Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2393645 A1 2001/06/14

(21) 2 393 645

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 1999/12/07
(87) Date publication PCT/PCT Publication Date: 2001/06/14
(85) Entrée phase nationale/National Entry: 2002/06/06
(86) N° demande PCT/PCT Application No.: NL 1999/000748
(87) N° publication PCT/PCT Publication No.: 2001/043129

(51) Cl.Int.$^{7}$/Int.Cl.$^{7}$ G11B 20/00, G06F 1/00

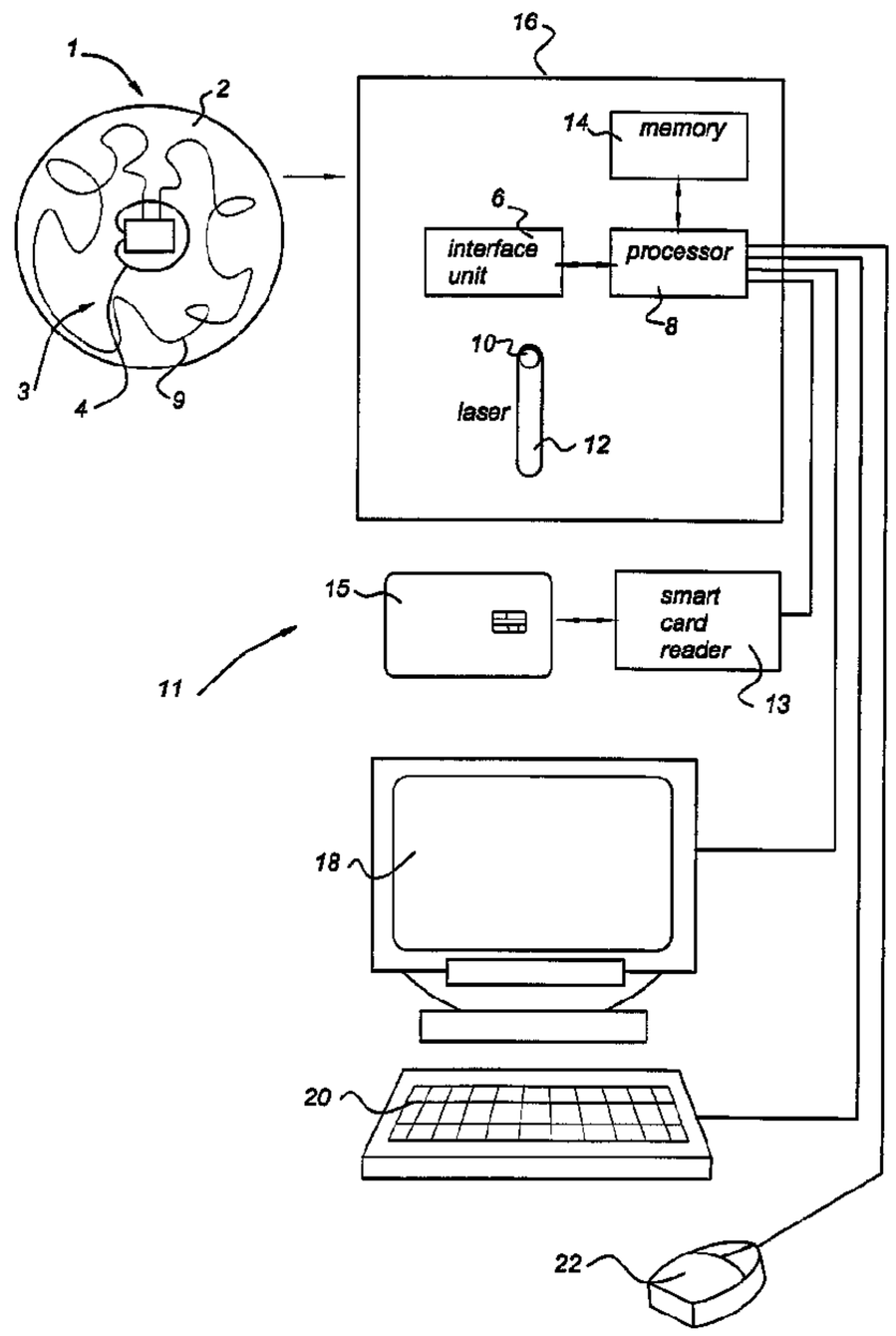
(71) Demandeur/Applicant:
SUN MICROSYSTEMS, INC., US

(72) Inventeur/Inventor:
DE JONG, EDUARD KAREL, NL

(74) Agent: MARKS & CLERK

(54) Titre : SUPPORT DE STOCKAGE LISIBLE PAR ORDINATEUR DOTE D'UN MICROPROCESSEUR DESTINE A COMMANDER LA LECTURE, ET ORDINATEUR CONCU POUR COMMUNIQUER AVEC UN TEL SUPPORT

(54) Title: COMPUTER-READABLE MEDIUM WITH MICROPROCESSOR TO CONTROL READING AND COMPUTER ARRANGED TO COMMUNICATE WITH SUCH A MEDIUM




(57) Abrégé/Abstract:
Computer-readable medium provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) having a communication interface (4), a memory unit (7) and a processor unit (5) connected to both the communication interface (4) and the memory unit (7). The data may include a first data portion which is arranged to be read and decrypted by a computer

CA 2393645 A1 2001/06/14

(21) 2 393 645

(13) A1

(57) Abrégé(suite)/Abstract(continued):
arrangement (11) provided at least one condition is met, and the microprocessor (3) being arranged to generate at least one cryptographic key once the condition is met that is necessary to decrypt the data. The invention is also directed to a computer arrangement arranged to communicate with such a medium.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/43129 A1

(51) International Patent Classification[7]: G06F 1/00 G11B 20/00,

(21) International Application Number: PCT/NL99/00748

(22) International Filing Date: 7 December 1999 (07.12.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **SUN MICROSYSTEMS INC.** [US/US]; San Antonio Road, MS PAL1-521, Palo Alto, CA 94303 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **DE JONG, Eduard, Karel** [NL/NL]; Ankersmidplein 63, NL-1506 CK Zaandam (NL).

