A security-protected portable medium for digital data and a security protection method using said data medium.

The present invention relates to security-protected portable media for digital data and the security procedures applied when using such data media.

More specifically, the invention relates to a security-protected digital data medium which can be read by an electronic user device having at least one input interface, this data medium being designed to be subjected to at least a predetermined movement imposed by the electronic user device when reading said data medium, said data medium having an electronic security device comprising :

- a receiving interface for receiving input data from the electronic user device,
- a transmission interface designed to transmit output data depending on the input data received, the output data corresponding (directly or indirectly) to a security code to be communicated to the input interface of the electronic user device,
- and a central electronic unit connected to the receiving and transmitting interfaces and programmed so as to determine the output data on the basis of the input data and to transmit said output data via the transmission interface.

Document US-A-5 652 838 describes an example of a security-protected, portable digital data medium of this type which, in this case, is an optical disc. The input interface consists of optical sensors set up to detect a reader laser beam in a computer using the optical disc, this laser beam being controlled so that the sequence in

which it passes across the optical sensors corresponds to a certain input code. The output interface of the optical disc consists of a screen which displays an output code based on the input code received by the computer. The user must remove the optical disc from its reader in order to read the output code, after which said user types in this code from the keyboard of his computer, which authorises the computer to use the optical disc. This prevents unauthorised copying of the disc.

The disadvantage of these procedures is that the reading beam has to be directed at the optical sensors of the data medium, which means that the optical sensors have to be positioned in the data storage zone of the data medium and this imposes constraints in terms of the data layout in said data storage zone and places limits on the storage capacity of said data storage zone.

The objective of this invention is to overcome these disadvantages.

To this end, the invention proposes a security-protected, portable digital data medium of the type outlined above which is characterised in that the receiving interface of said data medium has a motion sensor designed to detect movements of the data medium, the central unit of the data medium being set up to determine the input data on the basis of movements of the data medium detected over a period of time.

In preferred embodiments of the data medium proposed by the invention, one and/or the other of the following features may also be incorporated :

- the central unit is designed to determine the input data by detecting and/or by not detecting movement of the data medium over a period of time;

- the data medium is designed to be subjected to several predetermined movements imposed by the electronic user device when said data medium is being read, the central unit of the data medium being set up to determine the input data on the basis of said predetermined several movements of the data medium detected over time (these features may be used independently of the features outlined above and in particular regardless of whether the output interface is provided in the form of an acoustic transducer);

- the motion sensor is an acceleration sensor ;

- the data medium is designed to be rotated by the electronic user device at at least one predetermined speed whilst it is being read, the motion sensor being a radial acceleration sensor designed to detect rotation of the data medium at said at least one predetermined speed ;

- the motion sensor is a current micro-generator which is designed to generate an electric current when the data medium is in motion and which supplies the security-protection device at least partially with electrical energy;

- the central unit is designed to shut down if the motion sensor detects a movement of said data medium which does not correspond to certain predetermined criteria in keeping with normal use;

- the central unit is designed to shut down if the motion sensor detects a continuous motion over at least one predetermined period;

- the transmission interface has an acoustic transducer which transmits output data in the form of an acoustic signal (this feature may be used independently of

the above-mentioned input interface incorporating a motion sensor) ;

- the central unit of the data medium is set up so that the acoustic signal from the transducer is issued in the form of a series of sound signals of varying duration separated from one another by periods of silence of a predetermined duration, the output data being coded by the varying duration of the different sound signals;

- the central unit of the data medium is set up so that the acoustic signal from the transducer is emitted in the form of several streams of sound signals, each comprising several elementary sound signals of a constant duration, the number of elementary sound signals in each stream of sound signals being between 1 and a whole number n at least equal to 2, the streams of sound signals being separated from one another by periods of silence equal to at least one predetermined duration, and the output data being coded by the number of elementary sound signals in each stream of sound signals ;

- the transducer is an electronic buzzer which issues an acoustic signal having a constant spectrum of transmission frequencies;

- the transducer is a loudspeaker connected to voice synthesising means, the central unit of the data medium being set up to command the loudspeaker to transmit a sound message comprehensible to a human operator and containing the output data;

- the data medium is an optical disc.

It should be pointed out that in replacement of said input interface incorporating a motion sensor, one and/or the other of the following features may be incorporated if necessary :

- the data medium can be read by an electromagnetic beam (in particular a light beam) which locally heats said data medium as it is being read, the receiving interface having at least one thermoelectric element exhibiting at least one electric characteristic which varies depending on its temperature, this thermoelectric element being connected (directly or indirectly) to the central unit of the data medium, and the data unit being set up to detect passes of the electromagnetic beam across the thermoelectric element on the basis of variations in said electric characteristic and to determine the input data on the basis of these passes detected over time (if necessary, these features could be used independently of the features described above and in particular regardless of whether the transmission interface is provided in the form of an acoustic transducer);

- the thermoelectric element is designed to generate an electric voltage when heated by the electromagnetic beam, this electric voltage constituting said electric characteristic ;

- the thermoelectric element has a PZT base.

