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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/69353 A1

(51) International Patent Classification⁷: G06F 1/00, H04L 9/32, G06F 17/30

(21) International Application Number: PCT/SE01/00515

(22) International Filing Date: 12 March 2001 (12.03.2001)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
0000871-4 13 March 2000 (13.03.2000) SE

(71) Applicant and
(72) Inventor: VESTGÖTE, Örjan [SE/SE]; Doktorsvägen 6, S-570 82 Målilla (SE).

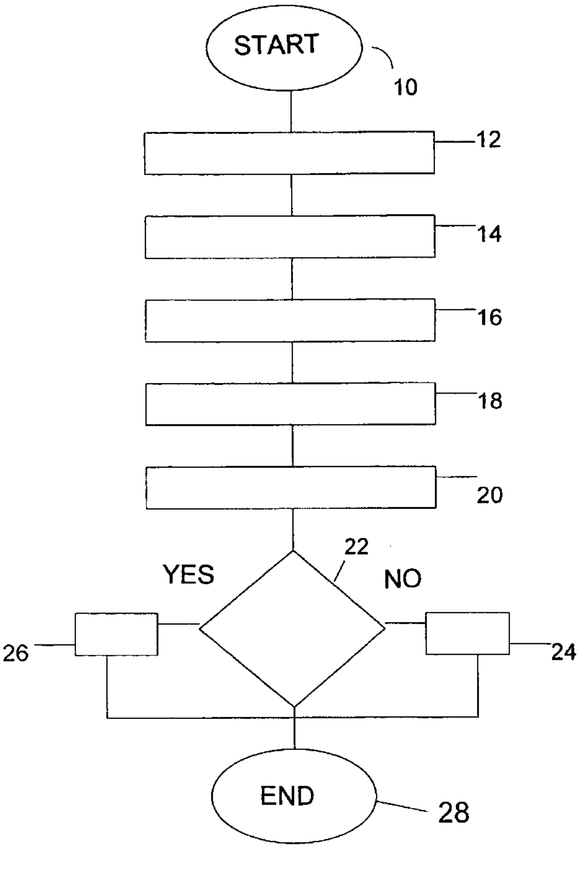
(74) Agents: ASKERBERG, Fredrik et al.; L.A. Groth & Co. KB, Box 6107, S-102 32 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), 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, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), 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, MZ, 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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A METHOD AND A SYSTEM FOR PREVENTING UNAUTHORISED USE OF COMPUTER PROGRAMS IN ELECTRONIC COMMERCE



(57) Abstract: The present invention relates to a method and a system for preventing unauthorised use of computer programs in electronic commerce. The method comprises the steps of: the user identifying himself to the sales point via the computer network; the sales point acknowledging the identification via the computer network; the user ordering a program via the computer network; the program ordered being downloaded into the user's computer; the program, upon execution, reading at least one code stored in a portable data carrier or in a memory in the user's computer and comparing this at least one code with a unique code for the program; and the program being terminated or one or more program functions in the program being unusable if the comparison step does not result in agreement between the codes compared; or the program being perfectly usable if the comparison step results in agreement between the codes compared.

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.

A METHOD AND A SYSTEM FOR PREVENTING UNAUTHORISED USE OF COMPUTER PROGRAMS IN ELECTRONIC COMMERCE

Technical field

The present invention relates in a first aspect to a method for preventing unauthorised use of computer programs downloaded into a computer from a computer network.

A second aspect of the present invention relates to at least one computer program product for preventing unauthorised use of programs downloaded into a computer from a computer network.

A third aspect of the present invention relates to a system for preventing unauthorised use of programs downloaded into a computer from a computer network.

Background art

Pirate-copying of software is carried on to a considerable extent nowadays. Pirate-copying entails software being copied and used by more users than is permitted by the user licence. It is estimated that more that 50% of all software is pirate-copied in one or more links. This naturally constitutes a major problem for the software industry.

Currently methods exist for protecting programs from illegal copying by connecting the program to a data carrier containing an identity or signature that is unique to the program. In order to function, the program must be able to read and approve the signature. The software and hardware are supplied to the customer together with documentation.

A considerable drawback with the known method mentioned above is the supply route from software manufacturer via printer (documentation), CD-ROM manufacturer, distributor, retailer to the final customer.

An arrangement is known through WO-97/03398 for protecting software against use without permission from the copyright owner.

By encrypting the program by means of a key (K1) that is separate from the key (K2) used for decoding, better protection is obtained against unauthorised use if the decoding key is kept secret from the user. Even better security is achieved by encrypting - decoding the communication between the computer in which the program is used and the external unit in which the decoding key is stored. The external unit is also arranged so that the host computer returns the result from its processing of data received from the host computer, which result is utilised in the further execution of the program in question.