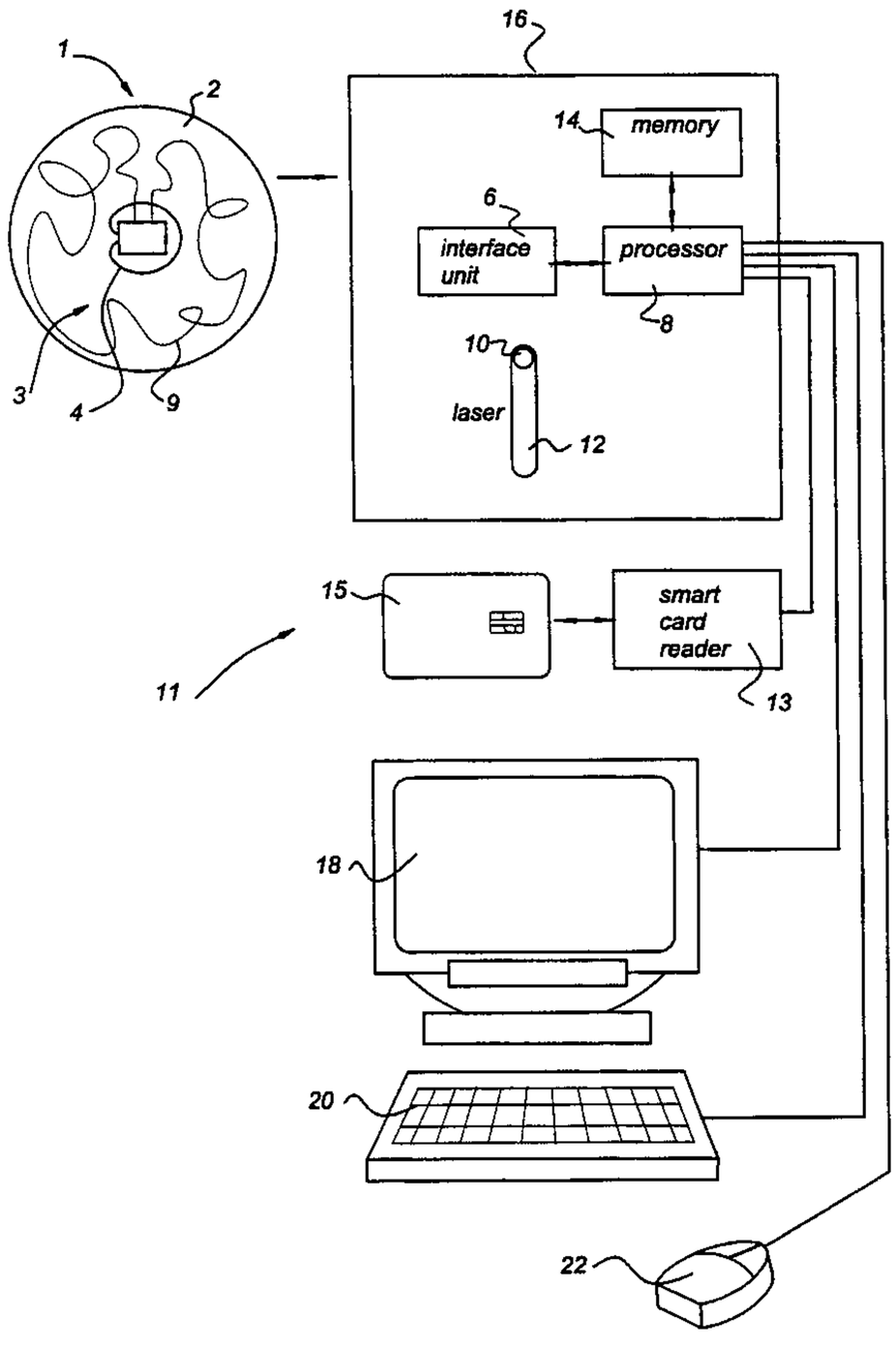
(74) Agent: **DE BRUIJN, Leendert, C.**; Nederlandsch Octrooibureau, Scheveningseweg 82, P.O. Box 29720, NL-2502 LS The Hague (NL).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: COMPUTER-READABLE MEDIUM WITH MICROPROCESSOR TO CONTROL READING AND COMPUTER ARRANGED TO COMMUNICATE WITH SUCH A MEDIUM




(57) Abstract: Computer-readable medium provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) having a communication interface (4), a memory unit (7) and a processor unit (5) connected to both the communication interface (4) and the memory unit (7). The data may include a first data portion which is arranged to be read and decrypted by a computer arrangement (11) provided at least one condition is met, and the microprocessor (3) being arranged to generate at least one cryptographic key once the condition is met that is necessary to decrypt the data. The invention is also directed to a computer arrangement arranged to communicate with such a medium.

WO 01/43129 A1

# WO 01/43129 A1

**Published:**
— *With international search report.*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# Computer-readable medium with microprocessor to control reading and computer arranged to communicate with such a medium

## BACKGROUND OF THE INVENTION

This invention relates to computer-readable medium provided with a memory area like a CD-ROM, a floppy disk, a cassette, a CD, a mini-disk and a DVD. For the sake of simplicity, hereinafter, these media will be called "data carriers".

Such a data carrier comprises data, e.g., in the form of computer software to be loaded into a computer of a user who bought it. However, in practice, often the data available on such a data carrier can be read many times whereas the producer of the data wishes to be paid again for every new loading in another computer. Nowadays, buyers are often signing a kind of contract promising not to infringe the copyright associated with the data. However, that is not a technical hindrance to illegal copying of the data. In practice, large-scale checking of illegal copies at the premises of, especially, end-users is almost impossible.

## SUMMARY OF THE INVENTION

Therefore, it is an object to provide technical means that provide a strong protection against illegal copying of data on the data carrier.

In accordance with the present invention such illegal copying may be prevented with a computer-readable medium provided with a memory area for storing data and a distinct microprocessor comprising a communication interface for communication with an external device, a memory unit and a processor unit connected to both the communication interface and the memory unit.

With such a device , the intellectual property rights of data, albeit music, pictures or executable software stored on mass produces digital data carriers can be upheld effectively at little additional costs. The microprocessor is used to carry out protecting functions as to the data stored on the data carrier. This protection may relate to the number of times the data may be loaded in a computer, who is authorized to load the data in a computer, etc.

Such a protection may, e.g., be implemented by a computer-readable medium as defined above, wherein the data comprises a first data portion which is arranged to be read by a computer arrangement and to be decrypted by the computer arrangement using at least one cryptographic key provided at least one condition is met, and the processor unit being arranged to communicate with the computer arrangement through the communication interface in order to check whether the condition is met and to generate the cryptographic key for the computer arrangement once the condition is met.

Moreover, the data may comprise a second data portion comprising key related data necessary for the processor unit to generate the at least one cryptographic key.

The computer-readable medium may have a circular shape with a center of rotation and the communication interface being an antenna symmetrically shaped about the center of rotation.

One of the conditions to be met may be user authentication and, then, the processor unit is arranged to receive authentication information through the communication interface and to establish user authentication based on the authentication information received.

Alternatively, or additionally, one of the conditions to be met is period of time the data may be read and decrypted by either the computer arrangement or an other computer arrangement, the period of time being part of the data.

Moreover, alternatively, or additionally, one of the conditions to be met is maximum number of times the data may be read and decrypted from the computer-readable medium, the maximum number of times being monitored by the processor unit.

In a further embodiment, the processor unit in the computer-readable medium is arranged for carrying out the decrypting based on executable codes received through said communication interface. Once again, the processor unit is, then, preferably, arranged to validate these executable codes, e.g., by means of a specific key stored in the memory unit.

In one embodiment, the computer-readable medium is provided with a physical structure connected to the processor unit, the processor unit being arranged to check physical integrity of the physical structure and stop operating as soon as the processor unit establishes that the physical integrity is violated.

The invention also relates to a computer arrangement arranged to communicate with a computer-readable medium, the medium being provided with a memory area for

storing data and a distinct microprocessor comprising a communication interface, a memory unit and a processor unit connected to both the microprocessor interface and the memory unit, the computer arrangement being provided with a processor, a memory connected to the processor, a first interface unit connected to the processor for communicating with the memory area of the computer-readable medium and a second interface unit connected to the processor for communicating with the microprocessor unit through the communication interface.

The invention also relates to a method of reading and decrypting data from a computer-readable medium, the medium being provided with a memory area for storing data and a distinct microprocessor comprising a communication interface, a memory unit and a processor unit connected to both the communication interface and the memory unit, the method comprising the following steps:

(a) receiving at least one cryptographic key from the processor unit;

(b) reading a first data portion from the memory area in the computer-readable medium

(c) decrypting first data portion using the at least one cryptographic key.

The invention also relates to a data carrier provided with a computer program and to a computer program product for carrying out such a method.

Moreover, the invention relates to a method of giving access to data stored on a computer-readable medium, said medium being provided with a memory area storing said data and a distinct microprocessor comprising a communication interface, a memory unit and a processor unit connected to both said communication interface and said memory unit, wherein said data comprises a first data portion which is arranged to be read by a computer arrangement and to be decrypted by said computer arrangement using at least one cryptographic key provided at least one condition is met, said method including the steps of:

(a) communicating with said computer arrangement through said communication interface;

(b) checking whether said condition is met and

(c) generating said cryptographic key for said computer arrangement once the condition is met.

