METHOD OF SECURE PIN ENTRY AND OPERATION MODE SETTING IN A PERSONAL PORTABLE DEVICE

The invention relates to a portable electronic device comprising: means for fingerprint user authentication having a fingerprint sensor; means for entering first data; wherein said means for entering said first data being coupled to the fingerprint sensor; said first data being entered by sensing a presence of an object relative to the fingerprint sensor, the first data being independent of biometric characteristics of the object.
FIELD OF INVENTION

The present invention relates to a method of secure PIN entry and operation mode setting in a personal portable device.

BACKGROUND AND RELATED ART

Typically, a fingerprint sensor is used to scan a fingerprint image. The retrieved fingerprint image is processed to extract identity parameters (template). The identity parameters are then compared with previously registered identity parameters which are stored within the portable device. US 6,484,260 B1, US 6,484,260 B1 and US 6,766,040 B1 describe fingerprint identification devices.


If the fingerprint is found to be valid (authenticated), specific functions are enabled, like access is granted. Several such personal portable devices are currently on the market, particularly as biometrics flash disks, biometrics tokens, biometrics smart cards etc.

Typically, these personal portable devices have features built in for situations where the fingerprint identity parameters are to be erased or the authentication of the fin-
gerprint identity parameter needs to be bypassed. In addition, there may be other requirements of adding an additional authentication factor. In both cases a password or PIN input is used where the password or PIN is entered from the PC. To operate without any special software on a PC, the personal portable device has an integrated PIN-Pad or switch.

In prior art devices, the PIN entry is done by entering the PIN via a computer terminal and transmitting the PIN via computer serial ports such as RS232 or USB, or a wireless interface. This allows a hacker to use known attacks like a keystroke logger to retrieve the PINs or modify the application which enables the PIN entry.

Additionally, this application software may work on one operating system such as Windows, but may not work on another operating system such as Mac OS or Linux. Therefore, the use of a password entry via a PC is quite limited.

In another type of prior art devices, one or several tactile switches (PIN-pad) are used. The use of a tactile switch is easily subjected to hacking too. A typical tactile switch circuitry is shown in Figure 1. It has an input line to the central processing unit of the device. The input line is connected to a pull up resistor. The line is typically HIGH. When a tactile switch is pressed, the LINE becomes LOW. Usually, a small tactile switch is pressed by a fingernail or a pencil tip. However, since it is only an input line, a potential hacker, who gets hold of the device and knows how the device works, could tap the line and send HIGH and LOW signals representing the PIN to get unauthorized access.

Another disadvantage of using tactile switches is that they are small mechanical parts which are additional components and potentially subjected to fail due to wear and tear.

A smart card typically contains non-volatile memory and microprocessor components with various tamper-resistant properties and is capable of providing security services. Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. The embedded chip of a smart card usually implements some cryptographic algorithm. Information about the
inner workings of this algorithm can be obtained if the precise time and electrical current required for certain encryption or decryption operations is measured. The smart cards are commonly used in both, financial and identification sectors. In the financial sector, the smart cards are commonly used as credit and ATM cards. Smart cards may also be used as electronic wallets. The smart card chip can be loaded with funds which can be spent in parking meters, vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the smart card and an accepting machine.

In the identification sector, smart cards are used for authentication of identity. The most common example is in conjunction with a PKI. The smart card will store personal keys and so called encrypted digital certificates, issued from the PKI, along with other relevant or needed information about the card holder. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC) and the use of various smart cards by many governments as identification cards for their citizens. Smart cards are a privacy-enhancing technology, as the person carries and controls it's personal information all the time.

Examples of cryptographic algorithms are provided below:

<table>
<thead>
<tr>
<th>Cryptographic Algorithm</th>
<th>Applicable Specification</th>
<th>Cryptographic Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RNG</td>
<td>ANSI X9.82, FIPS 180-2</td>
<td>Deterministic Random Bit Generator</td>
</tr>
<tr>
<td>SHA-1</td>
<td>FIPS 180-2</td>
<td>Secure Hash Algorithm - 160 bit</td>
</tr>
<tr>
<td>MD5</td>
<td>RFC 1321</td>
<td>Message Digest -128 bit</td>
</tr>
<tr>
<td>T-DES</td>
<td>FIPS 46-3</td>
<td>Basic Encryption and Decryption</td>
</tr>
<tr>
<td>FIPS 46-3</td>
<td>ECB Wrapper</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-38A</td>
<td>CBC Wrapper</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-38A</td>
<td>CTR Wrapper</td>
<td></td>
</tr>
<tr>
<td>AES (128-bit)</td>
<td>FIPS 197</td>
<td>Basic Encryption</td>
</tr>
<tr>
<td>Protocol</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>FIPS 197</td>
<td>Basic Encryption</td>
<td></td>
</tr>
<tr>
<td>FIPS 197</td>
<td>ECB Wrapper</td>
<td></td>
</tr>
<tr>
<td>FIPS 113</td>
<td>CBC-MAC Encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wrapper</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-38A</td>
<td>CBC Decryption Wrapper</td>
<td></td>
</tr>
<tr>
<td>NIST SP 800-38A</td>
<td>CTR Wrapper</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.11i</td>
<td>CCM Wrapper</td>
<td></td>
</tr>
</tbody>
</table>

In prior art, as in Figure 7, a USB HUB 06 is required to integrate a cryptographic processing unit, a mass storage unit and an identity processing unit. Inter-module data and command communication has to be done via connected PC host and not within the device. This implementation is not very secure as sensitive information is communicated and processed outside of the device.

In addition, an implementation using a USB2.0 HUB will consume a lot of current and generate a significant amount of heat. This will affect the quality and usability of the device.

It is therefore an object of the present invention to provide an improved portable electronic device.

**Summary of the invention**

The invention provides a portable electronic device and a method of PIN entry as claimed in the independent claims. Embodiments of the invention are given in the dependent claims.

Embodiments of the invention provide a portable electronic device, such as an USB stick, that has means for fingerprint user authentication having a fingerprint sensor and means for entering first data, wherein the means for entering said first data being coupled to the fingerprint sensor, the first data being entered by sensing a presence of an object relative to the fingerprint sensor,
the first data being independent of biometric characteristics of the object.

The means for fingerprint user authentication can implement any suitable prior art method for biometric user authentication based on the user's fingerprint. The portable device also enables entry of first data that is unrelated to the user's fingerprint or data extracted from the user's fingerprint. The first data can be a PIN, a cryptographic key or a seed value for generating a cryptographic key by the portable electronic device, or any other kind of user data.

Embodiments of the invention are particularly advantageous as the fingerprint sensor is not only used for sensing the user's fingerprint but also for entry of the first data. Entry of the first data using the fingerprint sensor is accomplished by the means for entering by sensing the presence of an object relative to the fingerprint sensor. This object can be an arbitrary finger, an entry pen or any other object that can be moved over the fingerprint sensor. The process of repetitively moving the object onto the fingerprint sensor and removing the object from the fingerprint sensor is sensed using the fingerprint sensor and a sensor signal delivered by the fingerprint sensor is used by the means for entering for the entry of the first data.