JP-11-249892 shows a method to be already known for preventing pirate-copying of software. An empty licence database is automatically produced upon installation of a program to be distributed. For the purpose of using this program the licence information registered in a smart card is entered into the database. The program can only be run if the requisite licence is obtained from the database. The licence information is then registered on the smart card which has a CPU unit that cannot be physically reproduced. A drawback with this method is that the user's computer must be connected to the database when the program is started.

Through the patent US-A-5,919,247 a method is known for distributing code and data updates to thousands of customers via a network. The software applications are called "channels" and the client is called a "tuner". The use of channels is based on subscription. The end user must subscribe to the channel before it can be executed. When the end user subscribes to a channel, the appropriate code and the data set are downloaded to the local hardware, and once the channel has been downloaded it can be executed many times without requiring further access to the network. The channels can be regularly updated by the tuner and this means that the end user no longer needs to install software-updating manually. Instead these program and data updates occur automatically in the background.

None of the above-mentioned documents shows a simple and efficient solution to the problem mentioned above.

Summary of the invention

One object of the present invention is to solve the problems mentioned above. Another object of the present invention is to provide a secure way of selling/distributing software in electronic form via the Internet, for instance, and obtaining protection against pirate-copying.

In accordance with a first aspect of the present invention a method is provided for preventing unauthorised use of computer programs downloaded into a computer from a computer network. The method comprises the steps of:

- the user identifying himself to the sales/distribution point via the computer network;
- the sales/distribution point acknowledging the identification via the computer network;
- the user ordering a program via the computer network;
- the program ordered being downloaded into the user's computer;
- the program, upon execution, reading at least one code stored in a portable data carrier or in a memory in the user's computer and comparing this at least one code with a unique code for the program; and
- the program being terminated or one or more program functions in the program being unusable if the comparison step does not result in agreement between the codes compared; or
- the program being perfectly usable if the comparison step results in agreement between the codes compared. The principal advantage with this method is that it provides a secure way to sell/distribute software in electric form via the Internet, for instance. It also provides protection against pirate-copying.

It is an additional advantage if the method also comprises the steps of:

- downloading a formatting program from a host in the computer network; and
- the formatting program receiving information concerning one or more codes, and entering these into the data carrier.

An additional advantage in this context is obtained if the formatting program is associated with the host via a connection.

In this context it is an advantage if the connection is encrypted.

A further advantage is obtained in this context if the method also comprises the steps of:

- the user paying electronically for the program ordered; and
- the formatting program thereafter sending a status message to the host for the relevant order balance.

In accordance with a second embodiment the method also comprises the steps of:

- a formatting program accessible on a host in the computer network transmitting a data set to an encryption program;
- the encryption program encrypting or signing the data set and transmitting the

result to the formatting program; and

- the formatting program modifying a data-area (A) in a manner unique to the user, whereby each program is associated with a data-area (A).

In this context it is an advantage if the encryption program is arranged in the user's computer or in the data carrier, and if the encryption program encrypts or signs the data set with the aid of the user's code.

A further advantage is obtained in this context if the step of modifying a data-area (A) is performed by the formatting program entering the data set and the signature in the data-area (A).

In this context it is advantageous if, after the step of modifying the data-area (A), the step is performed of:

- downloading the program with the modified data-area (A) to the user's computer.

A further advantage is gained in this context if, after the step of downloading the program and the modified data-area (A), the step is performed of:

- the program decoding the data-area (A) by means of the user's code.

In accordance with another embodiment of the method, after the step of downloading the program and the modified data-area (A), the step is performed of:

- the program verifying the signature in the data-area (A).

In this context it is advantageous if, after the step of modifying the data-area (A), the steps are performed of:

- downloading the program to the user's computer;
- downloading the data-area (A) to the data carrier for comparison of whether the content in the data-area (A) agrees with the user's code.

A further advantage in this context is obtained if the encryption program is in communication with the formatting program by means of an encrypted connection.

In this context it is advantageous if the data-area (A) consists of a data file.

In accordance with another embodiment of the method the data-area (A) consists of a part of the program or the whole program.

In this context it is an advantage if the data-area (A) consists of a combination of the above-mentioned alternatives.

An additional advantage is obtained in this context if the user's code consists of a certificate.

In this context it is advantageous if the certificate consists of a public/private key.

An additional advantage is obtained in this context if the data carrier consists of a smart card.

In accordance with a further embodiment of the method the data carrier consists of an "iButton®".

Another object of the present invention is to provide at least one computer program product directly downloadable into the internal memory of at least one digital computer. The at least one computer program product comprises program code parts for performing the steps in the method in accordance with the present invention when said at least one product is run on said at least one computer. The principal advantage with the computer program product(s) in accordance with the present invention is that it/they provide(s) a secure way of selling/distributing software in electric form via the Internet, for instance. It/they also provide(s) protection against pirate-copying.

