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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2007 (07.09.2007)

PCT

(10) International Publication Number
WO 2007/100267 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/PL2007/000009

(22) International Filing Date: 2 March 2007 (02.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

P-379085	2 March 2006 (02.03.2006)	PL
P-379095	3 March 2006 (03.03.2006)	PL
P-379096	3 March 2006 (03.03.2006)	PL

(71) Applicants and
(72) Inventors: **GAWRUK, Mariusz** [PL/PL]; ul. Bohaterow Warszawy 45/20, PL-11-200 Bartoszyce (PL). **CHECHLOWSKI, Krzysztof** [PL/PL]; ul. Poznanska 28, PL-62-051 Leczyca (PL). **GOSIENIECKI, Lukasz** [PL/PL]; ul. Fiedlera 12, PL-62-041 Puszczykowo (PL).

(74) Agent: **PLOTCZYK, Leokadia**; Polservice Kancelaria Rzeczników Patentowych Sp. z o. o., ul. Bluszczanska 73, PL-00-712 Warszawa (PL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:
— *without international search report and to be republished upon receipt of that 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.

(54) **Title:** METHOD, CARRIER, KEY AND SYSTEM TO SECURE AND READ SECURED DATA

(57) **Abstract:** A method of securing data on an information carrier in which a capacity of a total memory R of an information carrier, a data memory capacity for data to be secured on an information carrier, a capacity W of an unoccupied data memory part on an information carrier are determined; a verification key is determined, wherein such a key contains information concerning information carrier memory; data are saved on an information carrier. The information carrier containing the secured data, characterised in that it has a total capacity and an occupied memory part capacity of the information carrier, herein the total memory capacity R is a sum of the occupied memory part capacity D and the unoccupied memory part capacity W, wherein the data secured in the information carrier can be read with the help of the technical device serving to authorize access to the data and the verification key, wherein the verification key contains information on the memory of the information carrier.

WO 2007/100267 A2

Method, carrier, key and system to secure and read secured data

Field of the invention

The object of the invention is: a method of securing data on an information carrier, a method of authorizing access to a secured device, a method of reading of data secured on an information carrier, an information carrier containing secured data, an information carrier authorizing access to a secured device, a technical instrument (or „technical means") for authorizing access to data, a technical instrument designed to secure data, a secured device designed to authorize access, an encoding and verifying key, a verifying key, a system containing secured data, a system to secure and read secured data, a system to authorize communication between devices and a system for authorization of a secured device.

Description of the state of the art

Presently in the field of technology there are known various solutions for securing data on information carriers. For example according to a European patent application EP 1 538 529 A1 an information carrier was released in which a verification key is saved. Under American Patent Specification 6,789,177 B2 a solution for authorization of access to secured data by way of a method of identification of an original carrier was presented. Another patent worth mentioning here is a US patent US 6,882,987 B2, which describes a method of securing copied data against reading, where a verification key is used, a key containing „specific information", which according to American Patent

individual information carriers. Such a solution is, however, troublesome to manufacture serially. Therefore a technological problem ensues: considering on the one hand the specific aspect of individual information carriers and on the other hand the need to ensure their mass production, to establish what information contained in an verification key can be best used for securing data.

The goal of the invention is to find a way to secure data in an information carrier in such a way that a verification key contains best possible information on a carrier in which data are secured against unauthorized access. The purpose of the invention is also to prepare a method of reading data secured in such a manner and a method to read a carrier, to prepare a technical instrument (or „technical means") serving to authorize access to data, and further to prepare a verification key and a system bearing data secured in such way.

The gist of the invention

The object of the invention is a method to secure data on an information carrier, by which a method the total memory capacity R of the information carrier is determined. Also a capacity of a memory of data to be secured on an information carrier is determined. Further, a capacity of the unoccupied memory part W of an information carrier is determined. Next an encoding and verifying key containing information about a memory of an information carrier is determined. Finally, data are saved in an information carrier. However, the sequence of individual steps as presented above can be different. It is also advantageous to determine the capacity D of the occupied memory part D of an information carrier.

"Information carrier" can mean every structurally separate part of an information carrier memory which can be perceived as an independent member having a total capacity. A memory understood in such a manner means that a given information carrier can consist of a number of memories (e.g. hard disc partitions, independent layers of optical information carriers etc.)

A total memory capacity R is deemed to be a capacity of a memory of a carrier in which utility data, or a given information carrier memory capacity containing utility data or other carriers own (specific) data (e.g. resulting from carriers specifics, its standard features etc.) can be saved. The capacity of a memory, which will be saved on an information carrier after saving data, can be different from the capacity of a memory necessary to save these data. This difference can result from the fact that apart from these data also data containing information on the carrier itself are saved on the disc. Additionally the disc can contain also a verification key or a technical instrument (most usually a computer programme) for data access authorization. It is important here for the capacity of a memory which will be saved on an information carrier to be determined in the same way as the total memory capacity of the information carrier was determined, i.e. if the total information carrier memory contains the carriers specific information, the memory capacity stored on the information carrier must comprise the carriers specific information as well. Identically, should the information carrier memory capacity not include the information carrier specific information, then also the capacity of a memory which will be saved on an information carrier shall not contain specific information on the carrier itself. Thus in both cases one will have the identical

capacity W of the unoccupied memory part of the information carrier.

It is of benefit when information about the information carrier memory include information on the capacity W of the unoccupied memory part of the information carrier. "The unoccupied memory part of information carrier" shall mean a part of memory where users will be able to store data at any time. Under certain circumstances an unoccupied memory part of an information carrier can also be understood as a memory part which a user cannot use. Such a case occurs with in particular optical information carriers of the CR-R, DVD-R, or DVD+R format. This happens due to the fact that after having saved data on an information carrier it "closes" thus making further data saving impossible, therefore, a part of the memory will remain empty. In a situation when a system to secure data will enable to determine the capacity of such an unoccupied memory (e.g. with the aid of special reader or other device to this purpose), both the way to secure data and the way to read them according to the invention, can be appropriately modified so that the capacity of the unoccupied memory W takes also into account - includes - the above defined unoccupied memory.

It is also of benefit when information on the information carrier memory contain information concerning the capacity D of the occupied memory of the information carrier. The capacity D of the occupied memory of an information carrier can include all data saved in this carrier including data which are secured, all data which constitute the disc's specific information, a verification key, a technical instrument to authorize data access etc. It is of benefit when information on the information carrier memory contain also information concerning the total capacity R of the carrier's memory. Information on the carrier's memory can

include all the above-mentioned parameters concerning the information carrier memory under any configuration. The total memory capacity R of the information carrier is in any case a sum of the capacity W of the unoccupied memory of the information carrier and the capacity D of the occupied memory of this carrier.

According to an advantageous version of the invention a verification key is saved on an information carrier, wherein this key can be saved along with data, which are the carrier's own specific information (e.g. the so-called Lead-in in case of optical information carriers). A verification key can also be saved within the section of secured data (even as selected parameters of secured utility data). A verification key can also be saved on an information carrier in such a manner that it is placed there as e.g. data saved on an external label (or other physical part of a carrier). According to other version of the invention a technical instrument for authorization of data access can also be saved on an information carrier. A verification key and a technical instrument serving to authorize the data access can be saved on an information carrier in parallel and independent of each other. According to one more version of the invention both a verification key and technical instrument serving to authorize access to data are saved on an external information carrier, i.e. on any memory not being a given information carrier (e.g. a computer memory, other information carrier etc.).

It is also of benefit when information on the memory of the information carrier included in the verification key is encoded.

The object of the invention is a method of securing data of a data memory capacity X on an information carrier having a total memory capacity R_1. In the first step the technical

instrument serving to secure data is activated, next, parameters of the encoding and verifying key are determined. The parameter of the encoding-verifying key is at least one of parameters determined by: the total memory capacity R_1 of the information carrier or the data memory capacity D_1 which will be saved on an information carrier or the capacity W_1 of the unoccupied memory part of an information carrier, which after saving data in the carrier will remain unoccupied. The relationship that the capacity R_1 of the total memory of an information carrier is a sum of the data memory capacity D_1 that will be saved on this information carrier and the capacity W_1 of the unoccupied memory of the information carrier after having saved data will remain unoccupied is fulfilled. Next parameters of the encoding-verifying key are determined and herein at least one of the three capacities is determined: the total memory capacity R1 of an information carrier or the data memory capacity D1 which will be saved on an information carrier or the capacity W1 of the unoccupied memory part of an information carrier which after saving data in the carrier will remain unoccupied. Next, data of the X capacity are encoded with the encoding-verifying key parameters and encoded are saved on the information carrier. After saving data in an information carrier the memory capacity of data saved on this carrier is D_1 and the capacity of the unoccupied memory of the information carrier after saving data is W_1. The sequence of the above-described steps can be, however, other than that.