For entry of the first data using the fingerprint sensor predefined patterns can be stored by the portable device. For example, a first pattern is the sensor signal received when the object is moved from the left to the right over the fingerprint sensor and a second pattern is the sensor signal received when the object is moved from the right to the left over the fingerprint sensor. A first information is assigned to the first pattern and a second information is assigned to the second pattern. The first information can be a one bit information, such as logical 0, a digit, a letter or another information. The second information can also be a one bit information, such as logical 0, a digit, a letter or another information and is different from the first information.

By moving the object relative to the fingerprint sensor using the predefined patterns a sequence of the first and second information is entered that constitutes in combination the first data.
In accordance with an embodiment of the invention each pattern stored in the portable device defines a gesture to be entered by the user using his finger or another object, such as an entry pen.

In accordance with an embodiment of the invention by means of a predefined first pattern a first entry mode for the first data can be selected and by means of a predefined second pattern a second entry mode for the first data can be selected. In the first entry mode a first set of characters is assigned to each pattern of a predefined pattern set. In the second entry mode a second set of characters is assigned to each pattern of the predefined pattern set. For example, the first set of characters contains Chinese characters and the second set contains Latin characters. Alternatively, the first set contains letters and the second set of characters contains numbers.

When the means for entering first data detects the first pattern from the signal delivered by the fingerprint sensor, the first entry mode is selected. Next, when a pattern from the predefined pattern set is detected as a consequence the character from the first set of characters being assigned to that pattern is entered.

Likewise, when the means for entering first data detects the second pattern from the signal delivered by the fingerprint sensor, the second entry mode is selected. Next, when a pattern from the predefined pattern set is detected as a consequence the character from the second set of characters being assigned to that pattern is entered.

In accordance with an embodiment of the invention the means for entering first data is implemented as a computer program being executed by a processor of the portable electronic device. The fingerprint sensor delivers a sequence of images to the computer program. The computer program performs an analysis of the sequence of images for detection of the first or second mode selection patterns and/or any pattern of the predefined pattern set. For example, the computer program can be operable to repetitively poll the fingerprint sensor for image data.
In accordance with an embodiment of the invention the first data is a user credential, such as a PIN, for user authentication vis-à-vis the portable electronic device. This facilitates two factor user authentication based on the PIN and the fingerprint.

In accordance with an embodiment of the invention the first data is a user credential, such as a PIN, for user authentication vis-à-vis a chip or IC card that is coupled to the portable electronic device by means of a chip card reader that is integrated into the portable electronic device. The first data is entered only once and is permanently stored in a secure storage region of the portable electronic device when a user enrolment process is performed. After successful one factor user authentication vis-à-vis the portable electronic device based on the fingerprint, the portable electronic device internally reads the first data and sends the first data to the chip card for enabling a functionality of the chip card such as a signature function or the like.

Embodiments of the invention provide a method of a secure PIN (Personal Identification Number) entry and first data input respectively as well as operation mode setting using a fingerprint sensor integrated in a portable device, which comprises at least a fingerprint biometrics processing unit. The fingerprint biometrics processing unit retrieves the fingerprint data, from outside the device, performs signal processing, and authenticates the retrieved signal against identity parameters stored within the device, independent from a PC Host. The result of the authentication is used to enable secured portable device functions e.g. flash memory, security token, smart card etc. In the present invention, the fingerprint sensor is not only used to sense the fingerprint image but also to detect whether an object or a finger is present or absent. The finger detection together with the detection time and duration or together with the direction of movement of finger on the sensor defines a method of a secure PIN entry and first data input respectively as well as operation mode setting. It further describes a portable device that comprises an identity processing unit, a cryptographic processing unit and a mass storage unit. The identity processing unit in this invention authenticates the owner of the device. The identity processing unit can be a biometrics processing unit, a radio frequency identity reader (RFID) or a wireless smart card reader. The identity processing unit retrieves the identification signal, from outside the device, performs signal processing, and authenticates the
signal retrieved against identity parameters stored within the device independent from a PC Host. The cryptographic processing unit is used to read a smart card which enables seamless integration into Public Key Infrastructure (PKI) architectures and stores users' personal certificate credentials, such as private keys, passwords and digital certificate. Unlike other smart card systems which are accessed by entering a Personal Identification Number (PIN) in the personal computer; the identity processing unit is used to enable secure access to the smart card, once authenticated, by releasing the PIN without going through a PC. The PIN number is securely embedded within the device and cannot be accessed by any PC. In addition, the cryptographic processor can generate one time passwords and enable the security token by an authenticated identity entry. The access to the mass storage device storing second data is also protected by the identity authentication. The second data stored within the device is encrypted. The encryption keys are stored within the device. The encryption key is generated in the mass storage processor from two encryption keys that are physically stored in two separate integrated circuits.

In accordance with embodiments of the invention one or more unique identifiers are stored in the portable device. Each unique identifier can be a hardware address, such as a MAC address, a Computer Processing Unit (CPU) ID or a Hard Disk (HDD) ID. The unique identifier can be entered into the portable device to be stored there, using a specific software program or as the first data using the fingerprint sensor.

In accordance with embodiments of the invention the unique identifier stored in the portable device is assigned to an external computer, such as a personal computer (PC). The external computer has a Computer identifier (ID), such as a hardware address, such as a MAC address, a Computer Processing Unit (CPU) ID or a Hard Disk (HDD) ID. The portable device has an interface for coupling to an interface of the computer, such as an USB interface. When the portable device is coupled to the computer via the interface the computer sends its Computer ID to the portable device.

The portable device compares the Computer ID received from the computer with the unique identifier. The portable device grants access to the computer for use of any
one of its functions, such as access to its mass storage, if the received Computer ID and the unique identifier are matching. For example, the computer can only read data from the portable device when its Computer ID and the unique identifier are identical. If more than one unique identifier is stored in the portable device, the Computer ID needs to be identical to one of these unique identifiers. (Host ID authentication)

In accordance with an embodiment of the invention the external computer sends its computer ID in encrypted form to the portable device. This prevents the computer ID from being intercepted by unauthorized parties. The portable device decrypts the encrypted computer ID and compares the decrypted computer ID with the at least one unique identifier stored in the portable device.

In accordance with embodiments of the invention a two factor authentication is required as a further precondition for granting of access to any one of the functionalities of the portable device to the computer. The two factor authentication can require fingerprint authentication and entry of a PIN via the fingerprint sensor as first data.

In accordance with embodiments of the invention Host ID authentication is done concurrently with fingerprint authentication and/or two factor authentication. Host ID authentication can be completed in less than 5 seconds while fingerprint authentication may take the same time.

In accordance with embodiments of the invention the portable device is a portable data storage device that has to be loaded with an organization's Computer IDs before it is deployed in its organization. That is, the information security officer compiles a list of computer IDs, let say in Microsoft Excel.

The list of Computer IDs is then stored into the portable data storage device of the current invention before the portable data storage device is given to an employee of the organization. This list of Computer IDs specify all the computers in which this portable data storage device can work. The list of Computer IDs can be stored
within the portable data storage device's storage component, such as NAND Flash, EEPROM and processor's Flash program memory.