Another object of the present invention is to provide a system for preventing unauthorised use of programs downloaded into a computer from a computer network. The system comprises a computer network having at least one memory unit comprising various programs, each program including a code unique to that particular program. The system also comprises at least one computer, each computer being dedicated a user, and at least one portable data carrier, each data carrier being dedicated a user. The system also comprises one comparator per program, whereby a program ordered by a user is downloaded into the user's computer and, upon execution of said program, reads the at least one code stored in the data carrier or in a memory in the user's computer, whereupon the comparator compares this at least one code with the code unique to the program. The program is terminated or one or more program functions in the program cannot be used if the comparison does not result in agreement between the codes compared. On the other hand, the program can be fully utilised if the comparison results in agreement between the compared codes. The principal advantage with this system is that it provides a secure way of selling/distributing software in electronic form via the Internet, for instance. It also provides protection against pirate copying.

In this context it is advantageous if each memory unit in the computer network is a host from which a formatting program can be downloaded to the user's computer, which formatting program receives information about one or more codes and enters these into the data carrier.

An additional advantage in this context is if the formatting program is associated with the host via an encrypted connection.

In accordance with an additional embodiment of the system each memory unit in the computer network is a host comprising a formatting program that can transmit a data set to an encryption program arranged in the user's computer or in the data carrier which can encrypt or sign the data set with the aid of the user's code and transmit the result to the formatting program which can modify a data-area (A) in a manner unique to the user, each program being associated with a data-area (A).

It is in this context advantageous if the formatting program in the host modifies the data-area (A) by entering the data set and signature into the data-area (A), whereafter the program and the modified data-area (A) are downloaded to the user's computer, whereafter the program decodes the data-area (A) or verifies the signature in the data-area (A) by means of the user's code.

In accordance with a further embodiment of the system the formatting program in the host modifies the data-area (A) by entering the data set and signature into the data-area (A), whereafter the user's computer downloads the program from the host, whereafter the program and the modified data-area (A) are downloaded to the data carrier, whereupon the comparator compares whether the content in the data-area (A) is in agreement with the user's code.

It is in this context advantageous if the data carrier consists of a smart card.

In accordance with a further embodiment of the system the data carrier consists of an "iButton®".

It should be emphasised that when the term "comprise(s)" is used in this description, it should be interpreted as indicating the presence of the stated feature, step or component but not excluding the presence of one or more other feature, step, component or group thereof.

Brief description of the drawings

The embodiments in accordance with the invention will now be described with reference to the accompanying drawings, in which

Figure 1 is a flowchart for a method for preventing unauthorised use of programs downloaded into a computer from a computer network, in accordance with the invention;

Figure 2 shows a diagrammatic representation of some computer program products in accordance with the present invention, and;

Figure 3 shows a block diagram of a system for preventing unauthorised use of programs downloaded into a computer from a computer network, in accordance with the invention.

Detailed description of embodiments

Figure 1 shows a flowchart for a method for preventing unauthorised use of programs downloaded into a computer from a computer network. The method starts at block 10. At block 12 the method continues with the step of: the user identifying himself to the sales/ distribution point via the computer network. The method continues at block 14 with the sales point acknowledging the identification via the computer network. The next step, at block 16, comprises the user ordering a program via the computer network. The method continues at block 18 with the program ordered being downloaded into the user's computer. The next step, at block 20, comprises the program, upon execution, reading at least one code stored in a portable data carrier or in a memory in the user's computer and comparing this at least one code with a unique code for the program, as can be seen at block 22. In the event of a negative answer the method continues to block 24 which results in the program being terminated or one or more program functions in the program being unusable. If the answer is affirmative, however, the method will continue to block 26 and results in the program being perfectly usable, i.e. it can be fully executed. The method is then concluded at block 28. Naturally these steps can be repeated several times if a user wishes to order several different programs on different occasions, for instance.

In accordance with a first embodiment of the method according to the present invention, the user has a data carrier that can be entered and read by programs in the user's computer. The data carrier may be a fixed or a movable memory unit, e.g. a fixed or portable hard disk, a floppy disk or a smart card, or some other type of memory unit e.g. "iButton®" or iKey®. An iButton® is a portable unit provided with a microprocessor and a memory. The memory may be of ROM type or a read/write memory. The unit may also be provided with other functions such as various types of encrypting functions. An iButton® can be connected to the serial or parallel port of a computer. An iKey® comprises in principle functionally equivalent parts to an iButton®, but can be connected to the USB (Universal Serial Bus) of a computer. Each iButton® or iKey® also has an exclusive identity. A code/ signature for each program to be protected is entered into the data carrier. Each data carrier may contain one or more codes/signatures. Programs for sales or distribution are available from a host in the computer network for downloading to the user's computer. The host may be either a server or a client computer. A server often differs from the hardware aspect from the client computers. The difference may be, for instance, that the server has a reserve current supply with automatic current switching, so-called UPS (Uninterruptible Power Supply), large disk memories, magnetic band unit, etc. The host is also provided with a formatting program designed for downloading to and execution on the user's computer. The formatting program is in communication with the host via a connection, which may be encrypted. When the user has been approved by the host, e.g. after payment for software ordered, the formatting program receives information as to which code/ signature shall be entered into the data carrier. The formatting program then enters one or more signatures into the data carrier. When the program is executed it attempts to enter "its" code/signature in the data carrier. If the correct code/signature is not found, the program is terminated or one or more functions will not be available in the program. The formatting program can also send status messages to the host to count down the customer's order balance, for instance.