Another object of the invention is to provide a security protection method using a data medium of the type defined above, comprising the following steps whereby:

- the data medium is read in a reader belonging to an electronic user device which has an input interface,

- the electronic user device transmits the input data to the receiving interface of the data medium,

- the central unit of the data medium determines the output data on the basis of the input data,

- the transducer of the data medium emits the output data in the form of an acoustic signal,

- the security code corresponding to the output data is communicated to the electronic user device via the input interface of said electronic user device,

- depending on the security code received by the electronic user device, a certain mode of operation will or will not be authorised by said electronic user device.

In preferred embodiments of the method proposed by the invention, one and/or the other of the following features may be incorporated:

- a human operator listens to the output data contained in the acoustic signal and this operator determines the security code on the basis of the signal heard and communicates this security code to the electronic user device from the input interface;

- the acoustic signal containing the output data is received by the input interface of the electronic user device directly;

- the acoustic signal containing the output data is transmitted to a remote control station which determines the security code on the basis of said acoustic signal and transmits this security code or not to the input interface of the electronic user device.

Another object of the invention is a method using a data medium as outlined above, this method involving an exchange of coded data between a remote central station and the central unit of the data medium via the receiving interface and the receiving system of said data medium.

Accordingly, the user can be identified by means of the coded data exchanged between the remote central station and the central unit of the data medium in order to protect a remote transaction, for example a remote payment transaction.

The invention also relates to a method using a security-protected data medium of the type outlined above, in which method the electronic security device contains in its memory a count of units of value and said central unit of said security device is programmed to vary said unit count on the basis of coded data received and transmitted by the central unit via the receiving and transmission interfaces.

The invention also relates to a method using a security-protected data medium of the type defined above, in which method the electronic security device contains in its memory at least one user unit counter and the central unit of said security device is programmed to vary said counter on the basis of the movements of the data medium detected by the motion sensors.

Advantageously, the user unit counter can be read by an external reader by means of a communication interface belonging to said security device.

Other features and advantages of the invention will become clear from the following description of several of its embodiments, given by way of example and not restrictive in any respect, and with reference to the appended drawings.

Of the drawings:

- figure 1 is a schematic view of a microcomputer which is capable of using an optical disc of the type proposed by the invention, having an electronic security circuit,

- figure 2 is a block diagram showing a first embodiment of the electronic security circuit of the optical disc illustrated in figure 1, proposed by the invention,

- figures 3 and 4 are views similar to that of figure 2, illustrating second and third embodiments of the invention respectively,

- and figure 5 is a schematic view of a thermoelectric element which may be used with the embodiment illustrated in figure 4.

The same reference numbers are used in the different drawings to denote the same or similar elements.

Figure 1 shows a micro-computer 1 comprising a screen 1a, a keyboard 1b and a reader 2 for digital optical discs (CD-ROM, DVD, etc.) or other digital data media.

The specific purpose of the invention is to provide security protection for the use of the optical disc 3 or any other similar digital data medium which may be used with the micro-computer or with another electronic device, in order to prevent unauthorised copying of this optical disc (or other data medium).

To this end, the optical disc 3 (or other similar data medium) has an electronic security circuit 6, preferably outside its data storage zone 4 and advantageously in its central part 5 which does not contain data.

This electronic security circuit, which is illustrated in figure 2, is integrated in the resin matrix of the optical disc and comprises :

- a central electronic unit 7 such as a micro-controller or a micro-processor connected to a memory 8 which may be internal to said micro-controller or micro-processor (a micro-controller such as the P8WE5032 sold by PHILIPS SEMICONDUCTORS, a division of PHILIPS ELECTRONICS, Eindhoven, NETHERLANDS, might be used, for example, or alternatively the AT89SC micro-controller sold by ATMEL CORPORATION, 2325 Orchard Parkway, San Jose, CA 95131, USA),

- an electric power source 9 such as a miniaturised battery (for example a battery such as that sold under the TMF® brand by BOLDER TECHNOLOGIES CORPORATION, 4403 Table Mountain Drive, Golden, Colorado (CO) 80403, USA), which supplies the electronic circuit 6,

- a motion sensor 10 such as an acceleration sensor, designed to detect ortho-radial (tangential) acceleration of the optical disc, for example, or preferably a radial acceleration corresponding to the rotation speed of the optical disc 3 as it is being read in the reader 2 of the micro-computer (this sensor 10 is used to transmit data from the micro-computer to the optical disc 3 and, advantageously, also as a means of issuing commands to activate and shut down the central unit 7 depending on whether the optical disc 3 is being used),

- and an acoustic transducer, preferably a piezoelectric transducer such as a loudspeaker or an electronic buzzer 11, controlled by the central unit 7 and issuing sound signals having a constant frequency spectrum, for example.