For example, a processor may have a flash ROM size of 64Kbytes. 32Kbytes may be allocated to program codes while the other 32Kbytes may be used to store Computer IDs. Typically the Computer IDs are stored in encrypted form. This is the preferred method of storage as it is more secure. In addition, storing the Computer IDs within the processor the access speed to the storage data is faster too. In the device of the current invention, the list of computer IDs can only be stored within the processor and there is no programming command allowed to retrieve any of Computer IDs from the processor storage.

Storage components such as NAND Flash and EEPROM that are external to processor are usually much cheaper in cost and can be used to store the list of Computer IDs. However, they are slower and less secure as it can be potentially accessed by removing the storage components from the device.

In addition, all computers within the organization shall install a software driver. The software driver will send the Computer ID of the current PC to the portable data storage device of the current invention when it is found to be attached to the computer's USB port.

When the device of the present invention is attached to the USB port of a computer which is without driver installed, the device will not receive any Computer ID from the computer. Therefore, the device shall set a timeout for authentication. The current method of Computer ID authentication is failed if the Computer ID is not sent within a defined time frame.

When the device of the present invention is attached to the USB port of a computer with the proper driver installed, the device will be found by the driver, and the driver will send the Computer ID to the device for authentication. When the Computer ID is send, then this Computer ID will be compared with the list of Computer IDs stored within the device of the current invention. If the host Computer ID is found in the list,
then authentication is considered as pass or valid and the portable data store device is enabled to be used with the computer.

This scheme of authentication is unlike any other prior art authentication available in the market place for portable data storage device.

Prior art authentication methods such as password authentication allow the portable data storage device to be used in any PC as long as the PC is installed with the proper driver and if the entered Password is correct.

Most of the portable biometrics data storage have its fingerprint template stored within the device. Most of such devices in the market require a driver to be installed in the user's PC. The user can access the portable data storage device as long as they have the driver software installed and have the correct fingerprint biometrics authentication in any PC.

One objective of current method of authentication is to limit the use of portable data storage device to in an organization or to selected other computers that are allowed by the organization's information security office. That means, even if they install driver software in any other PC, the portable data storage device will not be functional as the current Computer ID is not one of the Computer IDs, stored within the portable data storage device.

Another objective of current method of authentication is to add another factor of authentication to the portable data storage device so that it is more secure.

The current method of authentication is also applicable to portable security tokens which consists of cryptographic processor and storage components such as EEPROM, or internal flash ROM.

The current method of authentication is also applicable to Smart Card as well. A smart card consists of storage component and cryptographic functionality. The Computer IDs can be stored within a Smart Card by the administrator. In this case, the Smart Card can be used only in designated Computers.
The current method of authentication requires 3 components to operate namely – a software driver, an administrator software and a device, described in the current invention, which includes storage components that store a list of Computer IDs.

The software driver that is installed on a computer (PC), is constantly looking if the device, described in the present invention, is attached to PC. If it is so, the computer ID of current PC will be sent to the device for authentication.

The administrator software is used to retrieve the computer IDs from a file and store the computer IDs into the device of the present invention. A scheme has to be developed to prevent the unauthorized use of the administrator software by any user. For example, administrator software may require a password, known only to the administrator, before it can be executed. The administrator software may be used only if the administrator is authenticated by an external portable device like a smart card or a personal biometrics portable device after authenticated by his fingerprint and PIN. In this case, the administration software will verify the authentication hardware (e.g. serial number) before it operates.

The invention provides a portable electronic device as claimed in the independent claims. Embodiments of the invention are given in the dependent claims.

In the present invention, the fingerprint sensor is used to detect the presence of a finger and the timing and duration of its presence. Indicators, like LEDs, are used to provide a feedback to the user e.g. to indicate the required time and duration for an entry. The mechanisms of a PIN input for both, a tactile switch and a finger detection appear similar. However, the finger detection is much more secure as it depends on detection algorithms to detect a finger instead of a low/high signal PIN input from a tactile switch. In addition, the biometrics fingerprint sensor is much easier to use and more robust, since it does not use any moving parts compared to tactile switches.
The device described in current invention comprises a cryptographic processing unit, a USB mass storage unit and an identity processing unit. The cryptographic processing unit which has a built in non-volatile memory also interfaces an external non-volatile memory and a smart card. The cryptographic processing unit can also function as a smart card reader.

Alternately, the cryptographic processor of the cryptographic processing unit of this present invention, which has both external and built-in non-volatile memory, can function as a combination of a smart card reader and smart card on board. That allows the cryptographic processor to generate encrypted digital personal keys.

The cryptographic processor communicates with a PC host via the mass storage processor by encrypted embedded commands. Both, PC host and the cryptographic processor, must have the same encryption key for communication. In addition, an exchange of private authentication keys has to take place between the cryptographic processor and PC host prior to any command or data communication. The cryptographic processor will stop functioning if it receives any invalid command from a PC host. Any invalid command or any hidden hacking activities from a PC will be recorded in the cryptographic processor built-in non-volatile memory for future retrieval. The device has then to be unplugged from the USB port in order to reset the cryptographic processor. The identity processing unit comprises an identity processor and identity scanner. In the context of RFID and wireless smart card, the identity scanner is an antenna. In the case of biometrics identity, the identity scanner is a biometric sensor.

An identity processor is an integrated circuit for storing and processing information, modulating and demodulating a Radio Frequency or biometrics information. The identity information which includes, but is not limited to, RFID, wireless smart card and biometrics information has to be enrolled prior to the use of the device. The identity parameter generated is then stored within the device for later authentication.

The mass storage unit consists of a mass storage processor and a plurality of mass storage media. The mass storage processor is tagged with a unique serial number as part of Universal Serial Bus information. The mass storage processor of the pre-
sent invention includes an on-the-fly hardware encryption/decryption unit which encrypts mass storage data prior to storing and decrypts mass storage data after retrieving it from a mass storage unit. The mass storage unit will appear to be as a removable disk to a PC host. Mass storage is referred to as storage of large amounts of information. Storage media for mass storage includes, but is not limited to, hard disks and flash memory. In the present invention, NAND flash memory is used.

Embodiments of the invention provide a method of a secure PIN (Personal Identification Number) entry and operation mode setting by using a fingerprint sensor integrated in a portable device, which comprises at least a fingerprint biometrics processing unit. The fingerprint biometrics processing unit retrieves first data from outside the device, performs signal processing, and authenticates the retrieved signal against identity parameters stored within the device, independent from a PC host.