The invention also relates to a data carrier provided with a computer program and to a computer program product for carrying out such a latter method.

## BRIEF DESCRIPTION OF THE DRAWINGS

Hereinafter, the invention will be explained with reference to some drawing which are intended to illustrate the invention and not to limit its scope.

Figure 1 shows a data carrier provided with a distinct microprocessor to protect its data from illegal copying, as well as a system to read data from the data carrier;

Figure 2 schematically shows the microprocessor embedded in the data carrier;

Figure 3 schematically shows an alternative data carrier with additional microprocessor;

Figure 4 schematically shows a possible data flow between the memory area of the data carrier, the microprocessor on the data carrier and the system arranged to read and decrypt data from the data carrier;

Figures 5 and 6 show flow diagrams of methods of the invention.

## DESCRIPTION OF PREFERRED EMBODIMENT

The invention relates to digital data storage devices in which digital data, possibly organized in distinctly referably sections, is stored. The data may be retrieved in some form by a computer system and then used by a user. Figure 1 schematically shows some key elements. Figure 1 shows a circular shaped data carrier 1, like a CD, or CD-ROM, having data stored in a memory area 2. The data may comprise both executable codes once loaded in a computer and non-functional data, like text, music and pictures.

In accordance with the invention, the data carrier 1 is provided with a microprocessor 3. Figure 1 shows a circular antenna 4 as communication interface for a microprocessor unit not shown in figure 1. Figure 2 shows an example of the micro-

processor 3 comprising a processor unit 5 connected to the antenna 4 and a memory 7. The antenna preferably comprises one or more circular loops arranged such that they are centered about the center of rotation of the data carrier 1. The memory 7 may comprise any kind of memory like RAM, ROM, EPROM, EEPROM, etc. allowing the processor unit 5 to carry out its functions.

Preferably, the processor unit 5 itself is embedded in the data carrier structure such that it is tamper-resistant. Together with memory 7, it may be implemented as a single-chip microprocessor of a similar type as used in smart cards. As shown in figure 1, in case of a circular data carrier designed to rotate during reading, like a CD or CD-ROM, the microprocessor 3 is preferably located such that its center of gravity coincides with the center of rotation of the data carrier 1.

Preferably, the data carrier comprises an embedded physical structure 9 connected to the processor unit 5. The physical structure 9 is, e.g., made of one or more wire loops, the presence of which being detectable by the processor unit 5. If the microprocessor unit 5 is disconnected from the physical structure 9, e.g., either by removing the microprocessor 3 from the data carrier 1 or by damaging the data carrier 1, the processor unit 5 will detect that and will not be able anymore to carry out its protection function anymore. To that end, the processor unit 5 may detect the resistance of wire loops. Alternatively, the physical structure 9 may have some predetermined capacitance or inductance or any kind of (complex) impedance that can be detected by the processor unit 5. With such an additional structure 9, one cannot use the microprocessor 3 anymore after having removed it from the data carrier 1. Only reverse engineering could then provide knowledge about the content of the microprocessor 3. However, this content may be unique for each different microprocessor 3 such that reverse engineering will never be worthwhile.

Figure 1 also shows a computer arrangement 11 comprising, e.g., a separate box 16 with a processor 8, a monitor 18, and input means like a keyboard 20 and a mouse 22. The box 16 also comprises a memory 14 connected to the processor 8. The memory is shown as one black box, however, it is to be understood that memory 14 may comprise any kind of memories, like RAM, ROM, EPROM, EEPROM, etc., to allow the processor 8 to carry out its normal operations.

In some embodiments, the computer arrangement 11 may comprise a smart card reader 13 connected to the processor 8 and arranged to read a smart card 15.

The processor 8 is shown to be connected to a laser unit 10 as an interface to read data from (and possibly write to) the data carrier 1. Of course, in case another kind of data carrier then a CD or CD-ROM is used, also another kind of interface 10 must be used. A groove 12 is provided to allow the laser unit 10 to move in a radial direction across the data carrier 1, as is known to persons skilled in the art.

Apart from the interface 10, the box 16 comprises another interface unit 6 that is arranged to allow the processor 8 to communicate with the processor unit 5 on the data carrier 1 when it is inserted into the box 16 to its reading position in which data may be read from the memory area 2 on the data carrier 1 by laser unit 10.

Figure 3 shows an alternative embodiment of a data carrier according to the invention. It shows a cassette 24 with tape storing data and wound around two shafts 26, 28 as is known in the art. Again, a microprocessor 3 is embedded in the physical structure of the cassette 24. Alternatively, the microprocessor 3 may be located on the small side surface of the cassette 24.

Instead of a CD/CD-ROM as shown in figure 1 or a cassette as shown in figure 3, any other known type of data carrier, such as floppy disk, may be applied to carry out the present invention.

The processor unit 5 embedded in the data carrier 1 is programmed to control read and/or write access of the processor 8 to the data carrier memory area 2. To that end, the processor unit 5 is, preferably, arranged to generate one or more secret, cryptographic keys which are, e.g., initialized at the final stages of manufacturing of the data carrier 1 with its processor unit 5. The one or more keys are, preferably, unique to the data carrier and may be simply stored in memory 7 of the microprocessor 3 or be calculated by the processor unit 5, as will be explained hereinafter. Below, for the sake of simplicity of the description, it will be assumed that only one key is used.

At least a portion of the data in memory area 2 is stored after being encrypted by the key. In one embodiment, the key is directly stored in memory 7 of the microprocessor 3. However, the processor unit 5 may be arranged to calculate the correct key based on one or more other (master) keys in memory 7 using key related data retrieved from memory area 2 on the data carrier 1. With reference to figure 4, such key related data will be read from the memory area 2 by processor 8 from the computer arrangement 11, preferably, without using any additional authorization mechanism, and then be transferred to the processor unit 5 through the communication interface 4. By using

key related data stored in memory area 2 to allow processor unit 5 to calculate the necessary key using its own master key from memory unit 7, the encryption algorithms used to conceal data to be protected on the data carrier 1 can be selected to use very long keys, like in one-time pad calculations which require keys of the same length as the protected data.

When the processor 8 of the computer arrangement 11 is instructed by a user, through its input means 20, 22, to read protected (encrypted) data from data carrier 1, it will request the processor unit 5 to generate the correct key. The processor unit 5 will send its key from memory 7 or calculate the correct key based on the key related data as indicated above and send the key to the processor 8. As indicated in step 40 of figure 5 the processor 8 will receive this key. Then, the processor 8 reads data from the memory area 2 of data carrier 1, step 42. As shown in step 44, the processor 8 will use the key to decrypt data read from the data carrier 1 and store the decrypted data in its memory 14. Instructions as to how to communicate with the data carrier 1 may be loaded from the data carrier 1 to the processor 8 in any way known to the person skilled in the art, e.g., by loading an execute file from data carrier 1 to processor 8.

In practice, the generation of the key by the processor unit 5 will be dependent on whether or not one or more conditions have been met. This is further explained in figure 6.

One such condition may be the time period that the data in the data carrier 1 may be read and decrypted after a predetermined date loaded in memory 7 of the micro-processor 3. The data may e.g. be a demonstration computer program which may be used during three months after which decryption will automatically be blocked.

Another condition may be the maximum number of times the data may be read from data carrier 1 and decrypted by processor 8 or any other processor external to data carrier 1. To that end, the microprocessor 3 may store such a maximum number and check whether the number of times it is requested by a computer arrangement to provide the key exceeds that maximum number. For instance, in many cases an end-user is allowed to read and decrypt the data twice, i.e., once for regular purposes and once for back up. In such cases, the maximum number equals 2.