The acceleration sensor 10 may be a micro-sensor, for example (having a surface area of 2 mm by 2 mm for example), produced by micro-machining on silicon, such as the 2g and 50g sensors made by Laboratoire d'Electronique, de Technologie et d'Instrumentation (LETI) of the CEA (ATOMIC ENERGY COMMISSION), FRANCE.

The device described above is capable of running a security protection procedure that will be able to check whether the optical disc 3 inserted is an original corresponding to a certain application (programme, data base, etc.) used when this application was initially installed on the micro-computer 1, for example.

To this end, when the micro-computer 1 is running the installation programme of the application in question, this programme will generate input data such as a first random code which is transmitted by the micro-computer 1 to the optical disc 3.

In the example illustrated here, this input data may be coded in the form of a stop and go sequence of the optical disc reader 2, the input being coded by varying the duration of go periods and/or stop periods of the disc.

For example, this stop and go sequence may start with a predetermined fixed series of stop and go periods which alerts the central unit 7 to the transmission of a message containing input data and which enables this central unit to synchronise with a predetermined time frame, each period of which contains a data bit. After this predetermined fixed series of stop and go periods, the stop and go sequence contains the input data in which the input data bit for each period of the time frame will be equal to 1 if the disc is moving and 0 if it is stationary, for example.

The sensor 10 detects whether the reader 2 is in stop or go mode and transmits the stop/go data to the central unit 7.

This central unit recognises the predetermined stop/go sequence at the start of the coded sequence containing the first random code and determines output data on the basis of the input data: this output data may be in the form of a second pseudo-random code, for example, generated on the basis of a coding key contained in the memory 8 of the central unit.

The central unit then issues output data in the form of an acoustic signal via the transducer 11, preferably without the disc 3 having to be removed from its reader 2.

This acoustic signal may comprise several streams of sound signals (for example 3 to 6 sound signal streams) each comprising several elementary sound signals close to one another (separated from one another by a period of 0.2 s for example) and of constant duration. The number of elementary sound signals in each stream of sound signals is between 1 and a predetermined whole number at least equal to 2 and it may be equal to 4, for example. The streams of sound signals may be separated from one another by periods of silence equal to at least one predetermined duration (for example, these periods of silence may all be equal to approximately 2 s).

The output data is then coded by the number of elementary sound signals in each stream of sound signals.

A human operator listens to the acoustic signal containing the output data and the human operator then determines the above-mentioned second code in the form of a series of digits ranging between 1 and n, corresponding respectively to the numbers of sound signals in the different streams of elementary sound signals emitted in succession by the disc 3.

The operator then communicates a security code based on said second code (in practice constituted by said second code) to the micro-computer 1, from the keyboard 1b, for example. By preference, guiding prompts are given for these operations by one or more messages displayed on a screen of the micro-computer.

If the security code received is linked to the first of the above-mentioned codes by a predetermined equation, the micro-computer 1 will then allow the installation programme to run; if not, it will prevent this programme from running normally.

Correct running of the installation programme may also be controlled as follows:

- by encrypting the data contained in the optical disc 3, it not being possible for this data to be decrypted except with a decryption key which will depend on the above-mentioned security code and the above-mentioned first code,

- or by incorporating in the installation programme or in a programme contained on the optical disc 3 a branch to a programming address, which is intended to be copied to the memory of the micro-computer and which can not be determined except by means of the above-mentioned security code or the abbve-mentioned first code.

The same principles may be used to control not only the one-off installation but also use of the computer application in question, by obliging the user to insert the optical disc 3 in the reader at least when said application is launched.

This being the case, it should be pointed out that it will also be possible to control the terms on which this computer application is used, depending on data contained in the memory 8 of the central unit of the optical disc 3 and to set the system up so that the central unit 7 does not return the above-mentioned second code unless the requisite conditions of use are complied with.

By way of example, the system might be set up to stipulate :

- a maximum number of times or a maximum period of time for which the computer application can be used,

- or alternatively a date from which the computer application will no longer run unless an optical disc 3 is purchased,

- or alternatively a limit on the programme modules or data which the user can access (in this latter case, the above-mentioned security procedure must be repeated every time the user wants to access a new programme module or data).