The result of the authentication is used to enable secured portable device functions e.g. flash memory, security token, smart card etc. In the present invention, the fingerprint sensor is not only used to sense the fingerprint image but also to detect whether an object or finger is present or absent. The finger detection together with the detection time and duration or together with the direction of a movement of finger on the sensor defines a method of a secure entry of first data like a PIN and operation mode setting. It further describes a portable device that comprises an identity processing unit, a cryptographic processing unit and a mass storage unit. The identity processing unit in this invention authenticates the owner of the device. The identity processing unit can be a biometrics processing unit, a radio frequency identity reader (RFID) or a wireless smart card reader. The identity processing unit retrieves the identification signal, external to the device, performs signal processing, and authenticates the signal retrieved against identity parameters stored within the device independent from a PC Host. The cryptographic processing unit is used to read a smart card which enables seamless integration into Public Key Infrastructure (PKI) architectures and stores users' personal certificate credentials, such as private keys, passwords and digital certificate. Unlike other smart card systems which are accessed by entering a Personal Identification Number (PIN) in the personal computer, the identity processing unit is used to enable secure access to the smart card, once authenticated, by releasing the PIN without going through a PC. The PIN
number is securely embedded within the device and cannot be accessed by any PC. In addition, the cryptographic processor can generate one time passwords and enables the security token by an authenticated identity entry. The access to the mass storage device in that second data are stored is also protected by the identity authentication. The second data stored within the device is encrypted. The encryption keys are stored within the device. The encryption key is generated in the mass storage processor from two encryption keys that are physically stored in two separate integrated circuits.

In accordance with embodiments of the invention a new and innovative way is provided which removes the use of a USB HUB in order to reduce current consumption and to allow secure communication among the cryptographic processing unit, mass storage processing unit and identity processing unit within the device. In the current invention, an innovative scheme is implemented. That is, only the USB mass storage processor is connected to a USB2.0 bus to a PC host. Communication for both, cryptographic processing unit and identity processing unit to and from PC host, are solely performed via encrypted embedded commands transported within the mass storage processor. Such communication channels are supported by USB Human Interface Device Class and USB Mass Storage Device class commands.

In accordance with embodiments of the invention there is provided a device that enables to have the encrypted embedded commands to be supported by the above communication channels so that a PC can send and receive command and data to and from the cryptographic processing unit and the identity processing unit. In addition, firmware of both, cryptographic processing unit and the identity processing unit, can be upgraded from a host PC.

In accordance with embodiments of the invention there is provided an encryption key alteration mechanism. That allows for modifying the encryption/decryption key for the mass storage unit. Once the key is modified, the mass storage unit has to be formatted by the PC operation systems in order to be used again. In the present invention, the encryption/decryption key, stored within the cryptographic processor,
can be triggered to generate a new random key by the PC utility software when none of the identity parameter is enrolled.

In accordance with embodiments of the invention the invention enables to integrate digital certificates (of the smart card) to identity features of a user.

In accordance with embodiments of the invention there are one time passwords, electronic tokens and other cryptographic functions that can be associated with an enrolled user identity. Such cryptographic algorithm data is released to the host PC via the secure embedded communication channels only after an enrolled user identity is authenticated.

In accordance with embodiments of the invention the device is to function as a multi-factor authentication for secure transactions. The USB processing unit has a serial number as part of USB information; the encrypted embedded commands include an encryption key; an authentication key has to be exchanged between the cryptographic processor and the host PC prior to the start of any encrypted embedded command communication; a digital certificate, a one-time password or a security token are released by one or multiple authenticated identity parameters.

In accordance with embodiments of the invention the advantage is provided to eliminate a user from remembering the PIN number and PASSWORD. Users tend to forget Pins and PASSWORDs. They are having even more problems of resetting PASSWORDs and PINs

**Brief description of the drawings**

In the following embodiment of the invention will be described in greater detail by way of example only making reference to the drawing is which:

- **Figure 1** shows the technical switch circuits and pulses generated;
- **Figure 2** shows a first embodiment of a portable biometrics device;
- **Figure 3** shows an internal building block of a portable biometrics device;
- **Figure 4** shows an example of setting the device in different modes of operation;
- **Figure 5** shows the TOP view of a second embodiment of a device;
Figure 6 shows the bottom view of the second embodiment of a device;
Figure 7 shows the device functional block based on prior art design methodology;
Figure 8 shows the device functional block diagram;
Figure 9 shows the typical device operation flowchart;
Figure 10 shows an example of device operating flowchart;
Figure 11 shows an example of the PIN Bank; and
Figure 12 shows an example of embedded cryptographic commands enabled by
two identity parameters,
Fig. 13 shows a graphical user interface (GUI) of a program for the administra-
tion of CPU IDs and HDD IDs for a portable electronic device.

Detailed description

Figure 2 shows an embodiment of a portable biometrics device according to the
present invention. The device 10 can be connected to a host PC via a communi-
cation interface connector 14. The device includes 3 LEDs as indicators 08 that are
visible and a fingerprint sensor 12 is accessible on the top surface of the device.
The fingerprint sensor 12 can be either a swipe sensor or an areal sensor.

An internal building block of device 10 is shown in Figure 3. It consists of a USB
connector 14, a flash memory 22, LED indicators 08, a fingerprint sensor 12 and a
micro-controller 50. The micro-controller 50 consists of a biometric fingerprint pro-
cessing unit and a USB flash controller unit. Device 10 is a biometric flash disk.

The user's fingerprint and first data respectively is sensed via the fingerprint sensor
12. Once the fingerprint is authenticated against stored identity parameters, the mi-
cro-controller 50 will activate its USB flash controller and the user will be enabled to
access the flash memory 22 storing second data.

The micro-controller 50 can be set into a 'PIN entry mode' to allow the sequential
entry of each PIN digit. When 'PIN entry mode' is detected, the micro-controller 50
within the device 10 will set a digital control parameter for the PIN entry to 0, to indi-
cate that this is the first digit of the PIN entry. The value of the digit is also set to zero.

User guidance is done by LED indicators 08 which consist of a blue LED, a red LED and a green LED. The blue LED indicates that the sensor has sensed the presence of a finger. The green LED indicates an input of a digit entry and indicates also OK when the entered PIN matches with a previously stored PIN, which is referred to as a first data. The red LED indicates that the PIN entered does not match with a previously stored PIN or a PIN entry time has expired.

If the presence of a finger on the sensor is short, let's say less that 1 second, it is considered as an increment of the current digit. If the presence of the finger on the sensor is longer than 1 second, it means that the current digit is complete and will be stored. Then the next digit to be entered is initialized to zero. If the finger is present on the sensor for more than 3 seconds, it means that the PIN entry is complete.

Here is an example of the sequence of entering the PIN and first data respectively 5034 in the PIN entry mode:

1. Briefly touch the sensor 5 times (each time less than 1 second). The blue LED confirms each time that the finger presence has been sensed and therefore, the digit value is incremented by one to a total of 5.

2. Touch the sensor continuously for 1 second to complete the first digit entry. There is a short blink of the green LED to indicate that the digit entry is complete. The blue LED is on to indicate the presence of the finger on the sensor.

3. To enter the next digit, the zero, just touch the sensor for 1 second until the green LED is on in order to complete the second digit entry. (Note: Each new digit is zero by default and for a zero no increment entry is needed)

4. Briefly touch the sensor 3 times. Each digit increment is confirmed by a short blink of the blue LED.

5. Touch the sensor for 1 second to complete the third digit entry. There is a short blink of the green LED to indicate that the digit entry is complete.