In accordance with a second embodiment of the method according to the present invention the use has a code/certificate stored on the hard disk of the user's computer or in a special data carrier that can be written and read by programs in the user's computer. A data-area A exists for each program for sales/distribution. The programs are available at a host in the computer network for downloading to the user's computer. A formatting program is also on the host, designed to modify the data-area (A) in a manner unique to the user. In the user's computer or in the data carrier is an encryption program which can encrypt or sign a data set received. The encryption program in the data carrier or in the user's computer is in communication with the formatting program in the host. This connection may be encrypted. When the user is approved by the host, e.g. when the program ordered has been paid for, the formatting program transmits a data set to the encryption program. The encryption program encrypts or signs the data set using the user's code/certificate, and sends the data set and signature back to the formatting program. The formatting program enters the data set and signature into the data-area A. The program is then downloaded to the user's computer together with the data-area A. With the aid of the user's code/certificate the program can decode the data-area A or verify the signature in the data-area A. Alternatively the data-area A can be sent to the data carrier for corresponding operation or check that the content in the data-area A matches the user's code/certificate. If the signature does not match the code/certificate the program will be terminated or one or more programs will be unavailable in the program. The code/ certificate may be a public/private key, for instance. The data carrier may be a fixed or movable memory unit, e.g. a fixed or portable hard disc, a floppy disk or a smart card, or some other type of memory unit e.g. "iButton®" or iKey®. An iButton® is a portable unit provided with a microprocessor and a memory. The memory may be of ROM type or a read/write memory. The unit may also be provided with other functions such as various types of encrypting functions. An iButton® can be connected to the serial or parallel port of a computer. An iKey® comprises in principle functionally equivalent parts to an iButton®, but can be connected to the USB (Universal Serial Bus) of a computer. Each iButton® or iKey® also has an exclusive identity.

Figure 2 shows a schematic representation of some computer program products in accordance with the invention. Figure 2 shows n different digital computers 100_1, ..., 100_n, where n is an integer. It also shows n different computer program 102_1, ..., 102_n, illustrated here as CDs. These computer program products 102_1, ..., 102_n, may be any type of computer-readable medium, such as floppy disks, smart cards or the like. The various computer program products 102_1, ..., 102_n, can be downloaded directly into the internal memory of the various digital computers 100_1, ..., 100_n. Each computer program product comprises program code parts to perform certain or all the steps in accordance with Figure 1 when the product(s) is/are run in said computers.

Figure 3 shows a block diagram of a system for preventing unauthorised use of programs downloaded into a computer from a computer network, in accordance with the invention. The system 30 comprises a computer network 32 having at least one memory unit 34. The memory unit(s) 34 comprise(s) various programs 36 for sale/distribution. Each program 36 includes a unique code. The system 30 also comprises at least one computer 38, each computer 38 being dedicated a user. Figure 3 shows n different computers 38_1, ..., 38_n. The system 30 also comprises at least one data carrier 40, each data carrier being dedicated a user. Figure 3 shows n different data carriers 40_1, ..., 40_n. The system also comprises one comparator 42 (for the sake of simplicity only one is shown) per program 36. A program 36 ordered by a user is downloaded into the user's computer 38 and, upon execution of said program 36, reads the at least one code stored in the data carrier 40 or in a memory in the user's computer 38, whereupon the comparator 42 compares this at least one code with the code unique to the program 36. The program 36 is terminated or one or more program functions in the program 36 cannot be used if the comparison does not result in agreement between the codes compared. However, the program 36 can be fully utilised if the comparison results in agreement between the compared codes.

The system 30 in accordance with the present invention can function, for instance, in accordance with the two embodiments described above in conjunction with Figure 1.

The invention is not limited to the embodiments described above. It is obvious to one skilled in the art that many different modifications are possible within the scope of the appended claims.

CLAIMS

1. A method for preventing unauthorised use of programs downloaded into a computer from a computer network, which method comprises the steps of:

- the user identifying himself to the sales point via the computer network;
- the sales point acknowledging the identification via the computer network;
- the user ordering a program via the computer network;
- the program ordered being downloaded into the user's computer;
- the program, upon execution, reading at least one code stored in a portable data carrier or in a memory in the user's computer and comparing this at least one code with a unique code for the program; and
- the program being terminated or one or more program functions in the program being unusable if the comparison step does not result in agreement between the codes compared; or
- the program being perfectly usable if the comparison step results in agreement between the codes compared.

2. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 1, **characterized** in that the method also comprises the steps of:

- downloading a formatting program from a host in the computer network; and
- the formatting program receiving information concerning one or more codes, and entering these into the data carrier.

3. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 2, **characterized** in that the formatting program is associated with the host via a connection.

4. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 3, **characterized** in that the connection is encrypted.

5. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 2-4, **charac-**

terized in that the method also comprises the steps of:

- the user paying electronically for the program ordered; and
- the formatting program thereafter sending a status message to the host for the relevant order balance.

6. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 1, **characterized** in that the method also comprises the steps of:

- a formatting program accessible on a host in the computer network transmitting a data set to an encryption program;
- the encryption program encrypting or signing the data set and transmitting the result to the formatting program; and
- the formatting program modifying a data-area (A) in a manner unique to the user, whereby each program is associated with a data-area (A).

7. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 6, **characterized** in that the encryption program is arranged in the user's computer or in the data carrier, and in that the encryption program encrypts or signs the data set with the aid of the user's code.

8. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 7, **characterized** in that the step of modifying a data-area (A) is performed by the formatting program entering the data set and the signature in the data-area (A).

9. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 8, **characterized** in that after the step of modifying the data-area (A) the step is performed of:

- downloading the program with the modified data-area (A) to the user's computer.

10. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 9, **characterized** in that

after the step of downloading the program and the modified data-area (A) the step is performed of:

- the program decoding the data-area (A) by means of the user's code.

11. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 9, **characterized** in that after the step of downloading the program and the modified data-area (A) the step is performed of:

- the program verifying the signature in the data-area (A).

12. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 8, **characterized** in that after the step of modifying the data-area (A) the steps are performed of:

- downloading the program to the user's computer;
- downloading the data-area (A) to the data carrier for comparison of whether the content in the data-area (A) agrees with the user's code.

13. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 6-12, **characterized** in that the encryption program is in communication with the formatting program by means of an encrypted connection.

14. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 6-13, **characterized** in that the data-area (A) consists of a data file.

15. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 6-13, **characterized** in that the data-area (A) consists of a part of the program or the whole program.

16. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 14-15, **characterized** in that the data-area (A) consists of a combination of the alternatives

defined in claims 14 and 15.

17. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 6-16, **characterized** in that the user's code consists of a certificate.

18. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in claim 17, **characterized** in that the certificate consists of a public/private key.

19. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 1-18, **characterized** in that the data carrier consists of a smart card.

20. A method for preventing unauthorised use of programs downloaded into a computer from a computer network as claimed in any one of claims 1-18, **characterized** in that the data carrier consists of an "iButton".

21. At least one computer program product (102_1, ..., 102_n) directly downloadable into the internal memory of at least one digital computer (100_1, ..., 100_n), comprising program code parts for performing the steps claimed in claim 1 when said at least one product (102_1, ..., 102_n) is run on said at least one computer (100_1, ..., 100_n).

22. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, which system comprises a computer network having at least one memory unit comprising various programs, **characterized** in that each program includes a code unique to that program, which system also comprises at least one computer, each computer being dedicated a user, and at least one portable data carrier, each data carrier being dedicated a user, which system also comprises one comparator per program, whereby a program ordered by a user is downloaded into the user's computer and, upon execution of said program, reads the at least one code stored in the data carrier or in a memory in the user's computer, whereupon the comparator compares this at least one code

with the code unique to the program, whereupon the program is terminated or one or more program functions in the program cannot be used if the comparison does not result in agreement between the codes compared, or that the program can be fully utilised if the comparison results in agreement between the compared codes.

23. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, as claimed in claim 22, **characterized** in that each memory unit in the computer network is a host from which a formatting program can be downloaded to the user's computer, which formatting program receives information about one or more codes and enters these into the data carrier.

24. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, as claimed in claim 22, **characterized** in that the formatting program is associated with the host via an encrypted connection.

25. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, as claimed in claim 22, **characterized** in that each memory unit in the computer network is a host comprising a formatting program that can transmit a data set to an encryption program arranged in the user's computer or in the data carrier which can encrypt or sign the data set with the aid of the user's code and transmit the result to the formatting program which can modify a data-area (A) in a manner unique to the user, each program being associated with a data-area (A).

26. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, as claimed in claim 25, **characterized** in that the formatting program in the host modifies the data-area (A) by entering the data set and signature into the data-area (A), whereafter the program and the modified data-area (A) are downloaded to the user's computer, whereafter the program decodes the data-area (A) or verifies the signature in the data-area (A) by means of the user's code.