It should be pointed out that the signal emitted by the transducer 11 could be coded in a different way from that described above, and in particular :

- by emitting this acoustic signal in the form of a sequence of sound signals of variable duration separated from one another by periods of silence of a predetermined duration, the output data being coded by varying the duration of the different sound signals;

- or by modulating the frequency of the sound signal emitted (in this case, the frequency spectrum of the transducer 11 must not be constant, in which case the transducer may be a piezo-electric loudspeaker).

In another embodiment, it would also be possible for the acoustic signal emitted by the transducer 11 to be received directly by the micro-computer 1, in particular via an external microphone 12 connected to an internal sound card of the micro-computer which the user can move close to the reader 2 at the appropriate moment in accordance with instructions displayed on the screen of the micro-computer. In view of the fact that the sound signal is not emitted in a very specific direction by the transducer 11, this sound signal will be very widely broadcast, in-

cluding outside the micro-computer housing : it can therefore be easily picked up by the microphone 12.

In another embodiment, the acoustic signal emitted by the transducer 11 is transmitted to a remote control station 13 :

- by means of said microphone 12 and a modem 14 belonging to the micro-computer 1 and linked to the remote central station 13 by means of the switched telephone network,
- or by the user dialling in to the central station 13.

In the latter case, the remote control station 13 will determine the security code on the basis of said acoustic signal and transmit this security code to the micro-computer 1 via the modem 14 (or the user will be issued with the security code by telephone and enter it into the micro-computer from the keyboard 1b). Optionally, the remote central station 13 may be set up so as not to transmit this security code to the micro-computer 1 if, for example, use of the computer application in question is subject to payment of a subscription and this has not been paid.

In another embodiment illustrated in figure 3, the acoustic transducer may be a loudspeaker 16 connected to a voice synthesising circuit 15 which is in turn controlled by the central unit 7: this being the case, the loudspeaker 16 issues a sound message which is comprehensible to the user and contains the output data corresponding to the security code. Optionally, the voice synthesising circuit 15 may be integrated in the central unit 7, which might be a micro-processor of the TSP50C0x/1x type, for example, sold by TEXAS INSTRUMENTS, Dallas, USA.

In another embodiment, the motion sensor 10 could communicate a rotation speed measurement of the optical disc to the central unit 7, for example via an analogue-to-digital converter (not illustrated) and a command would be issued to the optical disc reader 2 by the micro-computer 1 to rotate the disc at several different speeds in succession in order to encode the input data. Said input data could then be transmitted in the form of a multivalent signal having two values, for example a quadrivalent signal if the reader 2 is selectively able to stop the disc 3 or rotate it at three different speeds: in this particular case, the transmission rate of the input data will be double that at which said input data is coded in the form of a simple stop/go sequence.

Furthermore, in order to increase security of the optical disc 3 still further, the central unit 7 is preferably programmed so that it shuts down in particular:

- if the motion sensor 10 detects a movement by the disc 3 which does not meet certain predetermined criteria in keeping with normal use and in particular if the motion sensor detects continuous motion for at least one predetermined period (which may indicate an attempt to "pirate" the optical disc),
- and if it receives a shut-down command from the micro-computer 1, for example if the latter has received successive error codes instead of the security code corresponding to the output data of the central unit 7.

In another embodiment, the acceleration sensor 10 might be an electric current micro-generator capable of generating an electric current due to the rotating action of the optical disc. This current sensor, connected to an electronic power storage circuit incorporating a capacitor

for example, could then replace the battery 9 or supply at least some of the electric power consumed by the electronic circuit 6.

It should be pointed out in addition that the input data may be transmitted from the micro-computer 1 to the optical disc 3 by a method other than a stop and go sequence in the reader 2. This being the case, the motion sensor 10 could nevertheless still be provided in the circuit 6 in order to control activation and shut-down of the central unit 7, as illustrated in figure 4.

For example, data may be transmitted by controlling the laser beam of the optical disc reader 2 so that it passes across one or more light sensors connected to the central unit 7, in a manner known per se from the prior art.

In another embodiment, as illustrated in figure 4, use can be made of the occurrence of local heating of the optical disc 3 as it is scanned by the laser beam of the reader: in this case, instead of using light sensors, several thermoelectric elements 17 will be used, each of which will be connected to the central unit 7 via an analogue-to-digital converter 18 or another adaptation circuit and which will exhibit at least one electrical characteristic which varies depending on its temperature.

Accordingly, the central unit 7 will be able to detect the laser beam of the reader as it passes across the thermoelectric element 17 due to variations in said electrical characteristic and determine the input data on detection of the beam as it passes over a period of time.

