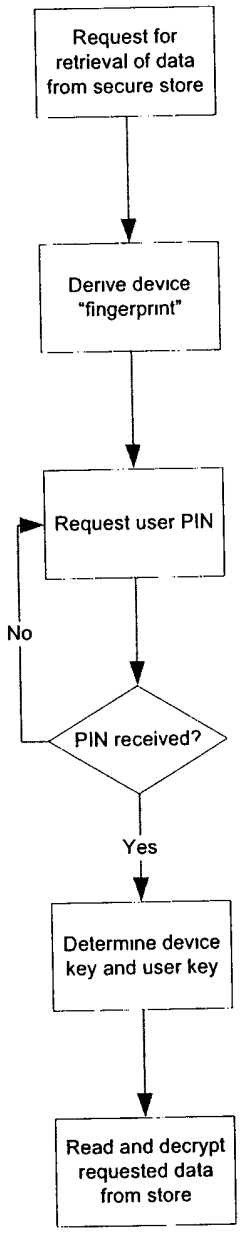

Fig. 3

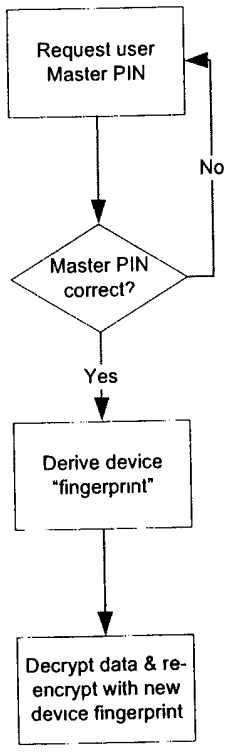

Fig. 4

Access Control

Field of the Invention

The present invention relates methods and systems for controlling access to data stored in a digital format.

Background

There is an increasing demand to be able to better protect data stored in a digital format, for example in the memory of devices such as personal computers (desktops, laptops, handhelds), PDAs (personal digital assistants), mobile (e g cellular and satellite) telephone and other portable communication devices, and other dedicated or general-purpose computers (e g servers), so that access to that data can be restricted only to authorised users. The data to be secured might include sensitive customer information or other business information, personal data or financial information for instance.

Generally data is secured by encrypting it with a key The data can only be accessed using the same key or a related key. The security of the data is therefore reliant on the security of the key(s)

Symmetric key cryptography uses a single key to encrypt and decrypt the data (or a decryption key that can be easily calculated from the encryption key). An example of single key protocol is the 'Data Encryption Standard' (DES)

More common, particularly where the person who will be decrypting the data is not the same as the person encrypting the data, is asymmetric or "public" key cryptography. This asymmetric approach uses a related pair of keys, a "public key" for encryption and a "private key" for decryption. The relationship between the two keys is a complex one. The public key can be freely distributed and used to encrypt data that can only be subsequently decrypted by a user who holds the private key The most commonly used public key protocol is the 'RSA public key cryptosystem'.

Symmetric key cryptographic methods are appropriate for securing data on a device, especially where the data is only ever intended to be stored and accessed by a single user or a group of users who can securely share a single "private" key. Asymmetric techniques can also be used, however, and may be more universally applicable.

Both symmetric and asymmetric encryption are inherently unreliable in an environment where keylogging applications and other forms of spyware are more prevalent and can be used to illicitly obtain copies of the cryptographic keys

Summary of Invention

The present invention provides a key-based symmetric encryption method for controlling access to data in which the encryption and decryption keys are based at least in part on an identifier, referred to in the following as a "device fingerprint", for the device on which the data is stored

In this way, not only is the data stored in an encrypted format but it also has an in-built association with the device on which it is stored This attribute of the data can be used to ensure that the data can only be accessed on the device it was originally stored on, preventing the 'theft' of such data

The term "data" used herein is intended to include any information, object, application, commands or other data that can be stored in a digital format and may include a collection of multiple types of data

In a first aspect, the invention provides a method for controlling access to data stored in a digital format on a device, the method comprising:

securely storing the data on the device by encrypting the data using a device key;

the stored data only being accessible by using the device key to decrypt the encrypted data thereby controlling access to the data,

the device key being based at least in part on a device fingerprint for the device on which the data is stored

In a second aspect, the invention provides a method of securely storing data in a digital format on a device, the method comprising encrypting the data using a device key based at least in part on a device fingerprint for the device on which the data is stored.

In a third aspect, the invention provides a method of accessing data stored in a digital format on a device, the data having been stored on the device in an encrypted format using a device key, the method comprising decrypting the data using the device key, the device key being based at least in part on a device fingerprint for the device on which the data is stored

Preferably, the device key (based on the device fingerprint) is constructed each time it is used for decryption of data It may also be constructed each time it is used for encryption.