In general, as shown in figure 6, for checking the condition to be met the computer arrangement 11 and the data carrier 1 start communicating in step 50. In order to enhance security the condition is preferably checked by processor unit 5 of the

data carrier 1, step 52. Only if the condition is met the processor unit 5 will generate the required key and send it to the processor 8 of the computer arrangement 11, step 54.

In order to be sure that both the key and the decryption algorithm are never entirely known to the computer arrangement protection and control over data use may be achieved by interaction between the processor unit 5 and the processor 8 such that the processor unit 5 performs additional computations necessary for the decryption algorithm. For effective operation with respect to speed of performance, such additional computations for decryption can be performed on a selected part of the data to be protected, e.g., every first 100 bytes of each retrieved 20 kbytes. To this end, figure 4 shows the situation that part of the encrypted data from the data carrier 1 is transferred to the processor unit 5 by computer arrangement 11.

Protection may further be enhanced by introducing an authentication mechanism of the user. Then, only when the user proves his/her authenticity to the processor unit 5 the latter will provide the correct key. To that end, passwords or user codes input by the user through one of the input means 20, 22 can effectively be used. Such a pass word or user code must then correspond to a password or user code stored in memory 7.

Alternatively, a password acceptance algorithm based on additional authentication data stored in the data carrier 1 may be used. Such authentication data may be read by processor 8 from the data carrier 1 and be transferred to the microprocessor 3 (see figure 4). A password input by a user may, e.g., be checked by the processor unit 5 as being valid upon checking whether or not it belongs to a dictionary of acceptable words stored as such authentication data in the data carrier 1 possibly complemented with rules for combining them, the rules being stored as an authentication key in memory 7.

User identification may also be carried out by using the smart card reader 13 and smart card 15 that belongs to a user who knows a password associated with the smart card 15.

As a further alternative, the smart card reader 13 may be arranged to read smart card 15 provided with an electronic purse facility and the processor unit 5 may be arranged to allow decryption of data from the data carrier 1 only when a predetermined amount of money has been paid through the electronic purse. A payment facility through the Internet is another option for paying in advance of any next decryption step.

The protection mechanism illustrated above may be expanded to providing different sets of keys for different sets of data on the data carrier.

The copy of the data to be protected and loaded in the computer memory 14 may be provided with a digital watermark calculated by the microprocessor 8 during the process of loading the data into the computer 11. The calculation algorithm used by the processor 8 to provide the watermark is derived from the data carrier 1. Alternatively, either a part of or the entire watermark is calculated by processor unit 5 and sent to the processor 8. The watermark may include the time of loading, user identity information or any other information to uniquely identify a stored copy of the loaded data. The watermark may use data elements of the data itself such that the data itself will at least be partly damaged if somebody tries to remove the watermark. The watermark serves as an identifier to locate the source of illegal copies of the data.

The processor 8 is shown to be one block. However, if preferred, the processor 8 may be implemented as several sub-processors communicating with one another each dedicated to perform a predetermined task. Preferably, the processor 8 is (or the sub-processors are) implemented as a computer with suitable software. However, if desired, it (or they) may be implemented as dedicated digital circuits.

The software running on the processor unit 5 of the data carrier 1 and on the processor 8 of the computer arrangement 11 may, prior to loading, be stored on a data carrier like a CDROM or may be distributed through a telecommunication connection (for instance entirely or partly wireless) like the Internet.

# Claims

1. Computer-readable medium provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) comprising a communication interface (4) for communication with an external device (16), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7).

2. Computer-readable medium according to claim 1, wherein said data comprises a first data portion which is arranged to be read by a computer arrangement (11) and to be decrypted by said computer arrangement (11) using at least one cryptographic key provided at least one condition is met, and said processor unit (5) being arranged to communicate with said computer arrangement (11) through said communication interface (4) in order to check whether said condition is met and to generate said cryptographic key for said computer arrangement (11) once the condition is met.

3. Computer-readable medium according to claim 2, wherein said data comprises a second data portion comprising key related data necessary for the processor unit (5) to generate said at least one cryptographic key.

4. Computer-readable medium according to claim 1, wherein said computer-readable medium has a circular shape with a center of rotation and said communication interface (4) being an antenna symmetrically shaped about said center of rotation.

5. Computer-readable medium according to claim 2, wherein one of said conditions to be met is user authentication and said processor unit (5) is arranged to receive authentication information through said communication interface (4) and to establish user authentication based on said authentication information received.

6. Computer-readable medium according to claim 5, wherein said authentication information comprises additional authentication data stored on said data carrier (1), said memory unit (7) storing an authentication key to validate said additional authentication data during said user authentication.

7. Computer-readable medium according to claim 2, wherein one of said conditions to be met is period of time said data may be read and decrypted by either said computer arrangement (11) or an other computer arrangement, said period of time being part of said data.

8. Computer-readable medium according to claim 2, wherein one of said conditions to be met is maximum number of times said data may be read and decrypted from said computer-readable medium, said maximum number of times being monitored by said processor unit (5).

9. Computer-readable medium according to claim 2, wherein said first data portion comprises a plurality of further data portions, and said processor unit (5) being arranged to generate at least one further cryptographic key for said computer arrangement (11) to decrypt each of said further data portions, said at least one further cryptographic key being generated only when the processor unit (5) has checked the validity of at least one further condition.

10. Computer-readable medium according to claim 1, wherein said data comprises a first data portion which is arranged to be read by a computer arrangement (11) for transfer to said processor unit (5) of said computer-readable medium (1) and said processor unit (5) is arranged to decrypt at least part of said first data portion using a decryption key stored in said memory unit (7) to provide decrypted data for said computer arrangement (11), which further decryption key is not provided to said computer arrangement (11).

11. Computer-readable medium according to claim 10, wherein said processing unit (5) provides said decrypted data with at least part of a digital watermark.

12. Computer-readable medium according to claim 10, wherein said processor unit (5) is arranged for carrying out said decrypting based on executable codes received through said communication interface (4).

13. Computer-readable medium according to claim 12, wherein said executable codes are part of said data.

14. Computer-readable medium according to claim 1, wherein said computer-readable medium is provided with a physical structure (9) connected to said processor unit (5), said processor unit (5) being arranged to check physical integrity of said physical structure (9) and stop operating as soon as said processor unit (5) establishes that said physical integrity is violated.

15. Computer arrangement arranged to communicate with a computer-readable medium, said medium being provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) comprising a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), said computer arrangement being provided with a processor (8), a first interface unit (10) connected to said processor (8) for communicating with said memory area (2; 26, 28) of said computer-readable medium and a second interface unit (6) connected to said processor (8) for communicating with said processor unit (5) through said communication interface (4).

16. Computer arrangement according to claim 15, arranged to carry out the following steps:

(a) receiving at least one cryptographic key from said processor unit (5);

(b) reading a first data portion from said memory area in said computer-readable medium;

(c) decrypting said first data portion using said at least one cryptographic key.

17. Computer arrangement according to claim 15 or 16, arranged to receive a second data portion comprising key related data from said memory area of said computer-readable medium, and to transmit said second data portion to said microprocessor (3) to allow generation of said at least one cryptographic key by said microprocessor (3).

18. Computer arrangement according to claim 15, 16 or 17, wherein one of said conditions to be met is user authentication and said computer arrangement is arranged to

transmit authentication information to said processor unit (5) through said communication interface (4) to allow said processor unit (5) to establish user authentication based on said information received.