The thermoelectric element 17 may be of a PZT base in particular (lead-zirconium titanate) and may be adapted to generate an electric voltage (due to the piezo-electric

effect in the case of PZT) when heated by the reader beam, this electric voltage constituting said electric characteristic detected by the central unit 7.

As illustrated in figure 5, for example, the element 17 may be a parallelepiped of PZT 19 with a thickness e of a few microns in the same direction of thickness as the optical disc and a surface area in the order of 1 to several μm^2 in the plane parallel with the faces of the optical disc, this parallelepiped being framed by two electrodes 20 connected to the above-mentioned circuit 18. Although the element 17 is only briefly illuminated by the reader laser beam as it passes (in the order of 1 μs), the light energy picked up by the element 17 is sufficient to generate a voltage of several Volts between the electrodes 20.

This embodiment has an advantage over the light sensors known from the prior art because the laser beam of the reader does not have to be so accurately positioned relative to the thermoelectric element 17: in practice, even if the laser beam does not pass exactly across the thermoelectric element 17 and instead passes slightly to the side of it, the pass of said laser beam will nevertheless produce heat which is detected by the thermoelectric element 17.

It should also be pointed out that one or the other receiving interface mentioned above could be used in conjunction with a transmission interface other than an acoustic interface, for example an optical interface.

Finally, it should also be pointed out that the security procedure permitted by the optical disc 3 or other data medium proposed by the invention is not limited to controlling the use of programmes or data contained on

the optical disc: on the contrary, this security procedure may be used as a means of identifying the user, for example, in particular to permit remote payment transactions to allow remote access to protected data and to do so without necessarily having to fit the micro-computer with a specific security device such as a memory card reader or similar.

In this case, if the micro-computer 1 is fitted with a microphone 12 and a modem 14, the security procedure will be initiated when the user enters a secret code from the keyboard 1b, after which said central station 13 (or similar) will exchange coded messages with the security circuit 7 of the optical disc in order to check the consistency of the code entered by the user and a secret key contained in the memory 8 of the central unit 7, in a manner already used with debit cards incorporating a memory.

A data medium of the type described above could also be used in an application such as the electronic purse or similar. In this case, the electronic security device 6 may run a count of value units (monetary units or similar) in its memory and the central unit 7 of said security device will then be programmed to vary the value units in said account depending on the coded data received and transmitted by the central unit 7 via the receiving and transmission interfaces, for example, when the user is purchasing units to top up the account for example or in the reverse situation to debit the account when purchases or other payment transactions are made by the user, for example on the internet network.

If the security device 6 is used to control or limit usage of the data medium, as described above, or to

establish a user profile, this electronic security device may have one or more user unit counters in its memory.

If it is desirable to limit use of the data medium, this counter may represent a period of usage, for example, or a number of times used and the central unit 7 of the security device can be adapted to increment or decrement said counter depending on the movements of the data medium detected by the motion sensor 10. For example, the transmission interface of the security device will cease issuing the coded output data that would normally allow the user device to run the data medium if the central unit 7 has detected that the data medium has been launched a predetermined number of times x, i.e. if the counter has reached x starting from 0 or if it has reached 0 starting from x.

If it is desirable to establish a user profile, the usage counter or counters may be incremented each time the data medium makes certain movements or certain predetermined sequences of movements representing certain predetermined operations, for example.

Advantageously, a reading of the user units in the counter can be taken from an external reader 22 (EXT. DRV - figure 2) via a communication interface 21 such as an electronic tag (TAG) programmed to communicate with the interface 22 via Hertzian channel and belonging to said security device 6. This method of taking a reading from the counter could be used in situations where the user is shopping in a retail outlet selling the data medium, for example. In this case, the data medium may advantageously be miniaturised, for example to credit card format.

CLAIMS

1. A security-protected portable medium for digital data which can be read by an electronic user device (1) comprising at least one input interface (1b, 12, 14), this data medium being designed to be subjected to at least one predetermined movement imposed by the electronic user device (1) when reading said data medium, said data medium having an electronic security device (6) comprising:

- a receiving interface (10) for receiving input data from the electronic user device,
- a transmission interface (11; 15, 16) designed to transmit output data depending on the input data received, the output data corresponding to a security code to be communicated to the input interface (1b, 12, 14) of the electronic user device,
- and a central electronic unit (7) connected to the receiving (10) and transmitting (11; 15, 16) interfaces and programmed so as to determine the output data on the basis of the input data and to transmit said output data via the transmission interface,

characterised in that the receiving interface of said data medium has a motion sensor (10) designed to detect movements of the data support, the central unit (7) of the data medium being adapted to determine the input data on the basis of movements of the data medium detected over a period of time.