The device fingerprint for the device on which the data is stored at the time of encryption or decryption is acquired and used to construct the key. By constructing the key 'on the fly' in this way, it avoids the possibility that someone obtains a copy of a key based on the fingerprint of the original device and uses it to decrypt a copy of the data on another device. In other words, it ties the data to the device.

As already noted above, the device fingerprint is an identifier, preferably a unique identifier, for the device on which the data is stored. The fingerprint is preferably based on one or more physical properties of the device, most preferably a combination of more than one

The physical properties may be any one or more properties of one or more component parts of the device, for example properties of a processor (e g. CPU), such as the serial no. or ID of the processor, a storage unit (e g. a hard disk), such as serial no., volume no , or a geometric property such as capacity or sector format; a video card, such as serial no., volatile or non-volatile memory components (e g RAM chips or flash memory chips), such as serial no. or capacity hardware interfaces (e.g network adapters), such as serial no. or transfer rate; etc.

Preferably the fingerprint is derived from at least three or more physical properties of the device, more preferably 4 or 5 or more. It may be based on as many as 10 or more properties. It is also preferred that the fingerprint is derived from the properties of two or more separate components of the device, preferably three or more separate components of the device

The fingerprint may be calculated as a function of values associated with the chosen physical properties of the device (e g. if one of the chosen properties is hard disk capacity and the capacity is 81,956,655,104 bytes, then the value used in the function could be 81956655104) The finger print may for example be calculated as a hash function of values of the chosen physical parameters. In some preferred embodiments of the invention is a hash function based MAC (Message Authentication Code) of the combination of the chosen physical properties.

The approach described above effectively locks the stored, encrypted data to a specific device It does not, however, serve to secure the data in the event that the device itself is stolen Nor does it prevent access by one legitimate user of a device to data stored on the device by another legitimate user of the device.

Preferably, therefore, the data is encrypted with a key that is specific to the user (a "user key")

This may be achieved by encrypting the data with a key that is derived from a combination of the device fingerprint and one or more user password values provided by (e g selected or input by) the user, for example a PIN

More preferably, the data is double encrypted with a user key and the device key (based on the device fingerprint as discussed above). The user key may be (or be derived from, e g. a hash function of) one or more user password values provided by (e.g. selected or input by) the

user, for example a PIN It is preferred that the data is first encrypted with the user key and then with the device key, but the reverse is possible. The user key can be a symmetric key or an asymmetric key.

In this way, not only is the data secured on a specific device but it is also only accessible to a user possessing the correct user key (e g password(s)).

In a fourth aspect, the invention provides a device for storing data securely, the device comprising.

a memory;

a secure data store in the memory,

means for adding data to the secure data store, including means for encrypting the data with a device key,

means for retrieving data from the secure data store, including means for decrypting the data with the device key;

the device key being based at least in part on a device fingerprint of the device.

The device fingerprint may be derived in the manner discussed above. The means for adding and retrieving data may also enable double encryption of the data with the device key and a user key in the manner discussed above.

The means for adding and retrieving data to and from the secure data store is preferably embodied in firmware or software resident on the device, the device having a processor operable under the control of the firmware or software to add and retrieve the data

The device preferably also includes means for constructing the device key at the time data is retrieved and/or stored, including means for deriving the device fingerprint. Such means are preferably embodied in firmware or software resident on the device

The device preferably also includes one or more components for inputting a password Possible input components include keyboards, pointer devices, touch screens, scanners to obtain biometric data (e g. finger prints) from a user, microphones, etc.

The device may be a personal computer (e g. desktop, laptop, handheld), PDA (personal digital assistant), mobile (e.g. cellular or satellite) telephone or other portable communication device, or some other dedicated or general-purpose computer (e.g. a server) Typically the device will have uses in addition to the secure storage of data but in some embodiments of the invention it may be dedicated to this use

The memory is preferably non-volatile memory. Possible examples include read-only memory (ROM), flash memory and storage devices such as hard disks and optical disks. The memory may be shared with other, non-encrypted data or may be reserved exclusively for the secure data store. The secure data store may be distributed across multiple physical memory components.

If a component of a device on which the fingerprint is based is changed (e g. upgraded or replaced because it has become faulty) then the fingerprint itself may change. Provision is therefore preferably made for updating the secure data store on a device so that a decryption key based on the updated device fingerprint can be used to access the encrypted data within the store This updating process may be automatic where only one or a small number of components (below a predetermined threshold) have changed, to allow for updating of the fingerprint without manual intervention when e g. a device component is upgraded as will happen from time to time.

To guard against abuse of this facility, however, particularly where multiple components are changed at the same time (or the number of components changed exceeds a threshold) a user may be required in such circumstances to provide one or more passwords (preferably necessarily different from any password used to derive the encryption keys) to effect any such change and/or to provide access to the encrypted data.