The parameter of the enocoding-veryfying key can be a parameter determined by the total capacity R_1 of the information carrier. The parameter of the enocoding-veryfying key can also be a parameter determined by the data memory capacity D_1 that will be saved on the information carrier. In such a case prior to encoding it is necessary to determine *a*

priori the capacity D_1 of the data memory, which will be saved on an information carrier, as after encoding the data memory capacity X can change. For this reason it is advantageously predetermined that the data memory capacity D_1 which will be saved on an information carrier is larger than the data memory capacity X, thus enabling for the data capacity to be filled up after encoding to the required capacity D_1 with lacking bits (bytes). In a similar way the parameter of the enocoding-veryfying key can also be a parameter determined by the capacity W1 of the unoccupied memory of the information carrier, which after saving data will remain unoccupied. For the same reasons as described above also in this case it is necessary to determine *a priori* the capacity W_1 of the unoccupied memory of the information carrier which after saving data on the information carrier will remain unoccupied. All the said parameters can occur jointly under any possible combination.

Every structurally separated part of an information carrier, which can be perceived as an independent member having the total capacity T, can also be understood as an information carrier. Understanding a memory in such a way means that a given information carrier can consist of a number of memories (e.g. hard disc partitions, independent layers of optical information carriers etc.)

Memory capacities are expressed in memory units e.g. in bits or bytes. A total memory capacity R is deemed to be a capacity of a an information carrier in which utility data can be stored (therefore the information carrier data memory capacity, where carriers own data such as e.g. data on the carriers specifics, its standards like the so-called TOC - *Table of Contents* in case of optical carriers etc. are stored, is neglected). The capacity D of the data memory includes all the data, which will be saved on an information

carrier excluding data on the carrier's own specifics - carrier's specific features. For example an encoding-verifying key or a technical instrument (most usually a computer programme) for data access authorization can also be saved on an information carrier. As an alternative, either for determination of the total capacity R or the data memory capacity D the memory part of a given information carrier, which holds carriers own characteristic data, can also be taken into consideration.

As the capacity W of the unoccupied memory of an information carrier shall be understood this part of a memory in which a user can at any time save data. The total memory capacity R of an information carrier is in any case a sum of the capacity W of the unoccupied memory part of an information carrier and the capacity D of the data memory. It is of benefit when the capacity W of the unoccupied memory of an information carrier is greater than zero.

Under certain circumstances this part of memory a user cannot use can also be understood as the unoccupied memory part of an information carrier. This is e.g. a case in particular with optical information carriers of the CR-R, DVD-R, or DVD+R format, as it can turn out that after saving data on a carrier it "closes", therefore, further saving of data on it will be impossible and a part of the memory will remain not utilized. In a situation when a system of data securing will enable to determine the capacity of such an unoccupied memory (e.g. with the aid of special reader or other device to this purpose) the way to secure data and the way to read them according to the invention can be appropriately modified so that the capacity of the unoccupied memory W takes includes also the above defined unoccupied memory.

According to an advantageous version of the invention a technical instrument serving to authorize the data access is

saved on an external information carrier, i.e. on any memory not being a given information carrier (e.g. a computer memory, other information carrier etc.).

The object of the invention is also a method of reading data secured on an information carrier having a total memory R_2 consisting in that that as a first step a technical instrument to authorize access to is activated. In the next step the parameters of the encoding and verifying key are determined, wherein the parameter of the encoding-verifying key is at least one of the parameters determined by the total memory capacity R of the information carrier or the data memory capacity D of the information carrier or the capacity W of the unoccupied memory part of the information carrier, wherein the total memory capacity R of the information carrier is a sum of the capacity W of the unoccupied memory part of the information carrier and the data memory capacity D. Next parameter values of the encoding-verifying key are determined and herein in order to determine these values at least one of the three capacities is determined: the total memory capacity R of the information carrier or the capacity D of the information carrier data memory or the capacity W of the unoccupied memory part of the information carrier. Next the data secured in the information carrier are decoded with the parameter values of the encoding-verifying key. Finally, in the event if the parameter values of the encoding and verifying key used to decode the data conform to the parameter values of the key used for encoding the data, the access to data secured on the information carrier is authorised. However, the sequence of individual steps as presented above, can be different. A parameter of an encoding-verifying key can be a parameter determined by the total memory capacity R of the information carrier or the capacity D of the information carrier data memory or the

capacity W of the unoccupied memory part of the information carrier. All the said parameters can occur jointly under any possible combination.

The object of the invention is a method to secure data according to which a technical instrument serving to secure data is activated, next, at least one parameter of the verifying key is determined, wherein the parameter of the verifying key is the parameter for identification of a device designed to authorise access to the secured data. As a next step parameters of the encoding-verifying key are determined and data are secured against the values of the encoding-verifying key parameters, and finally data are saved in the memory of the device designed to authorize access to the secured data. However, the order or the stages mentioned above can differ from the order as per above.

According to one of advantageous versions of the invention first the device designed to authorise access to secured data communicates with a system of distribution of secured data, which can be encoded by standard encoding methods. Next, the encoded data are sent from an encoded data distribution system to the device for authorisation of access to the secured data and the encoded data are saved in the memory of the device for authorisation of access to the secured data, finally in the last step the data are decoded. Next, all stages of securing data against the values of the verification key parameters are carried out, wherein the parameters of the verification key are parameters for identification of the device for authorisation of access to the secured data. Such a variation of the invention consists in fact in a specific way data are delivered to the device for authorisation of access to the secured data. As a system for distribution of encoded data the following can serve:

e.g. a data distribution server for e.g. computer programmes, computer games, mobile phone software etc.

According to other advantageous version of the invention data are not secured in a device for authorisation of data access but in a data securing system. With this version of the invention after activation of a technical instrument for data securing a device for authorisation of data access communicates with a system for data securing. Next after determination of the verification key parameters information which enable to determine the values of the verification key parameters are sent from the device for authorisation of access to secured data to the data securing system and additionally after securing data against the values of the verification key parameters the secured data are sent from the data securing system to the device for authorisation of access to the secured data. Additionally it is of benefit when the values of the verification key parameters used for data securing are sent from the data securing system to the device for authorisation of access to the secured data, moreover it is also of benefit when the values which were used for data securing and sent over from the data securing system to the device for authorisation of access to the secured data are encoded. It is also of benefit to encode the secured data sent from the data securing system to the device designed to authorise access to the secured data. A case is also possible that data securing consists in encoding them against the values of the verification key parameters; then it is not necessary to send the values of the parameter key parameters used for data encoding from the data securing system over to the device for authorisation of access to the secured data

A parameter for identification of the device for authorisation of access to the secured data can be a sequence

of digits (e.g. a sequence of digits and characters, abstract data saved in any part of the device for authorisation of access to the secured data). It can as well be a physically measurable parameter, e.g. capacities of various memories of the device to authorise access to the secured data.

According to an advantageous version of the invention a memory of authorisation of the device for authorisation of access to secured data is determined, wherein the parameter for identification of the device for authorisation of access to secured data is a parameter of the memory of the device for authorisation of access to secured data. The memory of the device for authorisation of access to the secured data can be a physically (structurally) separated memory (stem - nucleus) of the device. it can be also a partition of any part of a device memory made to this purpose. It is of benefit when a parameter of the device to authorise access to secured data is a parameter concerning the authorisation memory of the device for authorisation of access to the secured data. As such parameters can serve in particular the total memory capacity R_1 of the device for authorisation of access to secured data or the capacity D_1 of data saved in the authorisation memory of the device for authorisation of access to secured data, or the capacity W_1 of the unoccupied memory part the device for authorisation of access to secured data. These parameters can occur jointly under any configuration, however the relationship that the total capacity R_1 of the authorisation memory is a sum of the capacity D_1 of data saved in the authorisation memory and the capacity W_1 of the unoccupied part of the authorisation memory is always true. A good feature of the memory for authorisation of the device for authorisation of access to the secured data is its unique character, which can consist in it having non-standard (rarely occurring) features such as

a unique (non-standard) total capacity R_1 of the authorisation memory or a unique (non-standard) capacity D_1 of data saved in the authorisation memory or also a unique (non-standard) capacity W_1 of the unoccupied memory part of the authorisation memory. In such a manner a device designed to authorise access to the secured data can be given an "individualised" or "personalized" character.

For another version of the invention the total capacity R_2 of the memory designed to store the secured data of the device for authorisation of access to the secured data is determined and the parameters of this memory can be used as parameters of the verification key. It is an advantage when these parameters are the total capacity R_2 of the memory designed to save secured data, or the capacity D_2 of the data memory, which will be saved in the memory, designed to store secured data or the memory W_2 of the unoccupied memory part of the memory to save secured data. These parameters can occur jointly under any configuration, however, the relationship that the total capacity R_2 of the memory designed to store secured data is a sum of the capacity D_2 of the data memory which will be saved in the memory designed to store secured data and the capacity W_2 of the unoccupied memory part which will remain unoccupied in the memory designed to save secured data. In such a case it can turn out there will be a need to determine a priori the data memory capacity D_2 which will be saved in the memory designed to store the secured data, as e.g. after encoding / decoding the memory capacity can change. For this reason it is advantageously predetermined that the data memory capacity D_2 which will be saved in the memory designed to save secured data will be greater than the capacity of the data memory, thus it will be possible to complement the data memory after

encoding with missing bits (bytes) up the required capacity D_1.

The object of the invention is a method to secure data according to which a technical instrument serving to secure data is activated, next, parameters of the verifying key are determined, wherein the parameter of the verifying key is the parameter for identification of the device designed to authorise access to secured data. During a further stage the verification key parameter values are determined, the secured data are decoded with the values of the verification key parameters, and, if the values of the verification key parameters used for data decoding are equal to those of the verification key which have been used before for data securing, access to the secured data is authorised. The order of the above stages can however be other.