2. A data medium as claimed in claim 1, in which the central unit (7) is set up to determine the input data on the basis of whether movement of the data medium is detected or not detected over time.



3. A data medium as claimed in claim 1, designed to be subjected to several predetermined movements imposed by the electronic user device (1) when reading said data medium, the central unit (7) of the data medium being set up to determine the input data on the basis of said predetermined several movements of the data medium detected over time.

4. A data medium as claimed in any one of the preceding claims, in which the motion sensor is an acceleration sensor (10).

5. A data medium as claimed in claim 4, in which the electronic user device (1) rotates the data medium at at least one predetermined rotation speed when reading it, the motion sensor being a radial acceleration sensor (10) adapted to detect rotation of the data medium at said at least one predetermined speed.

6. A data medium as claimed in any one of the preceding claims, in which the motion sensor (10) is a current micro-generator which is designed to generate an electric current when the data medium (3) is in motion and which supplies the security device (6) at least partially with electric power.

7. A data medium as claimed in any one of the preceding claims, in which the central unit (7) is designed to shut down if the motion sensor (10) detects a movement of said data medium which does not meet certain predetermined criteria in keeping with normal use.

8. A data medium as claimed in claim 7, in which the central unit (7) is designed to shut down if the motion sensor (10) detects continuous motion for at least a predetermined period.

9. A data medium as claimed in any one of the preceding claims, in which the transmission interface has an acoustic transducer (11, 16) which emits the output data in the form of an acoustic signal.

10. A data medium as claimed in claim 9, in which the central unit (7) is set up so that the acoustic signal from the transducer (11, 16) is emitted in the form of a series of sound signals of variable duration, separated from one another by periods of silence of a predetermined duration, the output data being coded by the variation in the duration of the different sound signals.

11. A data medium as claimed in claim 9, in which the central unit (7) is set up so that the acoustic signal from the transducer (11, 16) is emitted in the form of several streams of sound signals, each comprising several elementary sound signals of a constant duration, the number of elementary sound signals in each stream being between 1 and a whole number n at least equal to 2, the streams of sound signals being separated from one another by periods of silence at least equal to a predetermined duration, and the output data being coded by the number of elementary sound signals in each steam of sound signals.

12. A data medium as claimed in any one of claims 9 to 11, in which the transducer is an electronic buzzer (11) which emits an acoustic signal exhibiting a constant emission frequency spectrum.

13. A data medium as claimed in claim 9, in which the transducer is a loudspeaker (16) connected to voice synthesising means (15), the central unit (7) of the data medium being set up so that the loudspeaker emits a sound message which is comprehensible to a human operator and contains the output data.

* C L M S *

14. A data medium as claimed in any one of the preceding claims, constituting an optical disc.

15. A method of providing security protection for a data medium (3) as claimed in any one of claims 9 to 13, and comprising the following steps, whereby :

- the data medium is read in a reader (2) belonging to an electronic user device (1) having an input interface (1b, 12, 14),
- the electronic user device (1) transmits the input data to the receiving interface (10) of the data medium,
- the central unit (7) of the data medium determines the output data on the basis of the input data,
- a transducer (11, 16) belonging to the data medium transmits the output data in the form of an acoustic signal,
- the security code corresponding to the output data is communicated to the electronic user device (1) via the input interface (1b, 12, 14) of said electronic user device,
- depending on the security code received by the electronic user device (1), a certain operating mode of said electronic user device will be authorised or not.

16. A security protection method as claimed in claim 15, in which a human operator listens to the acoustic signal containing the output data and said operator determines the security code depending on the signal heard and communicates this security code to the electronic user device via its input interface (1b).

17. A security protection method as claimed in claim 15, in which the acoustic signal containing the output data is received by the input interface (12) of the electronic user device directly.

* C L M S *

18. A security protection method as claimed in any one of claims 15 to 17, in which the acoustic signal containing the output data is transmitted to a remote control station (13) which determines the security code on the basis of said acoustic signal and transmits this security code or not to the input interface (14) of the electronic user device.

19. Use of a data medium as claimed in any one of claims 1 to 14, in which coded data are exchanged between a remote central station (13) and the central unit (7) of the data medium via the receiving interfaces (10) and receiving system (11 ; 15, 16) of said data medium.

20. Use as claimed in claim 19, in which the user is identified on the basis of coded data exchanged between the remote central station (13) and the central unit (7) of the data medium in order to provide security for a remote transaction.