The facility may also be configured to only recognise changes in a limited number of device components at any one time on the assumption that if more components change it is more likely to be an indication that the data has been moved to a new device rather than being on the same device with updated components.

Data resident on the device when the fingerprint is updated can be re-encrypted with the new device key (based on the new fingerprint).

In a fifth aspect the invention provides a computer program product comprising program code that when run on a computer device causes the device to operate in accordance with one or more of the methods of the first to third aspects above or as a device in accordance with the fourth aspect above

Brief Description of Drawings

An embodiment of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which

Fig 1 schematically shows a device in accordance with an embodiment of the present invention;

Fig 2 illustrates a process for storing data to a secure data store on the device of fig 1;

Fig 3 illustrates a process for retrieving data from the secure data store;

Fig 4 illustrates a process for initially setting up and/or modifying an encryption key for the secure data store

Description of Embodiment

Embodiments of the present invention are useful for a variety of applications where it is desired to store data securely, especially where it is desired to lock the data to a specific device Some examples include the provision of virtual (i e. software based) smart card functionality (as we describe, for example, in our application filed on the same date as this one with the title "Smart Card Systems") and other token-based authentication or digital signature applications for securely storing the tokens on a device

In the illustrated embodiment, data is stored on a device in an encrypted form in such a way that it is tied to the specific device as well as only being accessible to an authorised user (possessing a PIN). This is achieved by encrypting and decrypting the data using two keys, one that is based on a fingerprint of the device, constructed on the fly, and a second based on a PIN input by the user. The data is double encrypted when it is stored, using both keys, which must then both be used to decrypt the data

The encryption system itself may be any of a variety of available symmetrical, or more preferably asymmetrical encryption systems, e.g RSA encryption.

Fig. 1 schematically shows the main components of a device 2 that can be used to implement an embodiment of the present invention. The device 2 may be a personal computer (e.g desktop, laptop, handheld), PDA (personal digital assistant), mobile (e.g. cellular or satellite) telephone or other portable communication device, or some other dedicated or general-purpose computer (e g a server)

The device comprises, amongst other things, a processor 4, a display 6, an input component 8 and a non-volatile memory 10. The memory includes a secure data store 12 for encrypted data 14.

The processes necessary to add data to the secure store 12 and retrieve data from the store 12 are carried out by the processor 4 under the control of a software application (implemented either in firmware or software) resident on the device 2.

In use, as illustrated in fig. 2, data 14 is double encrypted using a user key (e g. a PIN or a key derived from a PIN entered by the user) and a device key (derived from the device fingerprint of device 2) and then written to the secure data store 12 in the memory 10

To extract encrypted data 14 from the store 12, in response to a request from a user (or some other source), as seen in fig. 3, the processor 4 must use the device key and user key to decrypt the data 14.

The keys are only ever stored in a temporal form to be used in a single encryption/decryption process The user key (e g. PIN) must be obtained from the user and the device key must be constructed before each decryption process To construct the device key, the processor 4 first derives the device fingerprint by interrogating one or more components or registers in the device 2 to obtain a series of physical attributes of these components, e g. processor serial no , hard disk volume no. and capacity and video card serial no., these in combination defining the device fingerprint. The user is then requested, for example by a message displayed on the display 6 of the device2, to enter their PIN. Once the PIN has been entered, using input component 8 (e g. a key pad), the processor constructs the keys based on the entered PIN and the device fingerprint respectively. The requested data 14 is then read from the data store 12 and the keys used to decrypt it.

When accessing data, if either the PIN entered by the user or the device fingerprint are incorrect (e g because the data has been copied to another device) then one or both of the keys constructed by the processor will not match the respective key(s) originally used to store the data 14 and the decryption will fail

To allow for the fact that some components in a device might change over time (and the device fingerprint and hence the device key may be based on a changed component) a tolerance mechanism may be built into the encryption application in order that data stored on the device can still be accessed in such circumstances. Preferably when the device fingerprint changes the stored data is automatically re-encrypted with the new device key based on the revised fingerprint, without the need for user intervention

If, however, the device fingerprint has changed to a greater degree that would be expected with the replacement of only one or two components, it may be an indication that the data has been stolen and an attempt is being made to access the data on a completely different device In such cases, automatic recovery of the data (as explained in the paragraph above) is not appropriate. On the other hand, there may be legitimate reasons for the change, and manual recovery of the data is preferably therefore possible.