6. Briefly touch the sensor 4 times. Each digit increment is confirmed by a short blink of the blue LED.

7. Touch the sensor for 3 seconds to complete the PIN entry. If the PIN
matches, the green LED will be on; otherwise, the red LED will be briefly on.

In another method, a PIN entry can be realized by sensing a movement of a finger relative to the fingerprint sensor. For example, a movement of the finger from the left to the right relative to the fingerprint sensor is considered as an increment of a current digit. If the finger is moved relative to the fingerprint sensor from the right to the left on the sensor, it means that the current digit input is complete and will be stored. Each digit entry starts with an initial value of zero.

Here is an example of entering the PIN 5034:

1. Swipe the finger 5 times on the sensor from the left to the right. The blue LED confirms each time that the finger swiping has been sensed and therefore, the digit value is incremented by one to a total of 5.

2. Swipe the finger from the right to the left on the sensor. There is a short blink of the green LED to indicate that the digit entry is complete.

3. To enter the next digit, the zero, just swipe the finger from the right to the left on the sensor, the green LED turns on to indicate that the second digit entry is complete. (Note: Each new digit initial value is zero by default and for a zero there is no increment entry needed)

4. Swipe the finger on the sensor from the left to the right 3 times. Each digit increment is confirmed by a short blink of the blue LED.

5. Swipe the finger on the sensor from the right to the left on the sensor to complete the third digit entry. There is a short blink of the green LED to indicate that the digit entry is complete.

6. Swipe the finger from the left to the right on the sensor 4 times. Each digit increment is confirmed by a short blink of the blue LED.

7. Touch the sensor for 3 seconds to complete the PIN entry. If the PIN matches, then the green LED will be on; otherwise, the red LED will be on briefly.

Instead of the finger, an object like an entry pen could be used.

There are several advantages of using a fingerprint sensor instead of tactile switches. It can be used without a pointing device like a paper clip or a pen to move
the tactile switches. It is more durable as it has no moving parts. It can be sealed much easier to protect it from humidity. Besides PIN entry it allows the entry of other integrated functions or setting modes of operation, like initiating a reset or erasing the flash. Integrating several functions into a personal device allows operating it independent of any operating system of a connected PC. It allows these functions for hardware protection and prevents several known hacking methods which attack PIN entries or the program which is needed on the PC or the authorizing communication with a personal device.

Additionally, sensing a finger allows a 2-factor authentication. In order to enable the device, the user has to provide both, a valid fingerprint AND a valid PIN entry, by using the fingerprint sensor.

An example of how to set integrated functions is shown in Figure 4. It depicts various options for a 2-factor authentication, the re-enrolment of fingerprints and a method of bypassing fingerprint authentication by PIN input can be achieved by simply sensing the absence and presence of a finger by analyzing timing and duration of its presence.

Compared to tactile switches, the described method of using the fingerprint sensor allows to add another layer of security for the PIN entry or the setting of a specific operation mode by distinguishing original images of live fingers from forgeries by using the biometric sensing functionalities of the sensor.

When the portable biometric fingerprint device is inserted into a USB port, the device checks if there is a finger present on the sensor [STEP 49]. If not, it proceeds with the blue LED blinking to invite the user to scan the finger for authentication [STEP 64].

If there is a finger present on the sensor, the blue LED is on until the finger is removed. When the finger is removed and then placed back again on the sensor within 3 seconds [STEP 52 & 54], it confirms to operate in other modes than the normal authentication mode.
A timer, FDTimer, is then started to measure the duration of the presence of the finger and to light up the green LED after the duration of 3 seconds and to light up the red LED when the duration of 8 seconds has been reached [STEP 56].

The blue LED is on as long as the finger is present on the sensor [STEP 58]. When the finger is lifted and the duration was longer than 8 seconds [STEP 60], the user is prompted to enter the PIN in order to enable the secured functions (like access to the flash memory) [STEP 66]. In this mode of operation, the user bypasses the fingerprint authentication. If the finger is present for more than 3 seconds [STEP 62], it will proceed a re-enrolment of the fingerprint [STEP 68]. The user is prompted to authenticate the re-enrolment with a valid fingerprint. Once a valid fingerprint is authenticated, all the fingerprint identity parameters are erased. Alternative, the user has to enter a PIN as the first factor of authentication [STEP 70]. Once the PIN entry is validated, the user will be prompted for the second factor of authentication which is an entry of a valid fingerprint [STEP 64).

Similarly, after the unit has been authenticated by a fingerprint and/or PIN entry, the user can for example:

1. Place the finger on the sensor for 3 seconds continuously and then enter the PIN number to delete the fingerprint identity parameters;
2. Place the finger on the sensor for 6 seconds continuously and then enter the PIN number for bypassing the fingerprint authentication;
3. Place the finger on the sensor for 9 seconds continuously and then enter the PIN number for deleting the fingerprint identity parameters.

Figure 5 shows a top view of a second embodiment of the device 10 according to the present invention. Although the use of a tactile switch 18 can be a disadvantage as described above, it can be used for various functional operations of the device. These include resetting of enrolled identities, entry of the PIN numbers, etc. The device 10 can be connected to the host PC via a communication interface connector 14. In the present invention, a USB plug is being used. The communication interface connector 14 provides a reliable communication connection of the device to host PC and supplies the current to the device for operation. In the drawing, the fingerprint sensor 12 is located on the top surface of the device in order to allow the user easy
an input of the biometric parameters. In the case of a radio frequency antenna, it will be embedded inside the housing without being visible. The LED indicator 08 is used to display the current status of the device. This includes prompting the user to enter biometric parameters via the fingerprint sensor 12, calling for a wireless signal from an RFID transponder or wireless smart card, displaying the PIN entry of the smart card, displaying the read and write status of the mass storage data, displaying the enrolment status of the biometric parameters, etc.

Figure 6 shows the bottom view of the device. A smart card cover 16 enables a user to access the smart card. The smart card cover 16 can be removed so that a user can insert or remove a smart card. The smart card cover 16 can be sealed permanently in case the user would like to have the smart card permanently attached to the device or have the smart card function built into the cryptographic processor. In this case, the device will not have any smart card connector installed.

The device according to the present invention includes an on the fly hardware encryption/decryption unit within the mass storage processor. The encryption keys are physically stored encrypted within the storage area of 2 different integrated circuits. The encryption/decryption engine which is located in a third integrated circuit reads two separately stored encrypted encryption keys, compiles the two keys into one, and then uses the final key for encryption/decryption of second data. This implementation will make hardware hacking almost impossible. In addition, the mass storage area is further secured by special epoxy. This epoxy will prevent the mass storage IC to be removed without being damaged in case of an attempted removal.

Referring to figure 7 and 8 of an embodiment of a device according to the present invention, it consists of a mass storage processor 20 which includes a hardware encryption/decryption engine, a mass storage media unit 22, a USB Plug 14, a tactile switch 18, a LED indicator 08, a cryptographic processor 30, a smart card connector 32, a non-volatile memory 34, an identity processor 40 and an identity scanner 42. The mass storage media unit 22 is a plurality of non-volatile solid state read/write memory.
A computer serial bus such as USB interfaces a host PC with the mass storage processor 20 which is connected to the mass storage media unit 22 and the cryptographic processor 30 within the device. The cryptographic processor 30 is connected to a smart card connector 32, a tactile switch 18, a LED indicator 08, a non-volatile memory 34 and the identity processor 40.