According to another good version of the invention the values of the verification key parameters sent from the data securing system to the device for authorisation of access to secured data are read and the determined values of the verification key parameters are compared to the values of the verification key parameter sent from the data securing system to the device for authorization of access to secured data. If there is such a need the encoded data are decoded; this can be possibly done with the values of the verification key parameters. In this case sending the parameters of the verification key from the data securing system to the device designed to authorise access to the secured data is not necessary. On the other hand it can turn out that it is also necessary to decode the parameter values used for securing/encoding the data sent from the data securing system to the device designed to authorise access to secured data.

The parameter for identification of the device for authorisation of access to the secured data can be a sequence

of digits (e.g. a sequence of digits and characters, abstract data saved in any part of the device for authorisation of access to the secured data). It can as well be a physically measurable parameter, e.g. capacities of varoius memories of the device to authorise access to the secured data.

Every structurally separated part of memory, which can be regarded an independent member characteristic for its total capacity can also be understood as a memory. A memory understood in such a way can be composed of several memories (e.g. a computer hard disc partition etc.).

Memory capacities are expressed in memory units e.g. in bits or bytes. A total memory capacity R is deemed to be a memory capacity where utility data can be saved (therefore the part of a memory where memory own specific data such as e.g. data on the memory specifics, its standards like an allocation map etc. are stored, is neglected). The capacity D of the data memory includes all the data, which will be saved in it excluding data on memory own specific information. As an example in a memory also a verification key or a technical instrument (most often a computer programme) can be saved. As an alternative, either for determination of the total capacity R or the data memory capacity D also the memory capacity, where memory own characteristic data are saved, can be taken into consideration.

According to an advantageous version of the invention the memory of authorisation of the device for authorisation of access to secured data is determined, wherein the parameter for identification of the device for authorisation of access to the secured data is a parameter of the memory of the device for authorisation of access to secured data. The memory of the device for authorisation of access to the secured data can be a physically (structurally) separated memory (stem - nucleus) of the device. It can be also a

partition of a memory of a device made to this purpose. It is of benefit when a parameter of the device to authorise access to secured data is a parameter concerning the authorisation memory of the device for authorisation of access to secured data. As such parameters can serve in particular the total memory capacity R1 of the device for authorisation of access to secured data or the capacity D1 of data memory saved in the authorisation memory of the device for authorisation of access to secured data, or the capacity W1 of the unoccupied memory part the device for authorisation of access to secured data. These parameters can occur jointly under any configuration however the relationship that the total capacity R1 of the authorisation memory is a sum of the capacity D1 of data saved in the authorisation memory and the capacity W1 of the unoccupied part of the authorisation memory is always true. A good feature of a memory for authorisation of a device for authorisation of access to secured data is this it has unique features, which can consist in it having non-standard (rarely occurring) features such as a unique (non-standard) total capacity R1 of the authorisation memory or a unique (non-standard) capacity D1 of data saved in the authorisation memory or also a unique (non-standard) capacity W1 of the unoccupied memory part of the authorisation memory. In such a manner a device designed to authorise access to secured data can be given an "individualised" character.

For another version of the invention the memory of the total capacity R2 of a device designed authorise access to secured data, in which memory these secured data are stored, is identified, and the parameters of this memory can be used as parameters of the verification key. It is good when these parameters are e.g. the total memory R_2 of the memory where secured data are saved or the capacity D_2 of the memory in

which secured data are saved or the capacity W_2 of the unoccupied memory part in which secured data are saved. These parameters can occur jointly under any configuration however the relationship that the total capacity R_2 in which secured data are saved is a sum of the capacity D_2 of the memory where secured data are saved and the capacity W_2 of the unoccupied part of the memory where secured data are saved is always true.

The object of the invention is also a technical instrument to secure data, which enables to determine at least one parameter of the verifying key, wherein the parameter of the verifying key is the parameter of identification of the device designed to authorise access to secured data and next to determine the values of the verification key parameters and to secure data against the values of the verification key parameters. According to another good version of the invention this technical instrument makes it also possible for the device for authorization of access to secured data to communicate with the data securing system and to send information which enable to determine the values of the verification key parameters from the device for authorisation of access to secured data to the data securing system. According to another good version of the technical device this technical instrument enables to encode data against the verification key parameter values. The task of the technical instrument is also to enable to determine the authorization memory of the device for authorization of access to secured data. If the parameters for identification of the device for authorisation of access to secured data are the parameters of the authorization memory of the device for authorization of access to secured data then the technical device designed to secure data enables also to determine these parameters such

parameters as e.g. the total capacity R_1 of the memory for authorization of the device for authorization of access to secured data, the capacity D_1 of the memory of data saved in the authorization memory of the device for authorization of access to secured data or the capacity W_1 of unoccupied memory part of the authorization memory of the device for authorization of access to secured data. According to another version of the invention this technical instrument enables to determine the total capacity R_2 of the memory designed to save secured data, the capacity D_2 of the memory for data which will be saved in the memory designed to store secured data or the capacity W_2 of the unoccupied memory designed to save secured data. It is of benefit that the technical instrument is saved in the memory of the device for authorization of access to secured data.

The object of the invention is a method of authorization of access to a secured device according to which method the secured device can communicate with an information carrier, which authorizes access to a secured device after which communication the technical instrument serving to authorize access to such secured device is activated. During the next stage at least one parameter of the verification key is determined, the values of the verification key parameters are determined against the parameters of the information carrier, which serves for authorization of the access to the secured device and the latter access is authorized. However, the order of individual stages can be other than that.

According to another good version of the invention additionally the data the information carrier, which authorizes access to a secured device, contains, are decoded against the verification key parameter values and the access to the secured device is authorized with these decoded data .

According to another good version of the invention additionally the values of the parameters for authorization of the secured device are determined and the verification key parameter values determined against the parameters of the information carrier, which authorizes access to the secured device, are compared to the parameters for authorization of the secured device.

In addition in case the data contained on the information carrier, which authorizes access to the secured device are encoded, they are decoded. This decoding can be performed with the help of the verification key parameter values, the values of parameters for authorization of a secured device. It can also be necessary to decode the parameters for authorization of the secured device and this decoding can be executed with the values of the verification key parameters.

The parameter of the verification key can be a sequence of digits (i.e. any set of digits or characters) or a physically measurable parameter. Advantageously the verification key parameter is the parameter of the memory of the information carrier, which authorizes access to the secured device, which parameter can be a unique parameter (i.e. a non-standard or rarely occurring parameter). The uniqueness can consist in the parameter having non-standard (rarely occurring) features. In such a manner an information carrier designed to authorise access to the secured device can be given an "individualised" character. The parameters of the information carrier for authorisation of access to the secured device can be in particular the following: the total capacity R_1 of the information carrier which authorizes access to the secured device, the capacity D_1 of the data saved in the information carrier, which authorizes access to the secured device, or the unoccupied capacity W_1 of the

information carrier, which authorises access to the secured device. These parameters can occur jointly under any configuration, however, the relationship that the total capacity R_1 of the information carrier, which authorizes access to the secured device, is a sum of the capacity D_1 of data saved in the information carrier authorizing access to the secured device and the unoccupied capacity W_1 of the information carrier authorizing access to the secured device is always true.

The parameter for authorisation of the secured device can be a sequence of digits or a physically measurable parameter. Advantageously the parameter for authorization of the secured device is the parameter of the memory for authorization of the secured device, wherein with this version of the invention of a method of authorizing access to the secured device, takes place identification of the authorisation memory of the secured device. The parameter of authorisation of a secured device can be a unique parameter (non-standard - rarely occurring). The uniqueness can consist in the parameter to have non-standard (rarely occurring) features. In this manner a secured device can be „personalized". The parameters of the memory for authorization of a secured device can be, among others, the following: the total capacity R_2 of the memory for authorisation of a secured device, the capacity D_2 of data saved in the memory for authorisation of a secured device or the capacity W_2 of the unoccupied part of the memory for authorisation of a secured device. These parameters can occur jointly under any configuration, however, the relationship that the total capacity R_2 of the memory for authorization of the secured device is a sum of the capacity D_2 of data saved in the memory for authorization of the secured device and the

capacity W_2 of the unoccupied part of the memory for authorization of the secured device is always true.

The object of the invention is also a method of reading the data secured on an information carrier consisting in that the technical instrument to authorize data access is activated. Next, the verification key is identified, and this identification consists in finding this key being saved on an information carrier (or anywhere else). Next, the information on the memory of the information carrier contained in the verification key is determined and then the actual parameters of the information carrier are determined. Under the next step the information contained in the verification key are verified against the actual parameters of the information carrier memory, wherein this verification consists in comparing the data contained in the verification key with the physically measurable parameters applying to the memory of the said carrier. If the said verification is positive, the access to the data secured in the information carrier is authorized, what signifies that, if the information contained in the verification key conform to the physical actual parameters of the carrier, a user is given access to the secured data. In the event the information contained in the verification key is encoded, they are decoded. Advantageously the parameters of the memory of the information carrier are such as the capacity W of the unoccupied memory of the information carrier, the capacity D of the occupied memory part of the information carrier and the total capacity R of the information carrier, at any combination of these parameters, wherein the total memory capacity R of the information carrier is in any case a sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory of the information carrier.