More specifically, as illustrated in Fig. 4 shows the process that can be used to access data and re-encrypt it with a new device fingerprint on a device whose fingerprint has changed beyond an acceptable threshold. First, the user is requested to enter a Master PIN (this is different from the PIN used for the user key), which they can do in the manner described above for entering the user key PIN. If this Master PIN is correct, the processor proceeds to read the new device fingerprint, and then uses the new fingerprint to create a new device key and re-encrypt the stored data so that it can subsequently be accessed again in the manner described above.

The skilled person will appreciate that the specific embodiment described above is given by way of example only. Many and various modifications are possible within the scope of the invention

Claims

1. A method for controlling access to data stored in a digital format on a device, the method comprising:

securely storing the data on the device by encrypting the data using a device key;

the stored data only being accessible by using the device key to decrypt the encrypted data thereby controlling access to the data;

the device key being based at least in part on a device fingerprint for the device on which the data is stored.

2. A method of securely storing data in a digital format on a device, the method comprising encrypting the data using a device key based at least in part on a device fingerprint for the device on which the data is stored.

3. A method of accessing data stored in a digital format on a device, the data having been stored on the device in an encrypted format using a device key, the method comprising decrypting the data using the device key, the device key being based at least in part on a device fingerprint for the device on which the data is stored.

4. A method according to any one of the preceding claims, wherein the device key is constructed each time it is used for decryption of data and/or each time it is used for encryption.

5. A method according to any one of the preceding claims, wherein the device fingerprint is based on a combination of physical properties of the device.

6. A method according to claim 5, wherein the physical properties are any one or more properties of one or more component parts of the device.

7. A method according to claim 6, wherein the physical properties are selected from the properties of: a processor; a storage unit; a video card; volatile or non-volatile memory components and hardware interfaces.

8. A method according to any one of claims 5 to 7, wherein the fingerprint is derived from at least three or more physical properties of the device

9. A method according to any one of claims 5 to 8, wherein the fingerprint is derived from the properties of two or more separate components of the device.

10. A method according to any one of the preceding claims, wherein the data is encrypted with a key that is specific to the user.

11. A method according to claim 10, wherein the data is encrypted with a key that is derived from a combination of the device fingerprint and one or more user password values provided by the user.

12. A method according to claim 10, wherein the data is double encrypted with a user key and the device key

13. A method according to claim 12, wherein the data is first encrypted with the user key and then with the device key.

14. A method according to any one of the preceding claims, wherein when a component of a device on which the fingerprint is based is changed the secure data store on a device is updated so that a decryption key based on the updated device fingerprint can be used to access the encrypted data within the store.

15. A method according to claim 14, wherein the data store is updated automatically if only a number of components below a predetermined threshold have changed.

16. A method according to claim 15, wherein if the number of components that change exceeds a threshold a user is required to provide one or more passwords to effect any such change and/or to provide access to the encrypted data.

17. A device for storing data securely, the device comprising:

a memory;

a secure data store in the memory;

means for adding data to the secure data store, including means for encrypting the data with a device key;

means for retrieving data from the secure data store, including means for decrypting the data with the device key;

the device key being based at least in part on a device fingerprint of the device.

18. A device according to claim 17, wherein the means for adding data to and/or the means for retrieving data from the secure data store is embodied in firmware or software resident on the device, the device having a processor operable under the control of the firmware or software to add and retrieve the data.

19. A device according to claim 17 or claim 18, comprising means for constructing the device key at the time data is retrieved and/or stored, including means for deriving the device fingerprint.

20. A device according to any one of claims 17 to 19, comprising one or more components for inputting a password.

21. A device according to any one of claims 17 to 20, wherein the device is a personal computer (e.g. desktop, laptop, handheld), PDA (personal digital assistant), mobile (e.g. cellular or satellite) telephone or other portable communication device, or some other dedicated or general-purpose computer (e.g. a server).

22. A device according to any one of claims 17 to 21, wherein the memory is non-volatile memory.

23. A computer program comprising program code that when run on a computer device causes the device to operate in accordance with any one of claims 1 to16 or as a device in accordance with any one of claims 17 to 22.

Intellectual Property Office

For Creativity and Innovation

12.

Application No: GB0600700.9 **Examiner:** Mr Steven Davies

Claims searched: 1-23 **Date of search:** 4 May 2007

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: 1,3, 5,17 at least Y: 12 at least	US 6968459 B1 (Morgan et al) e.g. column 3, line 5 to column 6, line 22
X,Y	X: 1,3, 17 at least Y: 12 at least	US 2003/0221113 A1 (Kupka et al) e.g. paras. 0060 - 0090, 0096 - 0103
Y	12 at least	US 6785810 B1 (Lirov et al) e.g. column 5, lines 53-67

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

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

G06F

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

Online: WPI, EPODOC, INSPEC

International Classification:

Subclass	Subgroup	Valid From
G06F	0012/14	01/01/2006
G06F	0021/00	01/01/2006