The mass storage processor 20 decodes all PC commands and performs the read/write commands to mass storage processor 20 via it's built in hardware encryption/decryption engine. In addition, it also transfers the encrypted embedded commands to and from the cryptographic processor 30 for the host PC. The cryptographic processor 30 decodes the encrypted embedded commands from a host PC. The decrypted identity embedded commands are sent to the identity processor 40. The cryptographic processor 30 processes the decrypted cryptographic embedded commands accordingly. As the cryptographic processing unit is connected directly to the identity processing unit, all cryptographic functions are securely and closely integrated with the identity functions.

The use of encrypted embedded commands between a host PC and the mass storage processing units eliminates the use of any USB hub to integrate the mass storage processor 20, the identity processing unit and the cryptographic processing unit. This represents a huge saving of power consumption, PCB layout space and cost; all host communication control of the device is performed by the mass storage processing unit 20. The modules are securely integrated and all identity cryptographic functions are performed within the device only.

One of the objectives of the tactile switch 18 is to be used to enter commands to the cryptographic processor 30. In the present invention, the device is set in an identity re-enrolment mode when the tactile switch 18 is pressed while the device is plugged into the USB port. After the device is authenticated against the stored identity parameter, it will erase all stored identity parameters and set the device into re-enrolment mode.

In a normal mode, commands to the cryptographic processor 30 can be activated by asserting the tactile switch 18 continuously for 3 seconds. The command entry is
then set to the first digit and the value of the digit is set to '0'. The LED 08 will display according to subsequent assertions. In the device of the present invention, an assertion of less than 1 second means to increment the current digit by one. An assertion of more than one second but less than 3 seconds means completion of current digit entry and the start of next digit entry and sets the next digit value to '0'. The user has to assert the tactile switch 18 for more than 3 seconds in order to complete the entry of a code. This allows secure entries of configuration data, PINs, etc. without the need of using the device driver utility or any host PC activity.

A typical sequence of an operation of the device is best described in Figure 9. When the device according to the present invention is connected to host PC via connector 14 [STEP 47], the device will power up and initialize [STEP 52]. During the initialization process, the cryptographic processor 30 will check if the tactile switch 18 is asserted. Thereafter, the cryptographic processor 30 will be checking if any identity parameter is enrolled into the device [STEP 54]. If the device had not been enrolled with any identity parameter, the cryptographic processor 30 will check if the communication with the PC host can be established. If the factory configuration data allows communication between the PC host and the device to be established when there is no identity parameter, the device of the present invention can then be accessed by the driver utility software from the host PC for identity enrolment [STEP 56]. The driver utility software on the host PC provides the following functionality:

1. user identity enrolment and authentication training during the initial use of the device;
2. a tool for identity enrolment. The user is guided through the enrolment process by using a PC graphics user interface;
3. entry of PINs for the smart card. A smart card PIN cannot be read but it can be modified;
4. tagging of smart card PINs to enrolled identity parameters;
5. tagging of PC passwords to enrolled identity parameters;
6. tagging of cryptographic functions such as one time passwords and electronic tokens to enrolled identity parameters, and
7. For a security option, it can be used to set that both the identity processor 40 and the cryptographic processor unit 30 are no longer allowed to be accessed by the
driver utility software and the encrypted embedded communication channel is permanently disabled.

Alternative, the configuration data can be set at the factory level. As an example, the device can be set to prevent any communication with the host until all identity parameters are enrolled after it is first plugged-in. In this case, the user has to enroll the identity [STEP 56] without the assistant of the driver utility software but guided by LED 08 and can be controlled by the tactile switch. In this way, the device is completely self-contained without allowing any access from any host PC.

Once all the identity parameters are enrolled, the mass storage processor 20 will retrieve the first and the second encrypted encryption key from the mass storage media unit 22 and cryptographic processor 30 respectively. The final encryption/decryption key is then generated via a proprietary computation method from the two encryption keys [STEP 66].

Once the device has been enrolled [STEP 54], a user has to be authenticated. The LED 08 will prompt the user to present his/her identity in the form of biometrics, RFID or wireless smart card [STEP 58] to the device. The retrieved identity is then authenticated against the stored identity parameters [STEP 60]. In the device of the present invention, the user is allowed to have a predefined maximum (of 3) authentication attempts within 60 seconds from the time the device is plugged in. The device will be shut down if the predefined number of attempts failed or more than 60 seconds have expired.

Once a user is authenticated, the cryptographic processor will check if any identity re-enrolment request [STEP 62] is made. In the present invention, the identity re-enrolment request is made when tactile switch 18 is asserted during device initialization [STEP 52]. If the re-enrolment request is made, then the current identity parameters are erased [STEP 64] and the device will proceed to identity enrolment [STEP 56].

After identity enrolment is completed [STEP 56], the encryption key is generated [STEP 66] and the enumeration of communication channel with the PC host will be
started [STEP 68]. The device will appear in a host PC as a removable disk. In the
device of the current invention, a vendor specific SCSI (Small Computer System
Interface) command is used to provide a communication channel between the host
PC and the cryptographic processor 30. The mass storage, cryptographic and iden-
tity function can then be accessed by the PC host. Access by the host PC to the
cryptographic processor 30 and identity processor 40 is supported by the encrypted
embedded commands. The cryptographic processing unit will recognize the en-
crypted embedded commands of the same encryption key. In addition, a valid au-
thentication code has to be sent from the host PC to the cryptographic processor 30
in order to start the communication process. In the device of the present invention,
the cryptographic processing unit allows up to two host PC attempts of sending a
valid authentication code.

The device will check continuously for any mass storage processing command
[STEP 70], embedded cryptographic command [STEP 74] or embedded identity
command [STEP 92].

If the embedded cryptographic command is received [STEP 92], the cryptographic
processing unit will check if the host PC is asking for a password [STEP 82]. If this
is the case, the user identity is authenticated [STEP 84 & STEP 86] prior to the
password associated with the identity parameter before it is released to the host PC
[STEP 88] from the identity processing unit. Otherwise, the identity processing unit
will process the identity command accordingly [STEP 90]. Should the command re-
quire authentication of a user, then LED 08 will blink to prompt the user to enter
his/her identity.

If the command is meant for the mass storage unit, the mass storage will process
the command and data accordingly. This includes decrypting of mass storage data
from the media storage unit 22 before sending it to the host PC and encrypting of
any second data in the mass storage before writing into the mass storage media
unit 22 [STEP 72].

If the embedded cryptographic command is received [STEP 74], typically a user
identity needs to be authenticated [STEP 76 & STEP 78] before a PIN is entered
into a smart card or the identity PIN is used to enable a cryptographic algorithm
[STEP 80]. This includes, but is not limited to, releasing of digital certificates or keys,
security tokens, or one time passwords. Alternatively, for a specific cryptographic
function, the user may be asked to authenticate against 2 or more different identity
parameters prior to enabling the cryptographic function.