The object of the invention is also an information carrier containing secured data, which can be read with a technical device serving for authorization of access to data and with the verification key containing information on the information carrier memory. The information carrier has a total memory and an occupied memory. Advantageously the parameters of the information carrier contained in the verification key are such parameters as the capacity W of the unoccupied memory part of the information carrier, the capacity D of the occupied memory of the information carrier and the total memory capacity R of the information carrier, at any combination of these parameters, wherein under boundary conditions the capacity W of the unoccupied memory part of the information carrier can be 0.

An information carrier can be any information carrier for saving and storing information. As an information carrier shall be understood any carrier including external memories, internal memories, volatile memories, permanent memories in particular hard discs, floppy discs, optical carriers, magnetic carriers, mechanical carriers, semi conductor memories (e.g. ROM, PROM, EPROM, flash EPROM, NVRAM, etc.). As an external and internal memory is understood every permanent and volatile memory in particular hard discs, floppy discs, optical carriers, magnetic carriers, mechanical carriers, semi conductor memories (e.g. ROM, PROM, EPROM, flash EPROM, NVRAM, etc.).

It is also of benefit when a verification key is saved on an information carrier. It is also possible to save a technical instrument for authorization of data access to data on an information carrier.

The object of the invention is also an information carrier containing secured data, characterized in that it has

a data memory capacity D and a total memory capacity R of the information carrier, wherein the latter is a sum of the data memory capacity D and the capacity W of the unoccupied memory part. The data saved in the information carrier can be read with the technical instrument serving to authorize access to data and the encoding and verifying key, wherein the parameter of the latter key is at least one of the parameters determined by: the total memory capacity R of the information carrier or the capacity D of the data memory or the capacity W of the unoccupied memory part of the information carrier. A parameter of an encoding-verifying key can be a parameter determined by the total memory capacity R of the information carrier or a parameter determined by the capacity D of the information carrier data memory or a parameter determined by the capacity W of the unoccupied memory part of the information carrier and all the said parameters can occur jointly under any possible combination.

An information carrier can be any information carrier for saving and storing information. Information carrier can be understood as any carrier including external, internal, or volatile memories, or permanent memories, in particular hard discs, floppy discs, optical carriers, magnetic carriers, mechanical carriers, semi conductor memories (e.g. ROM, PROM, EPROM, flash EPROM, NVRAM, etc.). As an external and internal memory is understood every permanent and volatile memory, in particular hard discs, floppy discs, optical carriers, magnetic carriers, mechanical carriers, semi conductor memories (e.g. ROM, PROM, EPROM, flash EPROM, NVRAM, etc.).

The object of the invention is also an information carrier which authorizes access to a secured device, which has at least one parameter of the information carrier, which determines values of the verification key parameters, wherein access to the secured device is authorized with the values of

the verification key parameters. In a good version of the invention the parameter of the information carrier, which authorizes access to the secured device, is a parameter of the information carrier memory, which authorizes access to the secured device, wherein this parameter can be a unique parameter. These parameters can be in particular: the total capacity R1 of the information carrier which authorizes access to the secured device, the capacity D1 of the data saved in the information carrier, which authorizes access to the secured device, or the unoccupied capacity W1 of the information carrier, which authorises access to the secured device.

An information carrier can be any information carrier for saving and storing information. Information carrier can be understood as any carrier including external, internal, or volatile memories, or permanent memories, in particular hard discs, floppy discs, optical carriers, magnetic carriers, mechanical carriers, semi conductor memories (e.g. ROM, PROM, EPROM, flash EPROM, NVRAM, etc.). As an external and internal memory is understood every permanent and volatile memory in particular hard discs, floppy discs, optical carriers, magnetic carriers, mechanical carriers, semi conductor memories (e.g. ROM, PROM, EPROM, flash EPROM, NVRAM, etc.).

Also every structurally separated part of a memory (e.g. of an information carrier, computer or any other device) can be understood as a memory, which memory can be regarded an independent member characteristic for its total capacity. A memory understood in such a manner signifies that a given information carrier or device can consist of a number of memories (e.g. hard disc partitions, independent layers of optical information carriers etc.)

Memory capacities are expressed as memory units e.g. in bits or bytes. A total memory capacity R is deemed to be a

capacity of a memory in which utility data can be stored (therefore the information carrier data memory capacity storing carriers own data such as e.g. data on the carriers specifics, its standards like the so-called TOC - Table of Content in case of optical carriers etc.), is neglected. The capacity D of the data memory includes all the data, which will be saved on an information carrier, to the exclusion of data on the carrier own specifics - carrier specific features. As an alternative, either for determination of the total memory capacity R or the data memory capacity D also the memory capacity where the information carrier own characteristic data are saved, can be taken into consideration - included. As the capacity W of the unoccupied memory shall be understood this part of the memory, in which a user can at any time save data, wherein in any case the total memory capacity R is a sum of the capacity W of the unoccupied memory and the capacity D of the memory where data are stored. It is of benefit when the capacity W of the unoccupied memory part is greater than zero.

Under certain circumstances as the unoccupied memory can also be understood the memory part, which a user cannot use. Such a case can occur in particular with optical information carriers of the CR-R, DVD-R, or DVD+R etc. format, as it can turn out that after saving data on a carrier it "closes", therefore a further saving of data on it will be impossible and a part of the memory will remain not utilized. In a situation when a system to secure data will enable to determine the capacity of such an unoccupied memory (e.g. with the aid of special reader or other device to this purpose) both the way to secure data and the way to read them according to the invention can be appropriately modified so that the capacity W of the unoccupied memory comprises also the above defined unoccupied memory.

The object of the invention is also a technical instrument for authorization of access to data, which enables to identify the verification key, to determine information contained in the later key and concerning the information carrier memory, to determine the actual parameters of an information carrier and to verify information contained in the verification key against the actual parameters of an information carrier memory. If the verification is positive the technical instrument enables to authorize access to data secured on the information carrier. it is of benefit when a technical instrument serving for authorisation of access to data is a computer programme. A technical instrument serving for authorization of access to data can also be a device.

The object of the invention is also a technical instrument designed to secure data, enabling to determine parameters of the encoding-verifying key, next to determine values of the parameters of the encoding- verifying key and to encode data with the values of the parameters of the encoding-verifying key. This technical instrument, which serves to secure data, enables also to determine the total capacity R_1 of the information carrier memory. Moreover this technical instrument enables prior to encoding *a priori* to determine the capacity D_1 of the data memory, which will be saved on the information carrier, and to determine the capacity W_1 of the unoccupied memory part of the information carrier, which after having saved data will remain unoccupied. It is of benefit when the technical instrument serving for securing data is a computer programme, however, it can be also a device.

The object of the invention is the technical instrument serving to authorise access o data, enabling identification of the encoding and verifying key, next to determine the parameters of the encoding-verifying key, wherein a parameter

of the encoding-verifying key is at least one of the parameters determined by the total memory capacity R of the information carrier or the data memory capacity D of the information carrier or the capacity W of the unoccupied memory part of the information carrier, wherein the total memory capacity R of the information carrier is a sum of the capacity W of the unoccupied memory part of the information carrier and the data memory capacity D. The technical instrument designed to authorise access to data enables as well to determine the values of the encoding-verifying key parameters wherein in order to determine the values of the encoding-verifying key parameters at least one of the three capacities is determined: the total memory capacity R of the information carrier or the capacity D of the data memory or the capacity W of the unoccupied memory part of the information carrier. All the said parameters can occur jointly under any possible combination. The technical instrument to authorise the access to data enables also to decode data secured in the information carrier with the values of the encoding-verifying key parameters and enables to authorise access to data secured in the information carrier in case the values of the encoding-verifying key used for data decoding comply with the encoding-verifying key parameter values used for data encoding. it is of benefit when the technical instrument serving for authorisation of access to data is a computer programme. The technical instrument serving for authorization of access to data can also be a device.

The object of the invention is also a technical instrument to authorise access to data, which enables to determine at least one parameter of the verifying key - wherein a parameter of the verifying key is the parameter of identification of the device designed to authorise access to

secured data - and next enables to determine the values of the verification key parameters and to decode data with the values of the verification key parameters. According to another good version of the invention in addition this technical instrument enables to read the values of the verification key parameters sent from the data securing system to the device for authorisation of access to the secured data and enables to compare the determined values of the verification key parameters to the values of the verification key parameter sent from the data securing system to the device for authorization of access to the secured data. According to another good version this technical instrument enables to decode the encoded data where this decoding of encoded data can be executed with the values of the verification key parameters. The task of the technical instrument is also to enable determination of the authorization memory of the device for authorization of access to the secured data. If the parameters for identification of the device for authorisation of access to secured data are the parameters of the authorization memory of the device for authorization of access to secured data then the technical device designed to secure data enables to determine these parameters i.e. such parameters as the total capacity R1 of the memory for authorization of the device for authorization of access to secured data, the capacity D1 of the memory of data saved in the authorization memory of the device for authorization of access to secured data or the capacity W1 the unoccupied memory of the authorization memory of the device for authorization of access to secured data. According to another version of the invention this technical instrument enables to determine the total capacity R_2 of the memory designed to save the secured data, the capacity D_2 of the memory for data, which will be saved in the memory

designed to store secured data or the capacity W_2 of the unoccupied memory designed to save secured data.