27. A system for preventing unauthorised use of programs downloaded into a

computer from a computer network, as claimed in claim 25, **characterized** in that the formatting program in the host modifies the data-area (A) by entering the data set and signature into the data-area (A), whereafter the user's computer downloads the program from the host, whereafter the program and the modified data-area (A) are downloaded to the data carrier, whereafter comparator compares whether the content in the data-area (A) is in agreement with the user's code.

28. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, as claimed in any of claims 22-27, **characterized** in that the data carrier consists of a smart card.

29. A system for preventing unauthorised use of programs downloaded into a computer from a computer network, as claimed in any of claims 22-27, **characterized** in that the data carrier consists of an "iButton".

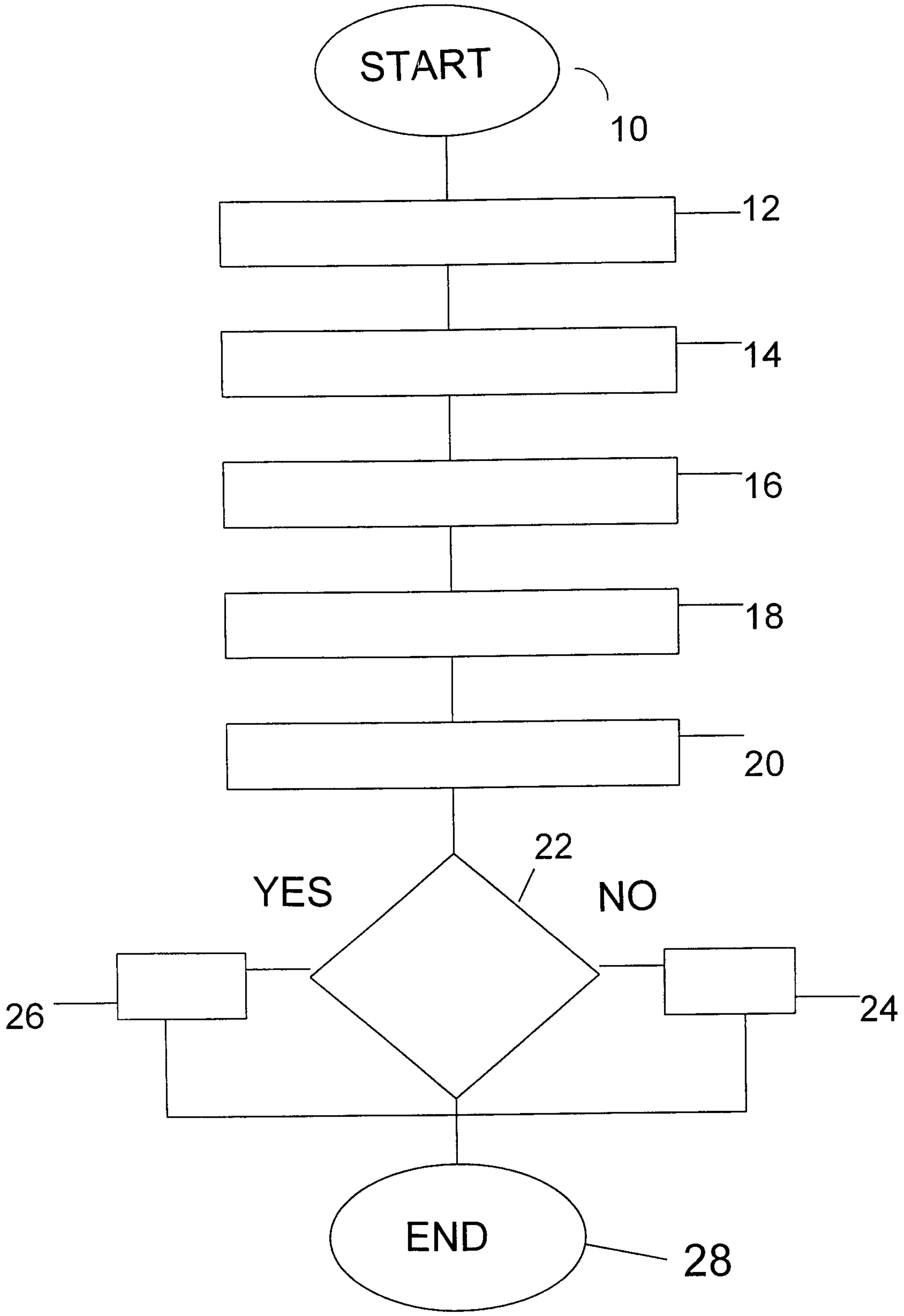


Fig 1

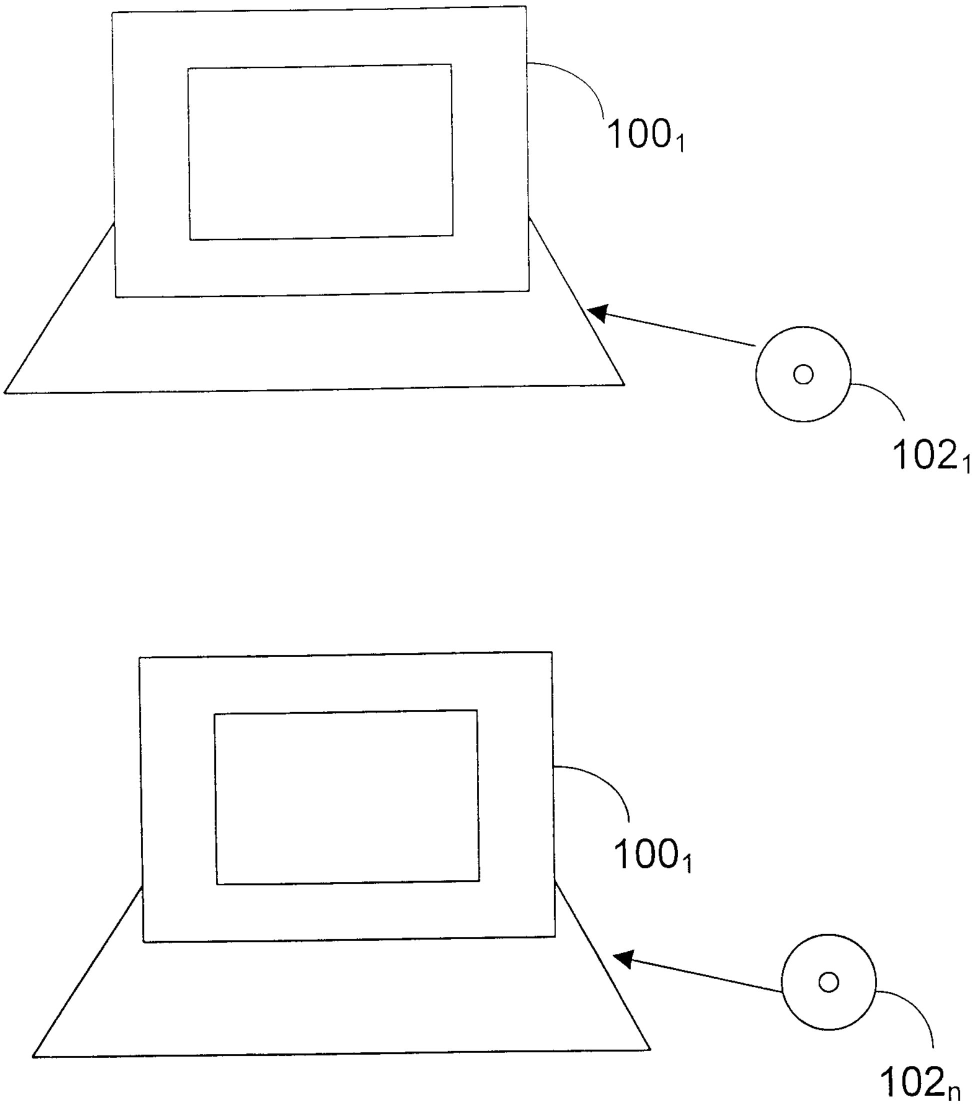


Fig 2

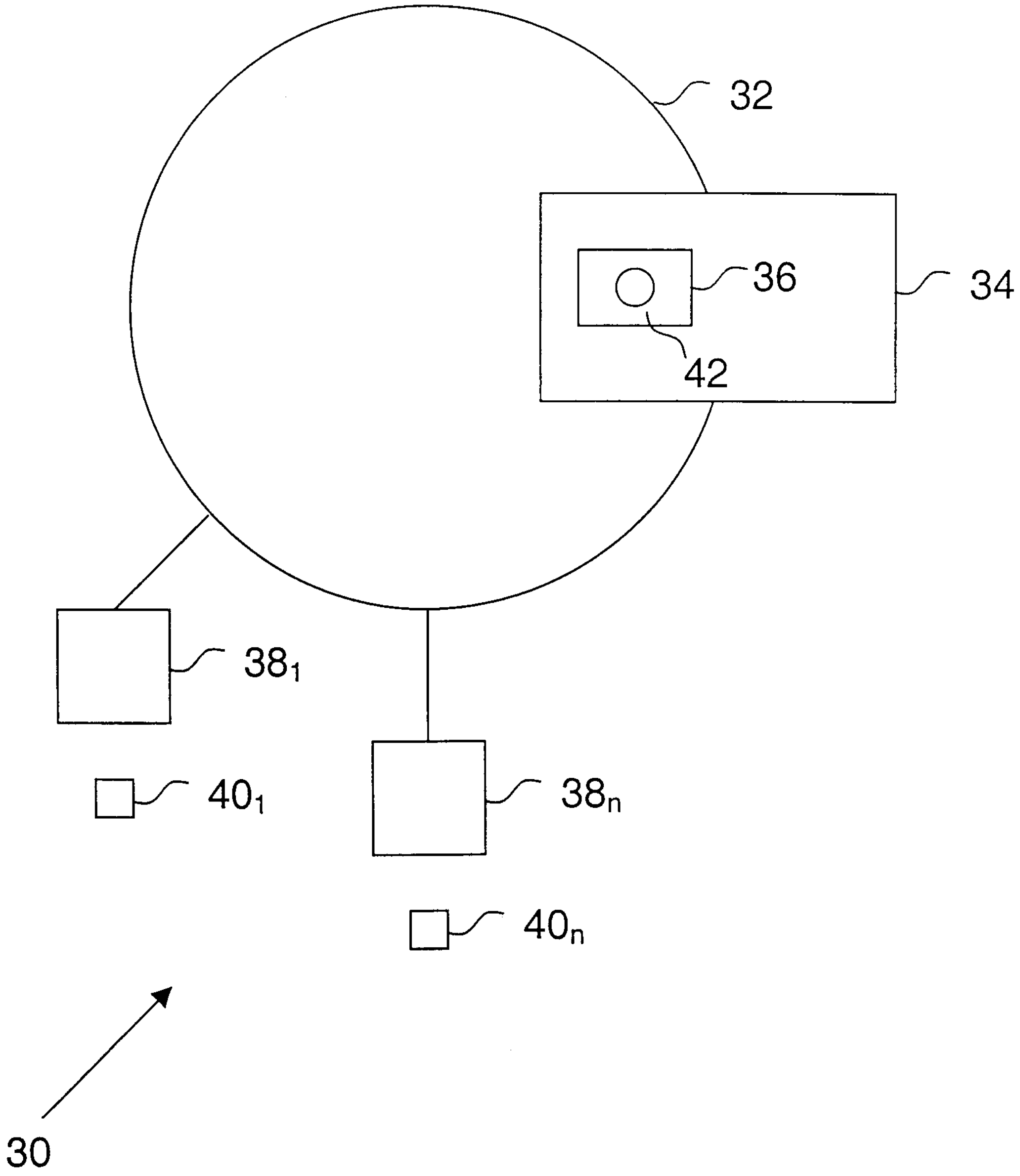


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/00515