21. Use as claimed in claim 20 as a means of providing security for a remote payment transaction.

22. Use of a data medium as claimed in any one of claims 1 to 14, whereby the electronic security device (6) has in its memory a count of units of value and the central unit (7) of said security device is set up so as to vary said count of value units on the basis of coded data received and transmitted by the central unit (7) via the receiving (10) and transmission (11 ; 15,16) interfaces.

23. Use of a security-protected data medium as claimed in any one of claims 1 to 14, whereby the electronic security device (6) has in memory at least one user unit counter and the central unit (7) of said security device is set up so as to vary said counter depending on

* C L M S *

movements of the data medium detected by the motion sensor (10).

24. Use as claimed in claim 23, whereby a reading of the user units on the counter is taken from an external reader (22) by means of a communication interface (21) belonging to said security device (6).



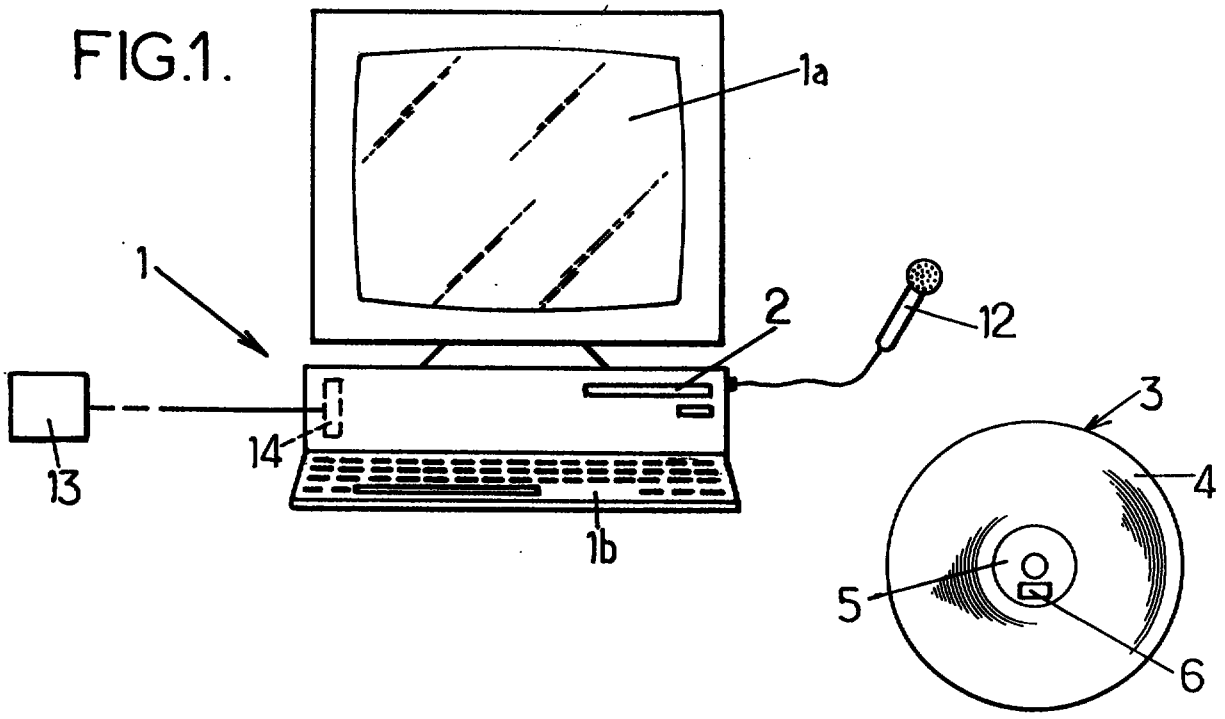
A security-protected portable medium for digital data and a security protection method using said data medium.

ABSTRACT

A security-protected medium for digital data comprising a receiving interface (10) set up to receive input data from an electronic user device by detecting the movements imposed on the medium by the user device, an output interface (11) set up to transmit output data on the basis of the input data received and an electronic central unit (7) connected to the receiving and transmission interfaces and set up to determine the output data on the basis of the input data and to transmit said output data.

FIGURE 2

FIG.1.