The object of the invention is also a secured device, characterised in that that during the process of authorization of the data access to the secured device the values of the verification key parameters are used, wherein the values of the verification key parameters are determined against the parameters of the information carrier, which serves for authorization of access to the secured device. According to an advantageous version of the invention a secured device is provided with an authorization memory, wherein the authorisation memory can have authorisation parameters and the parameter for authorisation of the secured device can be the memory parameter for authorisation of the secured device.In addition the parameter for authorization of the secured device can be a unique parameter. In particular parameters for authorization of the secured device are as follows: the total capacity R2 of the memory for authorization of a secured device, the capacity D2 of data saved in the memory for authorisation of the secured device or the unoccupied capacity W2 of the memory for authorisation of the secured device. Every device capable of communication with an information carrier for authorisation of an access can be understood as a device.

The object of the invention is in addition a device designed for authorized access to secured data, which has an authorization memory of the total capacity R_1, wherein the total capacity R_1 of the authorisation memory can be a unique memory (i.e. a non-standard one). The authorisation memory can contain also saved data of the data capacity D_1, wherein

the capacity D_1 of the data memory can also be a unique capacity (non-standard).

The object of the invention is also an encoding and verifying key, characterised in that it contains information about the information carrier memory. The verification key acting in conjunction with the technical device serving for authorization of access to data enables to get access to data. Information concerning the information carrier memory advantageously comprises the capacity W of the unoccupied memory part of the information carrier, the capacity D of the occupied memory of the information carrier and the total memory capacity R of the information carrier, at any combination of these parameters. The verification key can be saved at any place and at any amount. Therefore the verification key can be read from several points.

The object of the invention is also a system containing secured data, which consists of an information carrier contain secured data and of a technical instrument serving for authorization of access to data and of a verification key. The data secured in the information carrier can be read with the help of a technical instrument for authorization of access to data for which reading the data contained in the verification key are utilized. Advantageously the parameters of the memory of the information carrier are such as the capacity W of the unoccupied memory part of the information carrier and the total memory capacity R of the information carrier, at any combination of these parameters, wherein the total memory capacity R of the information carrier is in any case a sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory of the information carrier. The system can additionally consist of an external information carrier, in

which the verification key containing information on the information carrier memory or on the technical instrument is saved. Under certain circumstances the system containing secured data can be understood as a device.

The object of the invention is also the encoding and verifying key a parameter of which is at least one of the parameters determined by the total memory capacity R of the information carrier or the data memory capacity D or the capacity W of the unoccupied memory part of the information carrier, wherein the total memory capacity of the information carrier R is a sum of the capacity W of the unoccupied memory part of the information carrier and the data memory capacity D. A parameter of an encoding-verifying key can be the parameter determined by the total memory capacity R of the information carrier or the capacity D of the information carrier data memory or the capacity W of the unoccupied memory part of the information carrier, and all the said parameters can occur jointly under any possible combination.

The object of the invention is also a system containing secured data, which consists of an information carrier containg secured data, of a technical instrument serving for authorization of access to data and of an encoding-verifying key. The data secured in the information carrier can be read with the help of the technical instrument for authorization of access to data and the verification key. The parameter of the encoding-verifying key is at least one of parameters determined by: the total memory capacity R of the information carrier or the capacity D of the data memory or the capacity W of the unoccupied memory part of the information carrier. All the said parameters can occur jointly under any possible combination.

The object of the invention is also a system for securing and reading of the secured information consisting of the data security system and the device for authorization the access to the secured data it communicates of the total capacity R_1.

The system can consist of a greater number of devices, wherein a verification and authorization can be carried out from outer devices also remotely.

The object of the invention is a system for authorization of communication between devices, characterized in that it consists of at least two devices communicating with each other, wherein at least one of these devices has the authorization memory of the R1 capacity and these parameters can serve to secure data being transmitted between them. In addition they can serve to gain access to these data (or devices).

The invention can be applied in such a manner that every user can secure any data with unique parameters of his own computer (or other device). One can also imagine a computer network, which authorizes access to secured data only under condition that computers comply with requirements set by unique parameters with which these data have been secured.

The main advantage of the device is a fact that a legal user will always be able to make a legal safety copy of a legally obtained product against unique parameters of his own device (or several such devices/appliances - home cinema, car audio system, DVD, PCs, mobile phone etc.).

A verification key can comprise more than one unique parameter.

The object of the invention is a system authorising a secured device characterized in that it consists of at least one secured device and of at least one information carrier, which authorizes access to the secured device. According to a good version of the invention concerning a system for authorization of a secured device, a secured device can at the same time function as an information carrier, which authorizes access to the secured device. On the other hand an information carrier, which authorizes access to a secured device, can at the same time function as a secured device.

The object of the invention is in addition a technical instrument for authorization of access to a secured device, which is capable of performing all stages of the disclosed way to authorize access to a secured device. It is also of benefit when a technical device (or any programme) is saved in an authorisation memory of a secured device, which causes that any attempt of modification of its source code will result in a change of authorization memory parameters and thus consequently in making the authorisation of access to the secured device impossible. Moreover a change of the integrity of a code of a technical instrument can be detected by other technical instrument (e.g. a computer programme), thus it being an additional security measure. One can imagine creating in that way a cascadelike, mutual system of security with the aid of technical instruments. A technical instrument can be a computer programme or a device.

In a secured device there can be more than one authorization memory. On the other hand an essential programme of a secured device can be saved in the

authorization memory and should it be modified it will result in a faulty (or none at all) functioning of this secured device.

The object of the invention is also a method of adapting any information carrier to this purpose so that it can be used as an information carrier, which authorizes access to a secured device.

It is worth remembering that data saved on an information carrier, which authorizes access to a secured device, can be data concerning individual settings of functioning of a secured device and with time they can be subject to changes.

This invention finds application also for reciprocal identification of devices, which can cooperate and establish a special system. Other application can be an identification (or authorization) of data saved in an information carrier and secured with the values of identification key parameters.

Verification and authorisation can be carried out with the help of an additional external device. E.g. a verification key can be saved on an external information carrier (other than the information carrier, which authorizes access to a secured device).

A special use of the invention can be a case when a technical instrument performs an auto verification i.e. checks if a memory in which it is saved fulfils prescribed parameter requirements, for example a capacity D of data there stored, a total memory capacity R, etc.

A verification key can contain information required for verification of the integrity (or originality) of data saved in an authorization memory.

The object of the invention is shown as practical examples of its realization. Fig.1 illustrates an information carrier containing secured data, which also acts as an information carrier for authorisation of access to a secured device. A block diagram of a method of securing data on an information carrier is shown in Fig.2. This diagram is also a diagram of a method of authorization of access to a secured device. Fig.3 is a block diagram of a method of reading data secured in an information carrier and Fig. 4 presents a system containing secured data. Fig.5 presents a system for authorization of a secured device. In Fig. 6 we can see a system for securing and reading data.

The figure 7 presents schematically the system for reading data secured on an information carrier.

Practical examples of the invention

The intention of the examples of realization of the invention is to make it easy to understand the idea of the invention and in no way whatsoever does not restrict the scope of its protection.

In order to construct an instrument for securing data on an information carrier a CD released by EMTEC and shown in Fig. 1 can be used. With this CD it is possible to check the parameters of an information carrier, i.e. parameters of the carriers memory. Subsequent stages of securing data are presented schematically in Fig. 2. The total capacity memory R of this carrier including information from the CD contained in the so-called Lead-In is 736 958 464 bytes. The radius of the physical part of the disc on which data can be saved is designated in Fig 1 as A and the letter E in Fig. 2 signifies a stage for determination of the total memory capacity. Next, the capacity of information of a utility programme to be saved on the disc is determined - in this case this capacity is 188 953 640 bytes. To this value we add the amount of

information of the computer programme to be executed (type *.exe). The latter computer programme will be a technical instrument to authorize access to data to be secured. In our case the technical means will be saved on a carrier (it can be also placed elsewhere). The amount of this information is 5 505 981 bytes. Since for determination of the total memory capacity R the data concerning the standard specification of an information carrier were taken into account, the amount of these data of 23 490 560 must also be considered. In our example also the verification key will be saved on the carrier, therefore additional 27 memory bytes shall be reserved for the key. Consequently we determine the capacity D of the occupied memory part (precisely the memory that will be saved on a the carrier), which amounts to 194 459 648 bytes. Fig. 1 shows the radius of the physical part of the disc where the data were saved - the radius is designated B - and this stage was schematically designated F in the Fig. 2. Therefore the capacity of the unoccupied memory part will be 519 008 256 bytes and the radius of the physical part of the disc, in which no data were saved is designated in Fig. 1 as C - this stage, is presented schematically as G in Fig. 2. In a further stage the verification key is created which contains three determined it this way and joined together values R, D and W - this is presented schematically as H in Fig. 2. The utility programme i.e. the executable computer programme (which is the technical instrument for authorisation of access do data subject to securing) and the verification key are saved on the CD-R. Upon completion of the process we leave a free space on the CD-R, in other words, we do not close the CD-R. The stage of saving data on a carrier is illustrated schematically in Fig. 2 and designated as I.