Figure 10 shows an example of identity parameters tagged with PIN and Password.
PINs are associated with smartcards and other cryptographic functions and pass-
words are associated with PC applications.

Both, the PIN bank and password bank in the device of the present invention are
stored within the non-volatile memory of the identity processor 40. However, it can
also be stored within the non-volatile memory of cryptographic processor 30 and the
external non-volatile memory 34. Alternatively, it can also be stored in the remov-
able smart card.

The device in the current invention is able to offer multiple PINs for multiple smart
cards or multiple PINs for a single smart card. Therefore the device is flexible
enough to be used for multiple smart cards. The device is built-in with a write only
PIN bank. This PIN bank will store a limited number of PINs for various smart cards
used within the device. In the current invention, the PIN bank is limited to 16 PINs
and the user can select which PIN to be used with the inserted smart card. The
driver utility software can be used to activate the desired PIN to be used.

The device in the current invention can also be configured in such a way that differ-
ent identity parameters can be associated with different PINs. Such associations are
possible after all identities are enrolled in the device. In this case the driver utility
software will be used to configure different PINs to be associated with different iden-
tities.

Figure 11 shows an example of a PIN bank. An example of the device of the present
invention allows up to 16 PINs and 16 passwords to be stored. Each identity pa-
rameter enrolled can be tagged with a PIN and a password. Each PIN and each
password can be of any number of digits; it can be up to 16-digits in length in the
example of the present invention. In addition, the descriptor to each PIN or pass-
word can be up to 32 characters long.

Figure 12 shows an example of an embedded cryptographic command enabled by
two identity parameters. ID1 and ID2 indicate the identity parameters to be authenti-
cated before the embedded cryptographic command will be processed. CRC is a
type of hash function used to produce a checksum, in order to detect errors in com-
mand or data transmission.

Fig. 13 shows a graphical user interface (GUI) of a program for the administration of
CPU IDs and HDD IDs for a portable electronic device according to the present in-
vention. A list of CPU IDs and HDD IDs which are stored in a file "IDS2.xls" are im-
ported into the program by clicking "IMPORT". By clicking "Program IDs", the list of
computer unique identifiers is stored into the portable device.

Embodiments of the present invention include, among others, in particular:

1. Personal portable devices, which include a secure smart card reader, whereby
the PINs for the smart cards in the device and functions are enabled by a fingerprint
authentication and/or a PIN.

2. Personal portable devices, as described above which include a secure smart card
reader and a flash memory. The Smart Card is enabled by an input of a PIN and a
first signal respectively. The PIN refers to the identity parameter of a specific user.
PIN and identity parameters are both securely stored within the device. The PIN is
released to the smart card reader only with the proper authentication of the stored
identity parameters of the user. To enhance higher security, secure second data
from the smart card may be only accessed when 2 or more identity parameters are
presented.

3. Personal portable devices, as described above, which include a RFID trans-
ponder, whereby different transponder functions are enabled by using the sensor.
4. Personal portable devices, as described above which include a fast en- and de-
cryption processor to en-/decrypt data on the fly whereby the encryption key is ei-
ther generated using the fingerprint parameters or the PIN-entry or both and
whereby the authentication process to enable the en-/decryption functions is en-
abled only after a successful authentication by fingerprints and/or PINs. Specific
considerations include the secure storage of the encryption key that it can not be
retrieved easily by analyzing the hardware. Parts of the key are stored encrypted in
several different hardware locations in the device. Only after a successful authenti-
cation, the encryption key is generated. The key can be completely modified by us-
ing the function setting options. For high security tokens, it is mandatory that the key
never leaves the unit and can not be retrieved.

5. Personal portable devices, as described above, whereby a PIN number is stored
in the device in 2 different ways. One is during the initialization process of a smart
card: the device generates a random PIN for the smart card. The PIN is then stored
within the device. In another scenario, a smart card comes with a PIN number. The
user can either enter this PIN via a driver utility of the device at a host PC or by en-
tering the PIN number through a tactile switch of the device. The device driver utility
allows the new PIN number to be entered only after both are authenticated, the de-
vice and the user. The user needs a special password to enter the new PIN. The
PIN number cannot be read out from the device and therefore it is far more secure
than current implementations: the PIN is not displayed or subjected to be stolen by
any keystroke logger.

6. Personal portable devices which are used as a token to unlock a PC or any other
specific electronically locked unit. After authenticating the user by fingerprint and/or
PIN in the portable device, the device becomes "visible" to the unit to be unlocked
and parameters like a serial number, MAC-address, pass-phrase, PIN or key may
be transmitted.

7. Personal portable devices which include parts or all of the above and additional
electronic functions to be protected like a cellular phone, a car key or a subscription
module.
Although the invention has been described with reference to particular embodiments, the description is only an example of the invention's application and should not be taken as a limitation. Consequently, various adaptations and combinations of features of the embodiments disclosed are within the scope of the invention as
Claims

1. A portable electronic device comprising:
   means for fingerprint user authentication having a fingerprint sensor (12);
   means for entering first data;
   wherein
   said means for entering said first data being coupled to the fingerprint sensor (12),
   said first data being entered by sensing a presence of an object relative to the fingerprint sensor (12),
   the first data being independent of biometric characteristics of the object.

2. The portable electronic device of claim 1, wherein said fingerprint sensor is further adapted to sense a movement of the object relative to the fingerprint sensor and wherein the first data is entered by sensing the movement.

3. The portable electronic device of claim 1 or 2, wherein said fingerprint sensor is further adapted to sense a timing of the presence of the object relative to the fingerprint sensor and wherein the first data is entered by sensing the movement.

4. The portable electronic device of claim 1, 2 or 3, being adapted to distinguish original images of live fingers from forgeries by using the biometric sensing features functionalities of the sensor.

5. The portable electronic device of any one of the preceding claims, wherein
   said first data is a user authentication PIN.

6. The portable electronic device of any one of the preceding claims, being adapted to perform a plurality of modes of operation and further comprising means for selecting one of the modes of operation depending on the first data.
via the fingerprint sensor.

7. The portable electronic device of any one of the preceding claims, further comprising
- memory for storing encrypted second data;
- means for encryption and decryption of the second data being operable to encrypt the second data when a storage operation for storing the second data in the memory is executed and being operable to decrypt the second data when a read operation for reading the second data from the memory is executed, wherein at least one of the read operations or the write operations is enabled after user authentication has been executed successfully.

8. The portable electronic device of any one of the preceding claims, further comprising a smart card (IC) reader wherein the first data is a PIN that is assigned to a smart card for accessing the smart card.

9. The portable electronic device of any one of the preceding claims, further comprising a smart card reader, whereby a PIN for a smart card in the card reader and/or functions for the smart card being enabled by one of the following: PIN, fingerprint or PIN AND fingerprint.

10. The portable electronic device of any one of the preceding claims, further comprising a RFID transponder wherein the fingerprint sensor is further adapted to enable transponder functions.

11. The portable electronic device of any one of the preceding claims, whereby single parts of an encryption key being stored in different hardware locations and whereby the encryption key is compiled in response to a successful user authentication.