19. Computer arrangement according to one of the claims 15 through 18, wherein one of said conditions to be met is a period of time during which said data may be read and decrypted by said computer arrangement, data relating to said period of time being readable from said computer-readable medium by said computer arrangement and transferable to said processor unit (5).

20. Computer arrangement according to one of the claims 15 through 19, wherein one of said conditions to be met is maximum number of times said data may be read from said computer-readable medium, said computer arrangement being arranged to retrieve additional data from said computer-readable medium to allow said processor unit (5) to monitor said maximum number of times.

21. Method of reading and decrypting data from a computer-readable medium, said medium being provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) comprising a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), said method comprising the following steps:

(a) receiving at least one cryptographic key from said processor unit (5);

(b) reading a first data portion from said memory area in said computer-readable medium, and

(c) decrypting said first data portion using said at least one cryptographic key.

22. A data carrier provided with a computer program for a method of reading and decrypting data from a computer-readable medium, said medium being provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) comprising a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), said method comprising the following steps:

(a) receiving at least one cryptographic key from said processor unit (5);

(b) reading a first data portion from said memory area in said computer-readable medium, and

(c) decrypting said first data portion using said at least one cryptographic key.

23. A computer program product for a method of reading and decrypting data from a computer-readable medium, said medium being provided with a memory area (2; 26, 28) for storing data and a distinct microprocessor (3) comprising a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), said method comprising the following steps:

(a) receiving at least one cryptographic key from said processor unit (5);

(b) reading a first data portion from said memory area in said computer-readable medium, and

(c) decrypting said first data portion using said at least one cryptographic key.

24. Method of giving access to data stored on a computer-readable medium, said medium being provided with a memory area (2; 26, 28) storing said data and a distinct microprocessor (3) comprising a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), wherein said data comprises a first data portion which is arranged to be read by a computer arrangement (11) and to be decrypted by said computer arrangement (11) using at least one cryptographic key provided at least one condition is met, said method including the steps of:

(a) communicating with said computer arrangement (11) through said communication interface (4);

(b) checking whether said condition is met and

(c) generating said cryptographic key for said computer arrangement (11) once the condition is met.

25. A data carrier provided with a computer program for a method of giving access to data stored on a computer-readable medium, said medium being provided with a memory area (2; 26, 28) storing said data and a distinct microprocessor (3) comprising

a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), wherein said data comprises a first data portion which is arranged to be read by a computer arrangement (11) and to be decrypted by said computer arrangement (11) using at least one cryptographic key provided at least one condition is met, said method including the steps of:

(a) communicating with said computer arrangement (11) through said communication interface (4);

(b) checking whether said condition is met and

(c) generating said cryptographic key for said computer arrangement (11) once the condition is met.

26. A computer program product for a method of giving access to data stored on a computer-readable medium, said medium being provided with a memory area (2; 26, 28) storing said data and a distinct microprocessor (3) comprising a communication interface (4), a memory unit (7) and a processor unit (5) connected to both said communication interface (4) and said memory unit (7), wherein said data comprises a first data portion which is arranged to be read by a computer arrangement (11) and to be decrypted by said computer arrangement (11) using at least one cryptographic key provided at least one condition is met, said method including the steps of:

(a) communicating with said computer arrangement (11) through said communication interface (4);

(b) checking whether said condition is met and

(c) generating said cryptographic key for said computer arrangement (11) once the condition is met.

*****

Fig 1

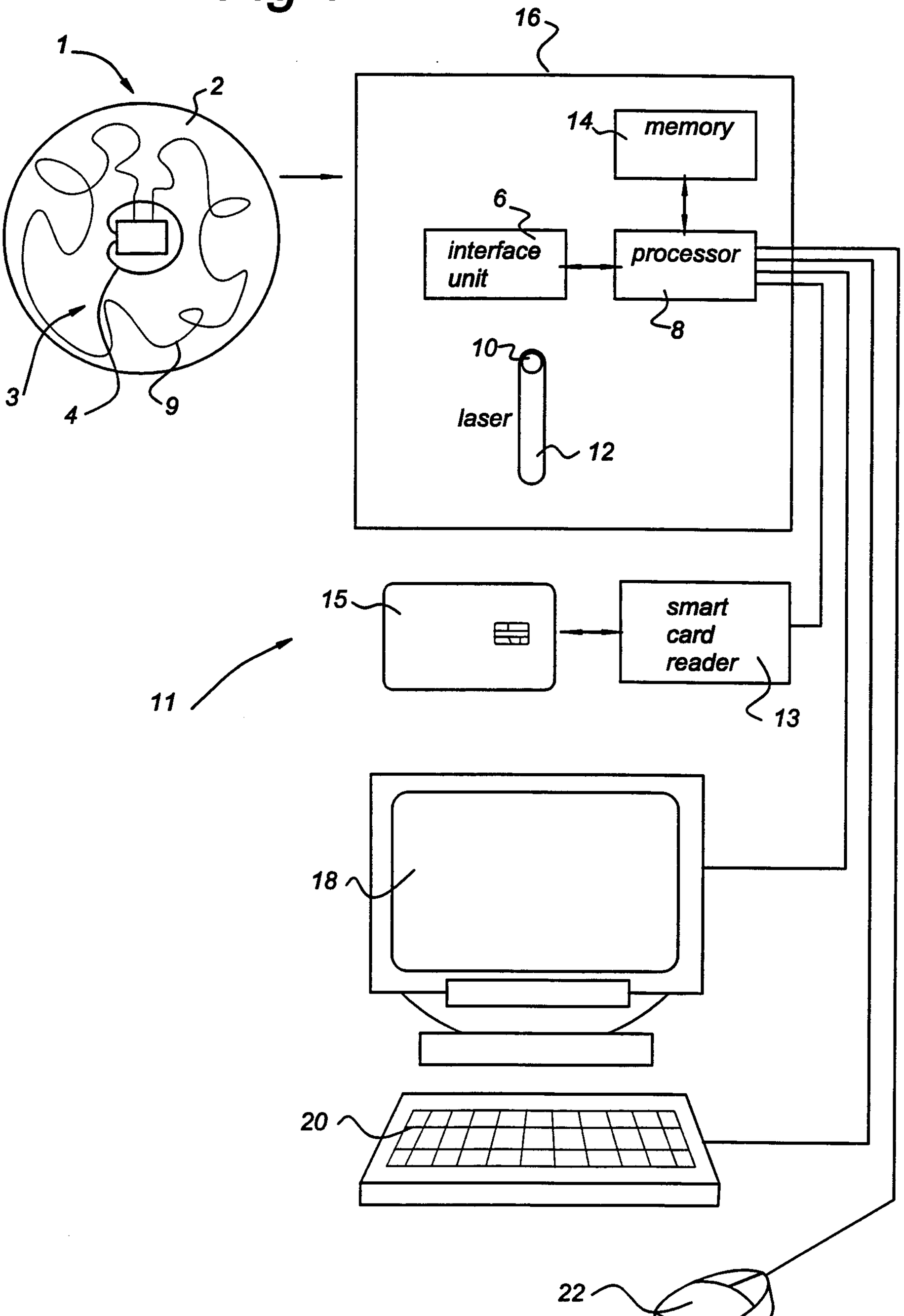

1
2
3
4
9
16
14
memory
6
interface unit
processor
8
10
laser
12
11
15
smart card reader
13
18
20
22