To realise an exemplary way to read data secured on a carrier we will use the system presented in Fig. 4, which consists of the CD-R with the secured data, saved as presented in the example above, and designated as P in Fig. 4. The system includes also a drive designated S in Fig.4. This drive is a part of part of a computer Q in Fig.4. We start inserting the secured disc into such a drive S that is capable of identifying and reading the free space - an unoccupied memory of the disc P (e.g. a recorder by Lite-On). Upon insertion of the disc into drive S an executable computer programme (type: *.exe) saved in this CD will automatically start. This programme constitutes also a technical instrument designed to authorise access to the secured data and this stage designated as J is presented schematically in Fig. 3. In its first step the programme identifies (i.e. localises) the verification key saved on the disc (presented schematically as K in Fig. 2), next it determines the values R, D and W, which are contained in the key (this is presented as L in Fig. 3). Further the programme determines the actual parameters of the carrier memory, i.e. the actual total memory capacity of the disc and the actual capacity of the unoccupied memory part of the disc and the actual occupied memory part of the disc (letter M in Fig. 3). Next the programme compares the values R, D and W with the actual values (designated N and presented schematically in Fig. 3). If the values are identical, the access to the secured data is authorised. In case the compared values differ, the access authorisation is denied (this step is designated with O in Fig. 3).

The utility data securing system operates in such a manner that if utility data were copied from an original carrier onto another one, a new carrier, then the values R, D and W

saved in the verification key will not be equal to the actual parameters of the memory of the new carrier (i.e. with the actual total capacity of the disc, the actual capacity of the unoccupied memory part and the actual occupied memory part of the disc). This occurs especially when an original carrier in which the secured data were saved has a "non-standard" total memory capacity. A „non-standard" total memory capacity is such a memory capacity, which is not available (or easy available) on the market of memories for saving data (e.g. CD-R, DVD-R or DVD+R format discs of a total memory unavailable on the market). On the other hand a „non-standard" total memory capacity can only slightly differ from standard memories - i.e. memories available on the market. The utility data securing system can be used in conjunction with other data securing systems, it can constitute their stem - nucleus or be subordinate to other solutions of this technical problem.

In order to construct a method of securing data on an information carrier one can use an optical carrier, a CD-R disc released by EMTEC and shown in Fig. 1. With this CD it is possible to check the parameters of an information carrier, i.e. parameters, which apply to the carrier's memory. The letter A in Fig. 1 designates a data area within which utility data can be saved (excluding CD-R own characteristic information contained in the so-called Lead-In) of a total capacity R which in our case amounts to 713 467 904 bytes. On the disc we intend to save and secure utility data having a total memory capacity X of 165 463 080 bytes.

Subsequent stages of securing data are presented schematically in Fig. 2, where the letter E signifies the first stage i.e. starting a technical instrument (which is an

executable computer programme) designed to secure utility data of a memory capacity X. The next stage of determination of the encoding-verifying key parameters is denoted F in Fig. 2. In our case the technical instrument serving to secure utility data determines that the parameters of the encoding-verifying key are the two described hereinafter. The first one Z_1 is the absolute value of the difference between the capacity D of the data memory to be saved on the disc and the capacity W_1 of the unoccupied memory part of the information carrier, i.e. $Z_1=|D-W|$, which after saving data will, will remain unoccupied. The second parameter Z_2 is a product of 2 and the total memory capacity R of the disc, i.e. $Z_2=2R$. Since the parameters of the encoding and verifying key are parameters depending on the data memory capacity D, which will be saved on the disc and the unoccupied memory part W_1 of the disc, which after saving data will remain empty, is necessary to determine these capacities *a priori*. This stage denoted G is presented in Fig. 2. We assume the data memory capacity D which will be saved on the disc to be larger than the utility data memory capacity X and will amount to 184 121 012 bytes. From that we know that the capacity W_1 of the unoccupied memory part of the disc, which remains empty on the disc because R=D+W, will amount to 529 346 892 bytes . The letter H in Fig. 2 denotes the next stage of securing data during which the parameters of the encoding-verifying key i.e. parameters Z_1 and Z_2 are determined. From simple calculation we obtain Z1 = 345225880 and Z2 = 14269935808. As we have these values we encode in the next stage - I in Fig.2 - the utility data of the capacity X with parameters Z_1 and Z_2. The algorithm of encoding we have used results in an increase in the capacity X of the utility data after encoding from 165 463 080 bytes to 182 009 388 bytes. The letter J in Fig. 2 denotes the next stage of adding the so-called

complementing 2 111 624 bytes to the capacity of the memory of the encoded data, so that the total memory capacity saved on the disc corresponds to the a priori determined value i.e. 184 121 012 bytes. At the last stage of the exemplary method of securing utility data presented schematically in Fig. 2 and denoted with K, the encoded utility data of the encoded utility data capacity of 182 009 388 bytes and the so-called complementing 2 111 624 bytes are saved on a disc of a total memory of R=713 467 904 bytes. Upon completion of the saving process we leave on the disc a free space, in other words we do nor "close" the disc, therefore it is still possible to save next data on it; the resulting unoccupied memory capacity W of the disc is 529 346 892 bytes.

Thus after having saved the secured (encoded) data on the disc we have a disc as presented schematically in Fig. 1 where A designates a data area within which utility data can be saved (excluding CD-R own characteristic information contained in the so-called TOC) of the total capacity R amounting in our case to R = 713 467 904 bytes. The letter B designates the part of the disc on which the data of the data memory capacity D of 184 121 012 bytes are saved. C denotes the unoccupied area the capacity W of the memory which is 529 346 892 bytes.

To read the data secured on a carrier according to the invention as an example we will use the disc on which utility data were secured (encoded) by the above described method of securing utility data. Next stages of reading data secured on the disc are presented schematically in Fig. 3, where letter L designates the first step, i.e. activation of a technical instrument (which is an executable computer programme) serving to authorise access to secured utility data and which is started automatically after insertion of the disc into its drive. The next stage of determination of the encoding-

verifying key parameters is denoted F in Fig. 3 with M. The activated technical instrument designed to authorise access to secured data is provided with information that the parameters of the encoding-verifying key are the two parameters as follows. The first parameter Z_1 is an absolute value of the difference between the data memory capacity D_2 of the disc and the capacity W_2 of the unoccupied memory part of the disc, i.e. $Z_1=|D-W|$. The second parameter is a product of 2 and the total memory capacity R of the disc, i.e. $Z_2=2R$. The next stage of reading the data secured on the disc is the determination of the values of these parameters and this is presented in Fig. 3 as the N. In order to determine the parameters of the encoding-verifying key we determine successively three capacities of the secured disc: the total memory capacity R_2 of the information carrier, the capacity D_2 of the data memory and the unoccupied capacity W_2 of the carrier memory. Thus we establish the capacities to be: R = 713 467 904 bytes, D = 184 121 012 bytes and W = 529 346 892 bytes. From that we calculate the parameter values Z_1 and Z_2, which are respectively $Z_1=345225880$ and $Z_2=1426935808$. At the next stage denoted O in Fig. 3 we decode the utility data with these parameters. Since we have read the secured data from the originally secured disc as a result of decoding the encoded data the technical instrument authorises access to the secured (encoded) utility data - this step is designated as R in Fig.3.

An exemplary system containing the secured data according to the invention is shown in Fig. 4, where the information carrier containing secured (encoded) data (a CD-R) is designated P. The system comprises also a drive - S in Fig. 4. This drive is a component of a computer - Q in Fig 4.

The utility data securing system operates in such a way that in case utility data were copied from an original carrier onto a new carrier, then the parameter values of a verification key will not be equal to the actual memory parameters of that new carrier. This is especially true when the original carrier the secured data were saved on has a "non-standard" total memory capacity R. Under a non-standard total capacity we understand such a memory capacity, which is not available (or hardly available) on the market of memories for storing data (e.g. CD-R, DVD-R or DVD+R discs of a total capacity not available on the marker). However, a non-standard total memory capacity can differ only slightly from standard capacities available on the market. The utility data securing system can be used in conjunction with other security systems, it can constitute their stem - nucleus - or be subordinated to other solutions of this technical problem.

To realise the exemplary data securing system according to the invention we can use a users computer of the PC class. At the first step one activates in a data security system (which is e.g. a server of a musical files distributor) a technical instrument serving for securing data which is an executable computer programme presented schematically in Fig. 2 under E. Due to operation of this programme the server connects to the users computer over Internet - Fig. 2, letter F. The computer programme determines that the verification key will be composed of two parameters - Fig.2, letter G. The first parameter will be the capacity D_1 of the data memory saved in the computer authorisation memory and the second one will be the capacity D_2 of the memory designed in the users computer memory to save the secured data. In order to determine the parameter values the computer authorisation memory and the

computer memory designed to save the secured data are determined - Fig. 2, letter H. In the next step the computer on request of the server sends to it the determined value of D_1 (7808798 bytes). It is worth mentioning here that the value D_1 - as a value of for authorisation of the computer memory - is a unique value ascribed to this computer. After sending over the determined memory values (i.e. in our case the determined values of the verification key) the server encodes a music file using the determined verification key parameter - D_1, Fig. 2, letter I. Upon encoding the music file capacity will amount to 16113319 bytes, what corresponds exactly to the value of the parameter D_2. At the next step the server encodes the parameter value D_2 with the parameter value D_1 and sends the encoded file and the encoded value of the parameter D_2 to the users computer - Fig. 2 - J. In the last step the users computer saves the encoded file in the predetermined computer memory designed to this purpose.