12. The portable electronic device of claim 8, being adapted to unlock the smart card via the smart card reader using the PIN after a user authentication has been executed successfully.
13. A portable electronic device which comprises at least a fingerprint biometrics processing unit whereby a fingerprint sensor is not only used to retrieve a user fingerprint image but is also used to detect a presence and absence of a finger and also a direction of movement of the finger.

14. The portable electronic device of claim 13 of said portable device together with a timing and sequence of detection of a presence and absence of a finger on the surface of the fingerprint sensor or together with the direction of movement of the finger, are used for a PIN input into said device.

15. The portable electronic device of claim 13 using a timing and sequence of detection of a presence and absence of a finger on the surface of the fingerprint sensor for enabling different modes of operations of said device, specifically enabling specific secured operations.

16. The portable electronic device of any one of the preceding claims, being embedded and/or integrated into other electronic devices like notebooks, smart card readers, phones, cameras, desktop boxes, TV-sets, cars etc. for securing specific functions and to allow an independence from an operating system or a bus structure.

17. The portable electronic device of any one of the preceding claims using the fingerprint sensor for adding another layer of security for the PIN entry or setting of a specific operation mode checking if a real finger is present before or when commands/PINs are entered, using biometric sensing features and functionalities of the fingerprint sensor.

18. The portable electronic device of any one of the preceding claims, including a secure class 2 smart card reader, whereby the PINs for the smart cards in the device and functions are enabled by a fingerprint authentication and/or a PIN.

19. The portable electronic device of any one of the preceding claims, which includes a flash memory which is enabled only after a successful user
authentication by fingerprint and/or PIN.

20. The portable electronic device of any one of the preceding claims, which includes RFID transponder(s) where different transponder functions are enabled using the fingerprint sensor.

21. The portable electronic device of any one of the preceding claims which includes a fast en- and decryption processor to en-/decrypt data on the fly whereby an encryption key is either generated using the fingerprint parameters or the PIN-entry or both and whereby an authentication process to enable the en-/decryption functions is enabled only after a successful user authentication by fingerprints and or PINs.

22. The portable electronic device of claim 21 whereby the encryption keys are securely stored in parts in different locations of the hardware in the device and only compiled after a successful user authentication by fingerprint and/or PIN.

23. The portable electronic device of claim 21 or 22 where the encryption key can be completely modified using function setting options.

24. The portable electronic device of any one of the preceding claims which is used as a token to unlock a PC or any other specific electronically locked unit.

25. The personal portable device of any one of the preceding claims which only becomes “visible” to a connected device after a successful user authentication by fingerprint(s) and/or PIN in the portable device, and then is allowed to receive the transmission of parameters like a serial number, MAC-address, or pass-phrase.

26. The personal portable device of any one of the preceding claims which becomes temporary “visible”, for a predetermined time duration, such as a few seconds, only, to a connected device, such as an external computer, during authentication by fingerprint(s) and/or PIN in the portable device, and concurrently allows to receive the transmission of parameters like a serial
number, HDD ID, CPU ID, or pass-phrase for additional factor authentication.

27. The portable electronic device according of any one of the preceding claims protection additional electronic functions of a cellular phone, a car key or a subscription module.

28. The portable electronic device of any one of the preceding claims wherein
one or more unique identifiers are stored in the portable device, the identifier being assigned to an external computer, the portable device having an interface for coupling to an interface of the external computer, such as an USB interface, the portable device being operable to receive an computer identifier from the external computer when the portable device is coupled to the external computer via the interface, to compare the computer identifier received from the computer with the unique identifier, and to grant access to the computer for use of at least one of its functions, such as access to its mass storage, if the received computer identifier and the unique identifier are matching.

29. The portable electronic device according to claim 28, a two factor authentication being required as a further precondition for granting of access to the at least one function of the portable device to the computer, wherein the two factor authentication can require fingerprint authentication and entry of a PIN via the fingerprint sensor as first data.

30. A method of PIN entry using the portable electronic device according of any one of the preceding claims wherein the fingerprint user authentication is performed for a two factor authentication.
Figure 1  Tactile Switch circuits and Pulses Generated

Figure 2  A Portable Biometrics Device

Figure 3  Internal building block of a Portable Biometrics Device
Figure 4 Example of setting the device in different modes of operation
Figure 5 Device TOP view

Figure 6 Device BOTTOM view

Figure 7 Device Block Diagram Typical Implementation
Figure 8 Device Block Diagram
Figure 9  Device Operating Flowchart
<table>
<thead>
<tr>
<th>PIN Bank No</th>
<th>Password Bank No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Parameter 1</td>
<td></td>
</tr>
<tr>
<td>Identity Parameter 2</td>
<td></td>
</tr>
<tr>
<td>Identity Parameter 3</td>
<td></td>
</tr>
<tr>
<td>Identity Parameter 4</td>
<td></td>
</tr>
<tr>
<td>Identity Parameter 5</td>
<td></td>
</tr>
</tbody>
</table>

Figure 10 Example of identity parameters tagged with PIN and Password, as displayed in the device driver utility program.

<table>
<thead>
<tr>
<th>PIN No</th>
<th>Bank</th>
<th>PIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>*****</td>
<td>Bank A Card A PIN A</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>*********</td>
<td>Bank A Card A PIN B</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>*****</td>
<td>Bank B</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>*********</td>
<td>Company C Card C</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 11 Example of the PIN Bank.

**Figure 12** Example of an embedded cryptographic command enabled by two identity parameters.
Fig. 13 Example of a graphical user interface (GUI) of a program for the administration of CPU IDs and HDD IDs for a portable electronic device.
**INTERNATIONAL SEARCH REPORT**

**INTERNATIONAL APPLICATION NO**

PCT/EP2009/000632

---

**A. CLASSIFICATION OF SUBJECT MATTER**

INV. G06F21/20

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 database consulted during the international search (name of database and, where practical, search terms used)

EPO-Internal

---

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Australia</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iolock-Fingerprint-Scanner-Standalone-Installation.pdf&gt; [retrieved on 2009-04-22]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the whole document</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0008] - paragraph [0011]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>paragraph [0030] - paragraph [0131]</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>WO 00/42491 A (RAINBOW TECHNOLOGIES INC [US]) 20 July 2000 (2000-07-20)</td>
<td>1-30</td>
</tr>
<tr>
<td></td>
<td>page 9, line 1 - page 39, line 3</td>
<td></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 document published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

---

**Date of the actual completion of the international search**: 22 April 2009

**Date of mailing of the international search report**: 12/05/2009

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

Pinto, Raúl
<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>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2007035469 A2</td>
</tr>
<tr>
<td>WO 0042491 A</td>
<td>20-07-2000</td>
<td>AU 2608200 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2002535746 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 7272723 B1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2001043702 A1</td>
</tr>
<tr>
<td>EP 1580697 A</td>
<td>28-09-2005</td>
<td>CN 1673946 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20050094223 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2005207626 A1</td>
</tr>
<tr>
<td>US 6509847 B1</td>
<td>21-01-2003</td>
<td>NONE</td>
</tr>
</tbody>
</table>