Fig 2

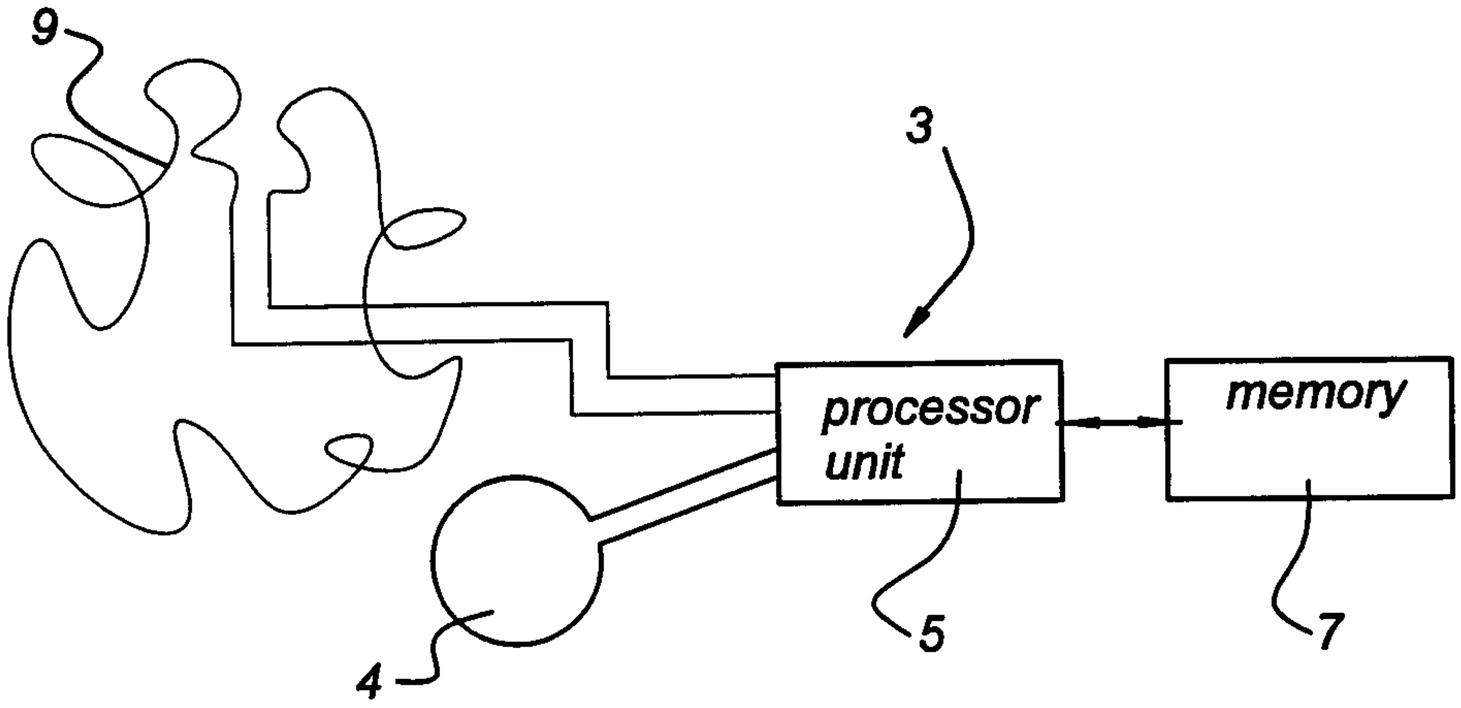



Fig 3

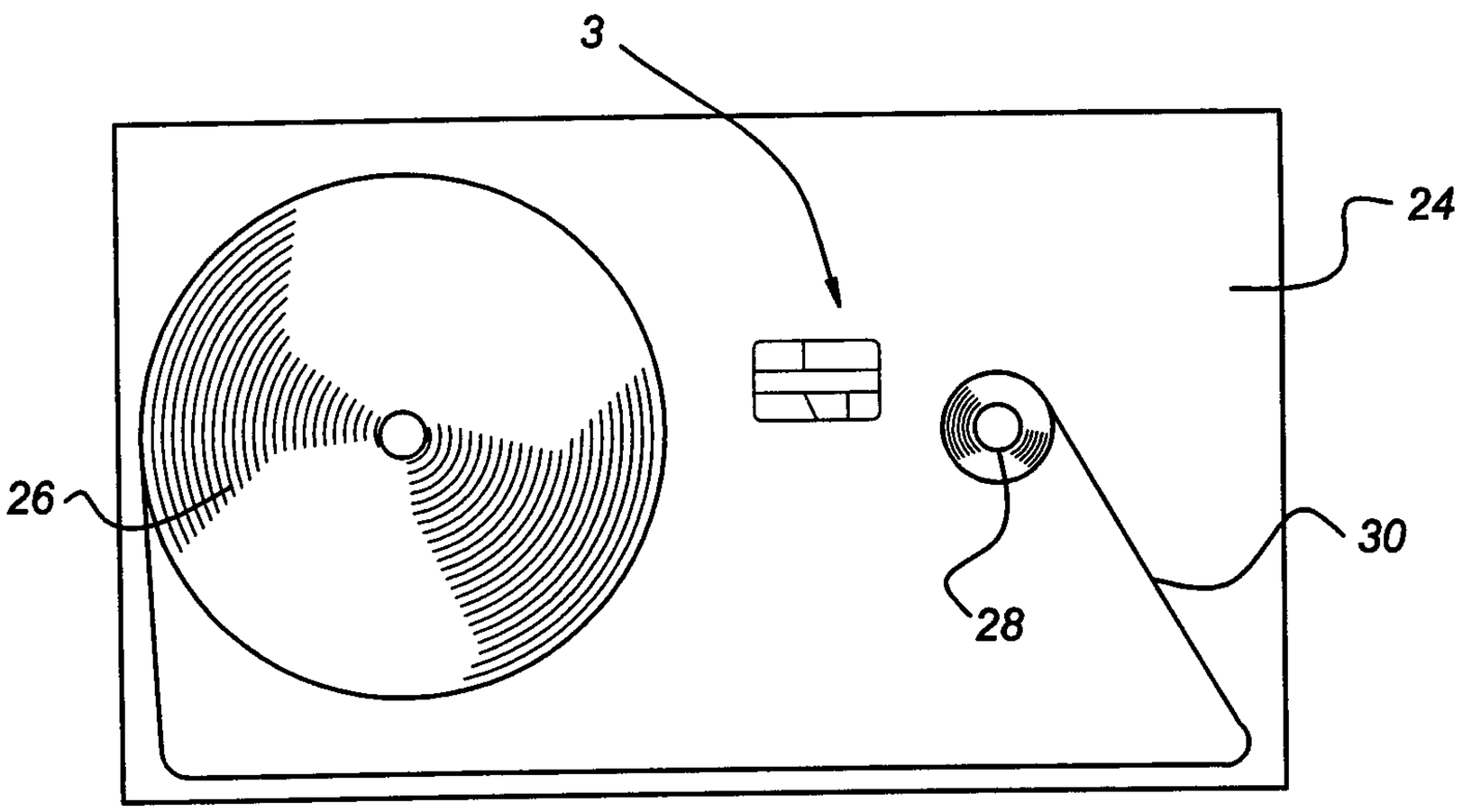


Fig 4

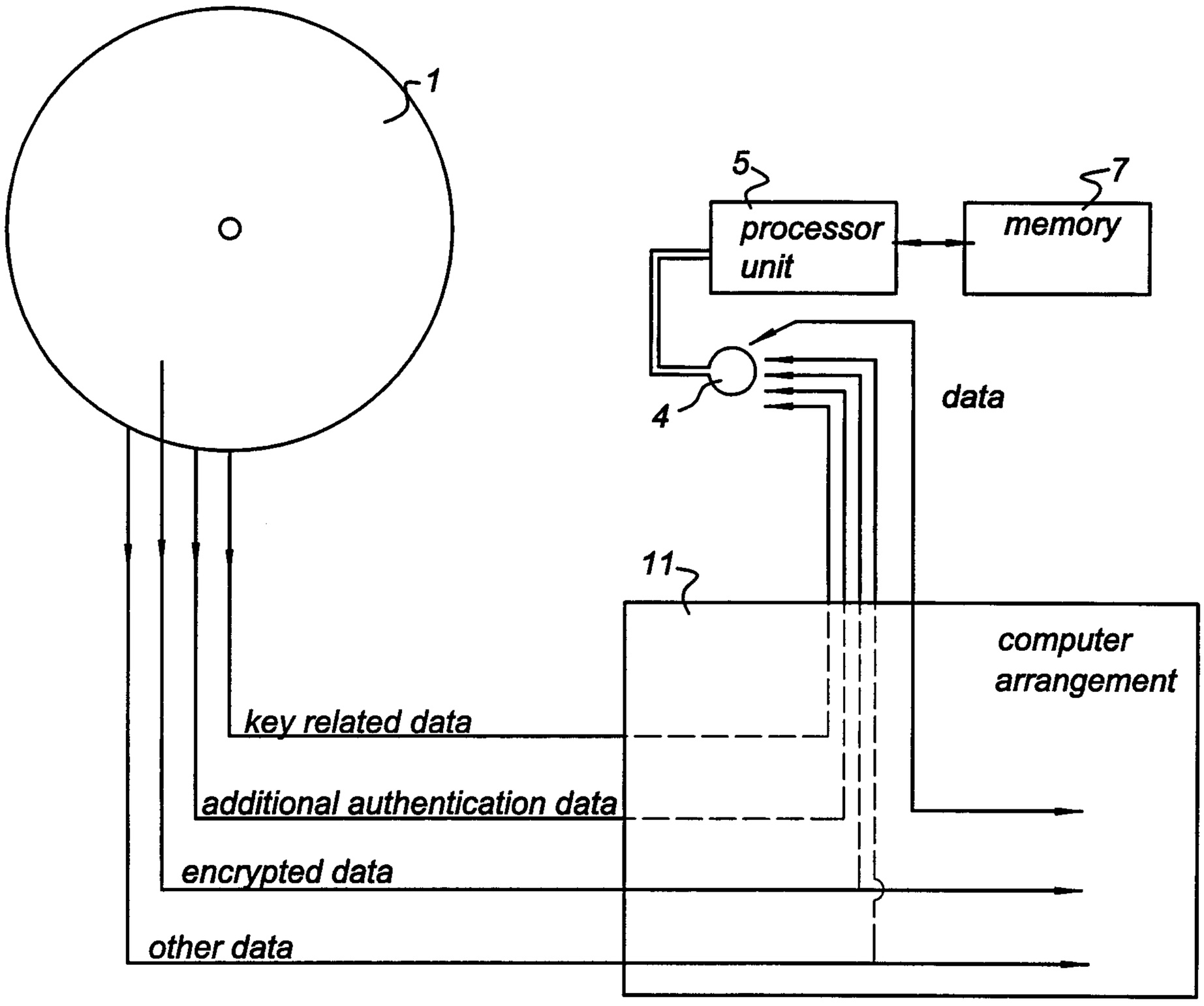

1
5
processor unit
7
memory
4
data
11
computer arrangement
key related data
additional authentication data
encrypted data
other data