For realisation of the exemplary method of reading the secured data according to the invention we will use the musical file secured according to the described above example of securing data. In the first step the technical instrument in the users computer is activated (an executable computer programme for authorisation of data access - Fig. 3 - L). Next this programme "decides" that the parameters of the verification key will be the capacity D_1 of the data memory saved in the computer authorisation memory and the capacity D_2 of the data memory saved in the memory of the users computer designed to save secured data - Fig. 3 - M. Next the programme determines the value (unique) of the capacity D_1 of the data memory saved in the authorisation memory of the users computer and with this value decodes both the parameter D_2 - the data memory capacity saved in the users computer -

and the downloaded musical file - see Fig. 3 - N. Further the programme verifies if the decoded parameter values D_2 corresponds to the actual value of the saved capacities - Fig. 3 - letter O. After checking whether these values are equal, the programme enables the users access to the downloaded musical file - Fig. 3 - letter R.

The figure 6 presents schematically the system for securing and reading data, where S signifies the server, which constitutes the data securing system, and P is the users computer - a device designed to authorise access to secure data.

In order to arrange the exemplary system for authorisation of access to a secured device according to the invention one can use as an information carrier which authorises access to secured data the CD-R released by EMTEC shown in Fig. 1, where A designates the total capacity R, in our case: R = 713 467 904 bytes. B designates the part of the disc storing data of the data memory capacity D_1 = 184 121 012 bytes (excluding the CD-R own characteristic data contained in the so-called Lead-In). C points to the unoccupied disc space of a memory capacity W = 529 346 89 bytes. An encoded library of the graphics controller is saved in the data area.

In the first stage shown in Fig. 2 - E, this disc is inserted into the drive for optical carriers of a secured device i.e. a PC thus it is possible for the disc to communicate with the PC. This causes the technical instrument to be automatically activated - Fig. 2, letter E. This technical instrument is an executable computer programme. Next the programme determines the verification key parameters - Fig. 2 - G. The first parameter Z_1 is the capacity D=1 of the memories saved in CD-R, i.e. $Z_1=D_1$. Fig.2 letter H shows the way the parameter values were determined. The second parameter Z_2 is a product

of 2 and the total memory capacity of the computer, i.e. $Z_2=2R_2$. To determine this value the authorisation memory of the computer is identified - Fig.2 - I. This identification is carried out with the aid of a special memory unit (stem) of a unique total capacity R_2 = 713 467 904 bytes. The encoded library of the graphic card controller is encoded with the determined parameter value Z_2 in the next process stage - Fig.2 - J. Next the capacity D_2 = 184 121 012 bytes of the memory saved in the authorisation memory of the computer is determined. A comparison of the values D_1 and D_2 follows. These values are identical therefore the access to the computer is authorised (Fig.2 - K). The access to the computer is authorised also due to the fact that the library of the graphic card controller was decoded with a correct value thus making it possible for the computer to function properly.

The utility data securing system operated in such a way that in case utility data were copied from an original carrier onto a new carrier, then the parameter values of a verification key will not be equal to the actual memory parameters of that new carrier. This happens especially when the original carrier the secured data were saved on has a "non-standard" total memory capacity of R. Under a non-standard total capacity we understand such a memory capacity, which is not available (or hardly available) on the market of memories for storing data (e.g. CD-R, DVD-R or DVD+R discs of a total capacity not available on the marker). However, a non-standard total memory capacity can differ only slightly from standard capacities available on the market. The utility data securing system can be used in conjunction with other security systems, it can constitute their stem - nucleus - or be subordinated to other solutions of this technical problem.

A system for authorisation of a secured device composed of the computer L and the disc P is shown in Fig.5.

Claims

1. A method of securing data on an information carrier characterized in that:
   - a capacity of a total memory R of an information carrier is determined;
   - a data memory capacity for data to be secured on an information carrier is determined;
   - a capacity W of an unoccupied data memory part on an information carrier is determined;
   - a verification key is determined, wherein such a key contains information concerning information carrier memory;
   - data are saved on an information carrier.
2. A method to secure data on the information carrier according to claim 1, characterised in that a capacity D of an occupied memory part of the carrier is determined.
3. A method of securing data on the information carrier according to claim 1 or 2, characterised in that as the verification key a verification key is used which contains information concerning the capacity W of the unoccupied part of the memory on the information carrier is used, wherein the total capacity R of the memory of the information carrier is a sum of the capacity W of the occupied memory part of the information carrier and the capacity D of the unoccupied memory part of the information carrier.
4. A method of securing data on the information carrier according to claims 1 or 2 or 3, characterised in that as the verification key the key containing information concerning the capacity of the occupied part of the

memory D of the information carrier is used, wherein the capacity of the total memory R of the information carrier is the sum of the unoccupied memory part W on the information carrier and the occupied memory part D of the information carrier.

5. A method of securing data on the information carrier according to claims 1 or 2 or 3 or 4, characterised in that as the verification key the key containing information concerning the capacity of the total memory R of the information carrier is used, wherein the capacity of the total memory R of the information carrier is the sum of the unoccupied memory part of the information carrier W and the occupied memory part of the information carrier D.

6. A method of securing data on the information carrier according to claim 1 or 2 or 3 or 4 or 5, characterised in that the verification key is saved on the information carrier.

7. A method of securing data on the information carrier according to claim 1 or 2 or 3 or 4 or 5 or 6, characterised in that technical means for authorization of access to data on the information carrier is saved.

8. A method of securing data on the information carrier according to claim 1 or 2 or 3 or 4 or 5 or 6, characterised in that the technical means serving for authorization of access to data is saved on an external information carrier .

9. A method of securing data on the information carrier according to claim 1 or 2 or 3 or 4 or 5 or 6 or 7 or 8, characterised in that information concerning the memory of the information carrier, which is contained in the verification key, is encoded.

10. A method of securing data on the information carrier according to claim 1, characterised in that the verification key contains information concerning the capacity of the unoccupied memory part of the memory W of the information carrier, wherein the capacity of the total memory R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

11. A method of securing data on the information carrier according to claim 1 or 10, characterised in that the verification key contains information concerning the capacity of the occupied part of the memory D of the information carrier, wherein the capacity of the total memory R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

12. A method of securing data on the information carrier according to claim 1 or 10 or 11, characterised in that the verification key contains information concerning the capacity R of the total memory of the information carrier, wherein the capacity R of the total memory of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

13. A method to read data secured on an information carrier, characterised in that:

- the technical means for authorization of access to data is activated;

- the verification key is identified;
- the information on the information carrier memory contained in the verification key is determined;
- actual parameters of the information carrier are determined;
- the information contained in the verification key is verified against the actual parameters of the information carrier;
- if a positive verification occurs, the access to data secured on the information carrier is authorized.

14. A method of reading data secured on the information carrier according to claim 10 or 11 or 12 or 13 , characterised in that the information contained in the verification key is deciphered.

15. A method of securing data on the information carrier according to claim 1, characterised in that the verification key contains information concerning the capacity W of the unoccupied part of the memory of the information carrier, wherein the capacity of the total memory R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory of the information carrier.

16. A method of securing data on the information carrier according to claim 1 or 10, characterised in that the verification key contains information concerning the capacity of the occupied part of the memory D in the information carrier, wherein the capacity of the total memory R of the information carrier is the sum of the capacity W of the unoccupied memory part of the

information carrier and the capacity D of the occupied memory part of the information carrier.

17. A method of securing data on the information carrier according to claim 1 or 10 or 11, characterised in that the verification key contains information concerning the capacity R of the total memory in the information carrier, wherein the capacity of the total memory R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

18. A method of reading data secured on the information carrier, characterised in that:

- the technical means for authorization of access to data is activated;
- the verification key is identified;
- an information carrier on the memory of the information carrier contained in the information is determined;
- the actual parameters of the information carrier memory are determined;
- the information contained in the verification key are verified against the actual parameters of the information carrier memory;
- if the verification is positive, the access to the data secured on the information carrier is authorized.

19. W method of reading data secured on the information carrier according to claim 10 or 11 or 12 or 13, characterised in that the information contained in the verification key are deciphered.

20. A method of reading the data secured in the information carrier having a total memory capacity of R_2, characterised in that:

- technical means for authorization of access to data is activated;
- the parameters of the encoding-verification key are determined, wherein as an encoding and verifying key parameter at least one of the parameters determined by the total memory capacity R_2 of the information carrier or the total memory capacity D_2 of the information carrier or the unoccupied memory capacity W_2 of the information carrier is used, wherein the total memory capacity R_2 of the information carrier is the sum of the unoccupied memory capacity W_2 of the information carrier and the data memory capacity D_2 of the information carrier.
- the parameter values of the verification key are determined, wherein in order to define the encoding and verifying key parameters at least the total memory capacity R_2 of the information carrier or the information carrier data memory capacity D_2 or the unoccupied memory capacity W_2 of the information carrier are determined;
- with the parameter values of the encoding and verifying key the data secured on the information carrier are deciphered;
- if the encoding-verifying key parameter values used for deciphering the data conform to the encoding-verifying key parameter values used for encoding the data, the access to the data on the information carrier is authorized.