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, H04L 9/32, G06F 17/30
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)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI-DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5337357 A (CHOU ET AL.), 9 August 1994 (09.08.94), column 1, line 56 - column 2, line 3; column 3, line 48 - column 4, line 3, figure 1, claim 1, abstract	1-5,21-24
Y		6-18,25-27
	--	
X	WO 9703398 A1 (SIGBJØRNSEN, SIGURD), 30 January 1997 (30.01.97), page 4, line 15 - page 5, line 2; page 7, line 22 - line 23, figures 1,7,9, claim 25, abstract	19-20,28-29
Y		6-18,25-27
	--	

☒ 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 application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 15 May 2001	Date of mailing of the international search report 12 -06- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Pär Heimdal /OGU Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/00515

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5398285 A (BORGELT ET AL.), 14 March 1995 (14.03.95), column 2, line 22 - line 52; column 4, line 5 - line 27, figure 2, claim 1, abstract	1,21,22
A		2-20,23-29
	--	
X	US 5982889 A (DEMONT), 9 November 1999 (09.11.99), column 1, line 63 - column 2, line 16; column 11, line 25 - line 42, claim 1, abstract	1,21,22
A		2-20,23-29
	--	
X	US 5982892 A (HICKS ET AL.), 9 November 1999 (09.11.99), column 1, line 29 - column 2, line 17, figures 1-2, claim 1, abstract	1,21,22,
A		2-20,23-29
	--	
A	US 5651064 A (NEWELL), 22 July 1997 (22.07.97), column 2, line 5 - line 46, claim 1, abstract	1-29
	--	

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/04/01

International application No.
PCT/SE 01/00515

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5337357 A	09/08/94	CA 2120816 A	18/12/94
		EP 0636962 A	01/02/95
WO 9703398 A1	30/01/97	AU 713872 B	09/12/99
		AU 6535796 A	10/02/97
		CA 2226386 A	30/01/97
		CN 1192814 A	09/09/98
		EP 0855052 A	29/07/98
		IL 122888 D	00/00/00
		JP 11509023 T	03/08/99
		NO 302388 B	23/02/98
		NO 952795 A	14/01/97
		NZ 313319 A	28/10/99
		PL 324525 A	08/06/98
US 5398285 A	14/03/95	NONE	
US 5982889 A	09/11/99	US 6173403 B	09/01/01
US 5982892 A	09/11/99	NONE	
US 5651064 A	22/07/97	NONE	