Fig 5

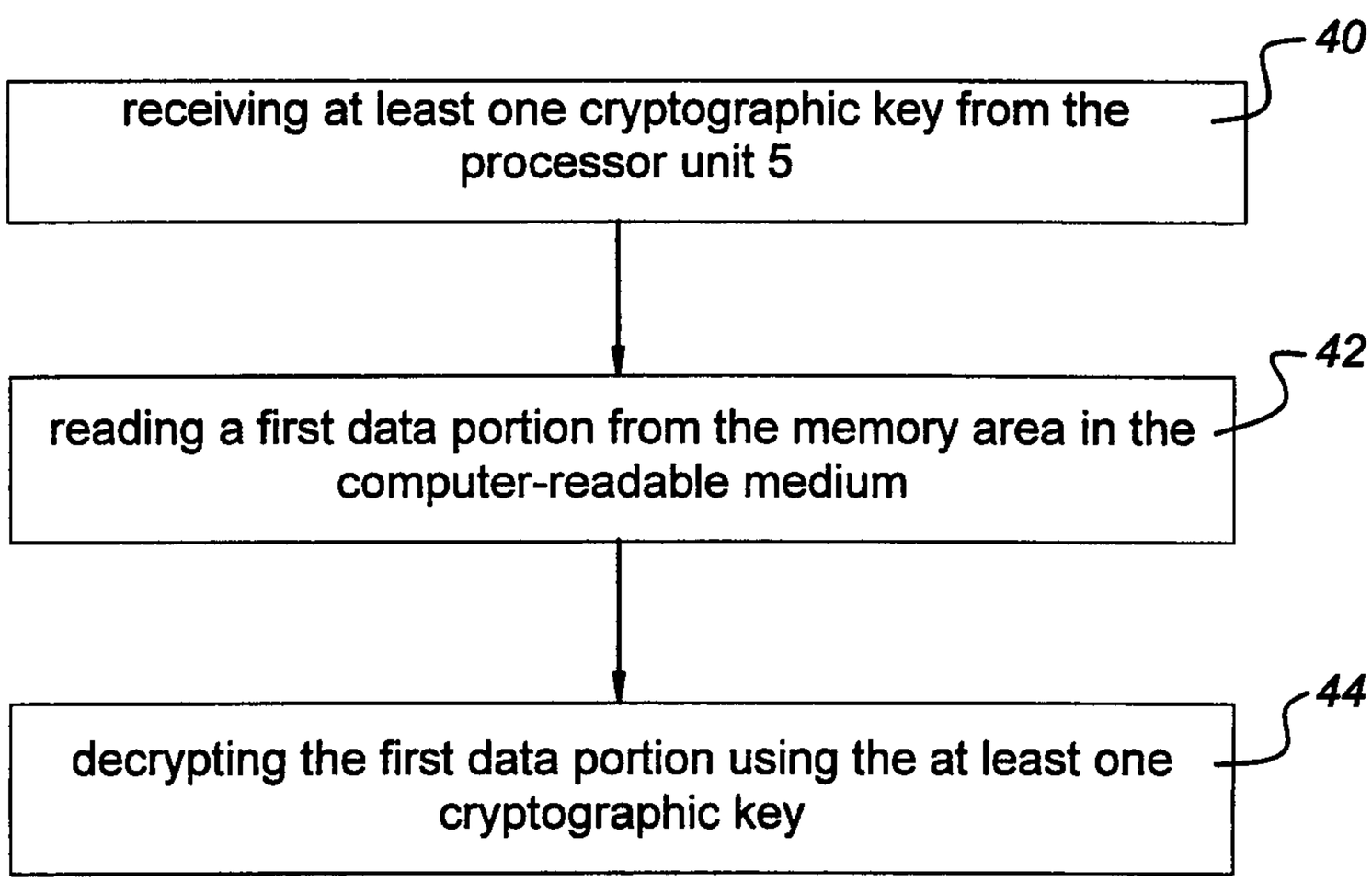
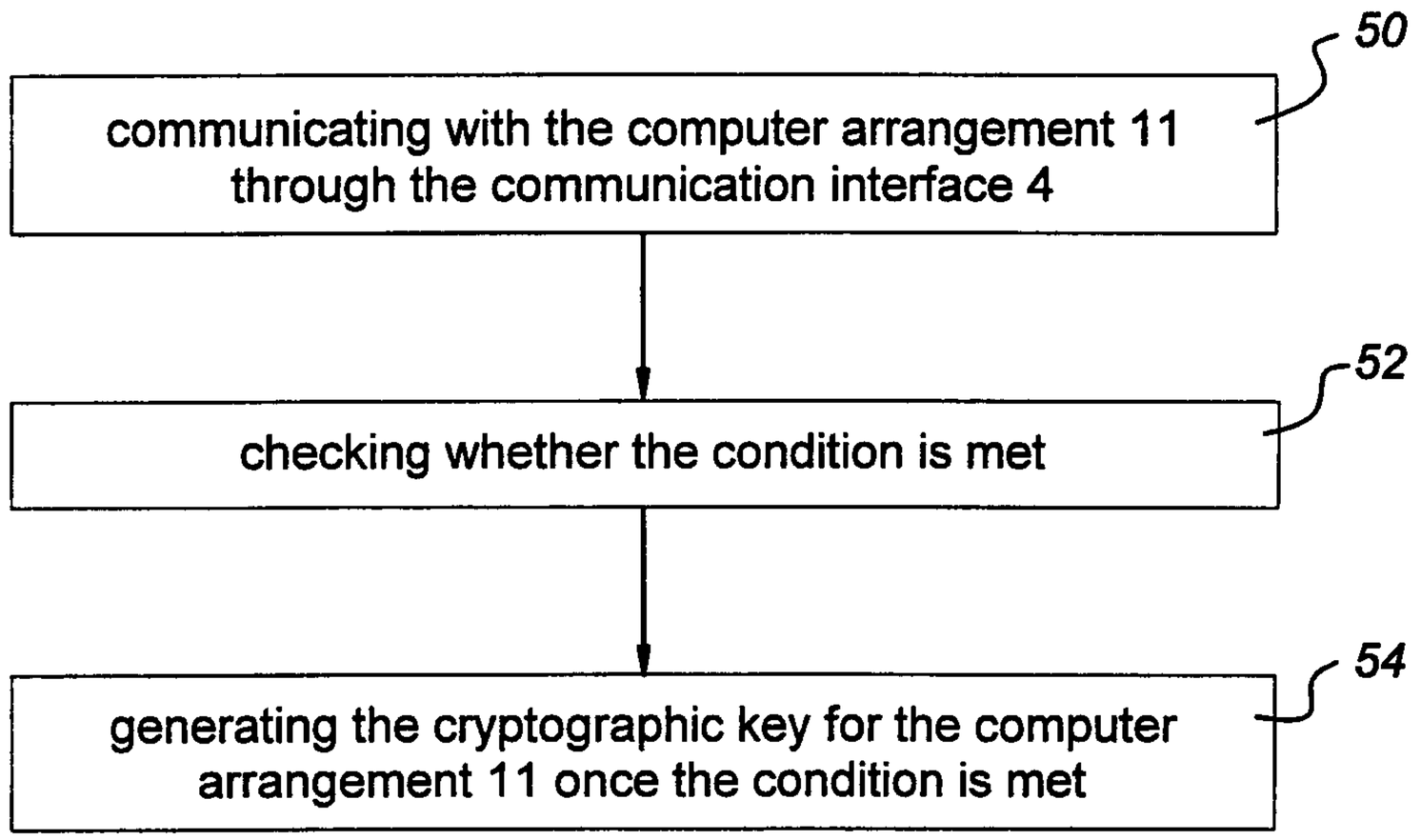
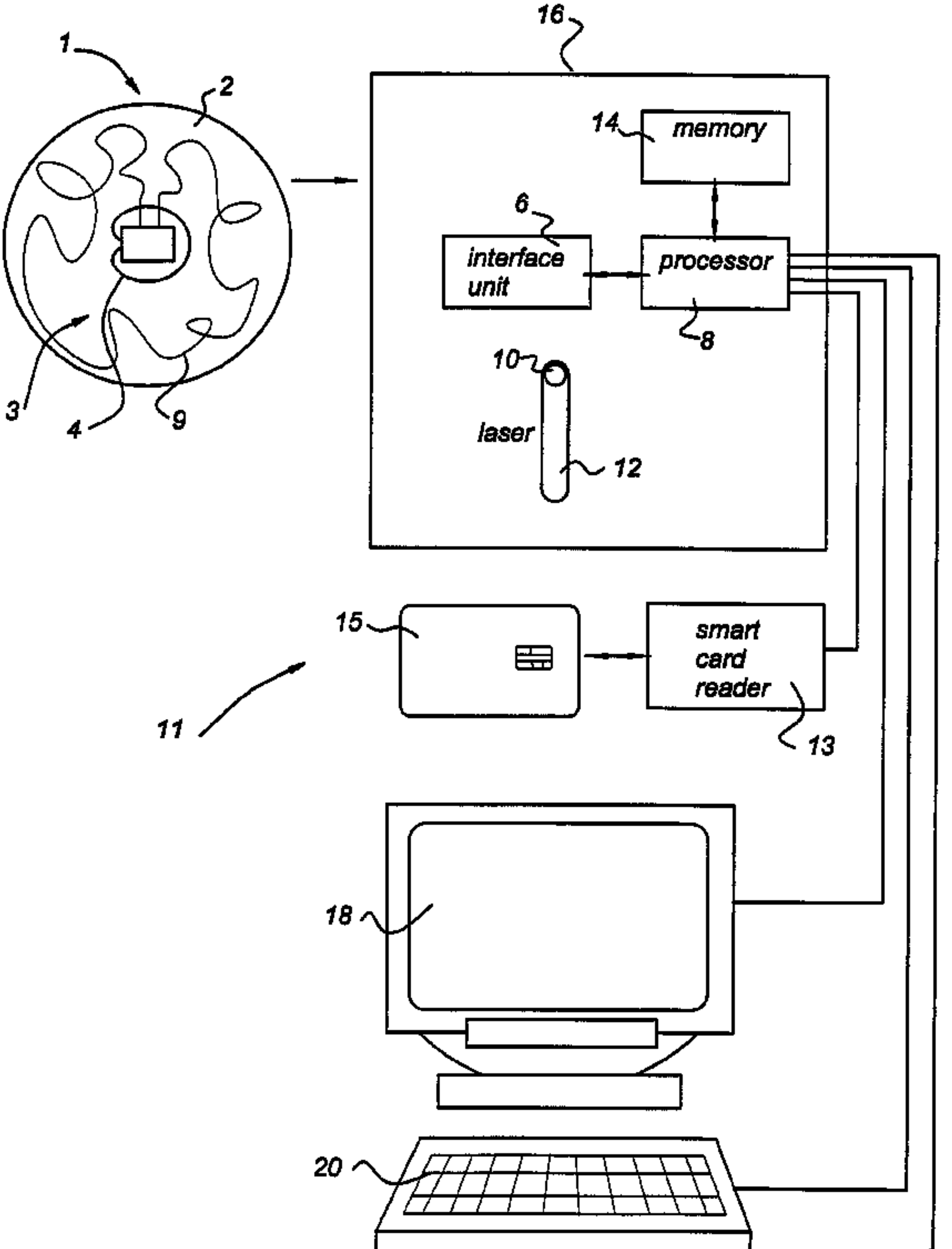

receiving at least one cryptographic key from the processor unit 5
40
reading a first data portion from the memory area in the computer-readable medium
42
decrypting the first data portion using the at least one cryptographic key
44

Fig 6


communicating with the computer arrangement 11 through the communication interface 4
50
checking whether the condition is met
52
generating the cryptographic key for the computer arrangement 11 once the condition is met
54


1
2
3
4
9
16
14
memory
6
interface unit
processor
8
10
laser
12
15
11
smart card reader
13
18
20
22