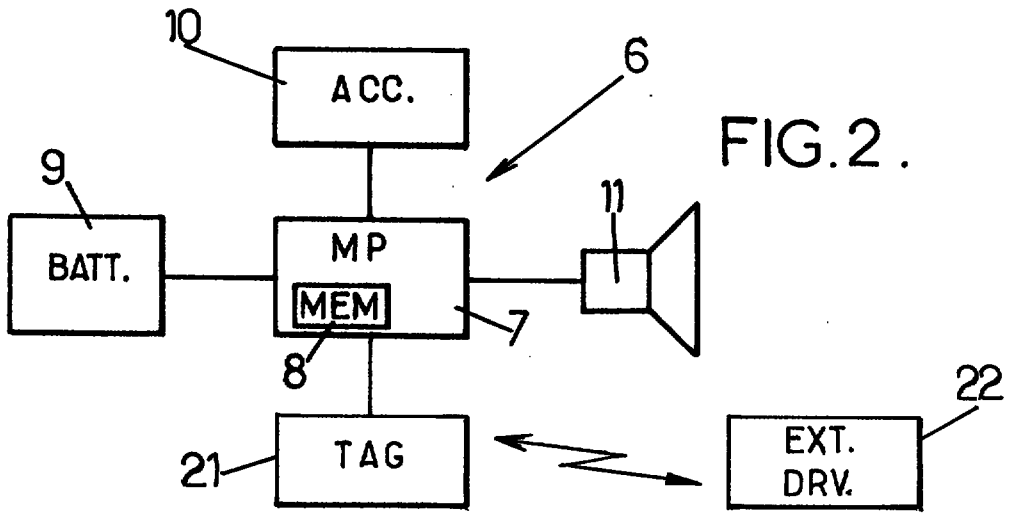
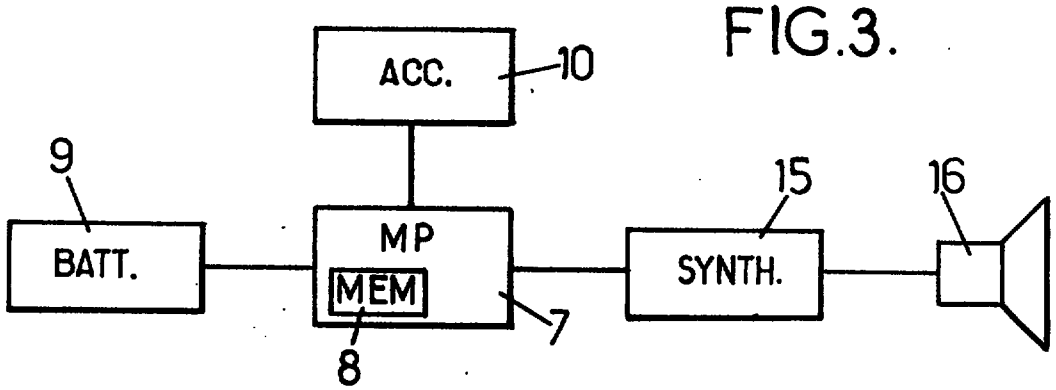


FIG.2.

FIG.3.



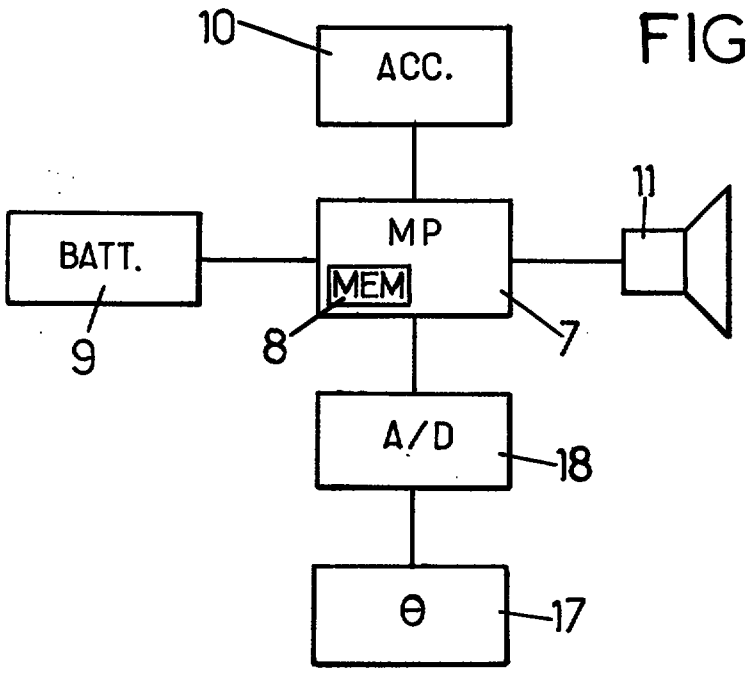


FIG.4.

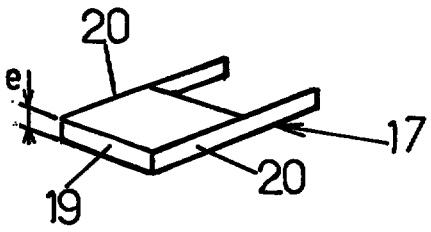


FIG.5.