21. A method of reading the data secured on the information carrier according to claim 20, characterised in that the parameter determined by the total capacity of the memory R_2 of the information carrier is used as a parameter of the encoding and verifying key.

22. A method of reading the data secured on the information carrier according to claim 20 or 21, characterised in that the parameter determined by the capacity of the information carrier data memory capacity D_2 is used a parameter of the encoding and verifying key.

23. A method of reading the data secured on the information carrier according to claim 20 or 21 or 22, characterised in that the parameter determined by the capacity of the unoccupied memory part W_2 of the information carrier is used a parameter of the encoding and verifying key.

24. A method of securing data, characterised in that:

- the technical means for authorization of access to data is activated;
- at least one parameter of the verification key is determined, wherein the parameter of the verification key is the parameter to identify the device to authorize access to the secured data;
- parameter values of the verification key are determined;
- the data are secured in relation to the verification key values ;
- the data are saved in a memory of the device to authorize access to the secured data.

25. A method to secure data according to claim 24, characterised in that that first:

- the device for authorization of access to the secured data communicates with a distribution system of the encoded data;
- the encoded data are sent from the encoded data distribution system to the device for authorization of access to the secured data;
- the encoded data are saved in the memory of the device for authorization of access to the secured data;
- the data are deciphered.

26. A method of securing data according to claim 24 , characterised in that:

- upon the activation of the technical means which serves to secure data the device for authorization of access to the secured data communicates with the data security system;
- upon determination of the verification key parameters information which enables to determine the parameter values of the verification key is sent from the device for authorization of access to the secured data to the data security system;
- upon securing the data against the verification key parameters the secured data are sent from the data security system to the device for authorization of access to the secured data.

27. A method of securing data according to claim 26, characterised in that the verification key parameter values, which were used to secure data, are sent from

the data security system to the device for authorization of access to the secured data.

28. A method of securing data according to claim 26 or 27, characterised in that the secured data, being sent over from the data securing system to the device for authorization of access to the secured data are encoded.

29. A method of securing data according to any of the claims from 24 through 28, characterised in that during securing the data they are encoded against the parameter values of the verification key.

30. A method of securing data according to any of the claims from 24 through 29, characterised in that the parameter used for identification of the device for authorization of access to the secured data is a sequence of digits.

31. A method of securing data according to any of the claims from 24 through 30 characterised in that the parameter used for identification of the device for authorization of access to the secured data is a physically measurable parameter.

32. A method of securing data according to any of the claims from 24 through 30 , characterised in that:

- an authorization memory of the device for authorization of access to the secured data is determined, wherein as
- a parameter for identification of the device for authorization of access to the secured data the parameter of the authorization memory of the device to authorize access to the secured data is used.

33. A method of securing data according to claim 32, characterised in that the parameter used for identification of the device for authorization of access to the secured data is a parameter concerning the authorization memory capacity of the device for authorization of access to the secured data.

34. A method of securing data according to claim 33, characterised in that the parameter used for identification of the device for authorization of access to the secured data is the total capacity R_1 of the authorisation memory of the device for authorization of access to the secured data, wherein the total capacity R_1 of the authorization memory is a sum of the data memory capacity D_1 saved in the authorization memory and the capacity of the unoccupied memory part W_1 of the authorisation memory.

35. A method of securing data according to claim 33 or 34, characterised in that the parameter used for identification of the device for authorization of access to the secured data is the capacity D_1 of the memory of the data saved in the authorization memory of the device designed for authorization of access to the secured data, wherein the total memory capacity R_1 of the authorisation memory is a sum of the capacity D_1 of the memory of data saved in the authorization memory and the capacity W_1 of the unoccupied memory part of the authorization memory.

36. A method of securing data according to claim 33 or 34 or 35, characterised in that the parameter used for identification of the device for authorization of access to the secured data is the capacity W_1 of the unoccupied memory part of the device designed for authorization of access to the secured data, wherein

the total memory capacity R_1 of the authorisation memory is the sum of the capacity D_1 of the memory of data saved in the authorization memory and the capacity W_1 of the unoccupied memory part of the authorization memory.

37. A method of securing data according to any of the claims from 32 through 36, characterised in that a unique memory is used as the authorization memory of the device for authorization of access to the secured data.

38. A method of securing data according to any of the claims from 24 through 31, characterised in that:

- a memory of the total capacity of R_2 of the device for authorization of access to the secured data; which a memory is designed to store the secured data, is determined, wherein as :
- a parameter for identification of the device for authorisation of the access to the secured data the total memory capacity R_2 of the memory designed to store the secured data is used, wherein the total capacity R_2 of the memory designed to store the secured data is the sum of the memory capacity D_2 of data to be saved in a memory designed to store secured data and the capacity W_2 of the unoccupied memory part ; i.e. of the memory part to store secured data which, will remain unoccupied.

39. A method of securing data according to any of the claims from 24 through 31 and 38, characterised in that:

- the memory of the total capacity R_2 of the device for authorisation of access to the secured data designed to store secured data is determined, wherein as:

- a parameter for identification of the device designed for authorization of access to the secured data the capacity D_2 of the data memory - i.e. the part of the memory to store the secured data - is used, wherein the total capacity R_2 of the memory designed to store the secured data is the sum of the data memory capacity D_2 which shall be stored in the memory designed to store the secured data and the capacity W_2 of the unoccupied memory part ; i.e. the part of the memory to store secured data, which will remain unoccupied.

40. A method of securing data according to any of the claims from 24 through 32 and 38 or 39, characterised in that:

- a memory of a total capacity R_2 - designed to store the secured data - of the device for authorization of access to the secured data is determined, wherein as :

- a parameter for identification of the device for authorisation of access to the secured data the capacity W_2 of the unoccupied memory part within the memory designed to store the secured data is used, wherein the total capacity R_2 of the memory designed to store the secured data is a sum of the capacity D_2 of the memory of data to be saved in a memory designed to store secured data and the capacity W_2 of the unoccupied memory part ; i.e. the part of the memory to store secured data, which will remain unoccupied.

41. A method of securing data according to any of the claims from 26 through 40, characterised in that the verification key parameter values used for securing data

and sent from the data security device to the device for authorization of access to the secured data are encoded.

42. A method of reading the secured data saved in the device, characterised in that:

- the technical means for authorization of access to data is activated;
- the parameters of the verification key are determined, wherein as a encoding and verifying key parameter is a parameter designed to identify the device for authorisation of the access to the secured data;
- the parameters of the verification key are determined;
- the secured data are decoded with the parameter values of the verifying key;
- if the verification key parameter values used for decoding the data conform to the verification key parameter values, which were used to secure the data, the access to the secured data is authorized.

43. A method of reading the secured data according to claim 42, characterised in that the verification key parameter values sent from the data securing system to the device for authorisation of access to the secured data are read.

44. A method of reading the secured data according to claim 42 or 43, characterised in that the determined verification key parameter values are compared against the verification key parameter values being sent over from the data securing system to the device for authorization of access to the secured data .

45. A method of reading the secured data according to any claim from 42 through 44 , characterised in that the encoded data are deciphered.

46. A method of reading the secured data according to any claim from 42 through 45, characterised in that the encoded data are deciphered with the aid of the verification key parameter values.

47. A method of reading the secured data according to any claim from 42 through 46, characterised in that a sequence of digits is used as the identification parameter to authorize access to the secured data.

48. A method of reading the secured data according to any claim from 42 through 47, characterised in that a physically measurable parameter is used as the identification parameter to authorize access to the secured data.

49. A method of reading the secured data according to any claim from 42 through 48, characterised in that:

- an authorization memory of the device designed for authorization of access to the secured data is determined, wherein
- a parameter to identify the device to authorize access to the secured data is the parameter of the authorization memory of the device designed for authorization of access to the secured data.

50. A method of reading the secured data according to claim 49, characterised in that the parameter concerning the capacity of the authorization memory of the device designed to authorize the access to the secured data is

used as the parameter to identify the device for authorization of access to the secured data.

51. A method of reading the secured data according to claim 50, characterised in that the total capacity R_1 of the authorization memory of the device designed to authorize the access to the secured data is used as the parameter to identify the device designed to authorize access to the secured data, wherein the total capacity R_1 of the authorization memory is the sum of the capacity D_1 of the memory of the data stored in the authorization memory and the capacity W_1 of the unoccupied memory part of the authorization memory.

52. A method of reading the secured data according to claim 50 or 51, characterised in that the capacity D_1 of the memory of the data stored in the authorization memory of the total memory R_1 of the device designed to authorize access to the secured data is used as the parameter to identify the device for authorisation of access to the stored data, wherein the total memory capacity R_1 of the authorization memory is the sum of the capacity D_1 of the memory of the data stored in the authorization memory and the capacity W_1 of the unoccupied memory part of the authorization memory.

53. A method of reading the secured data according to any claim from 50 to 52, characterised in that that as a parameter to identify the device for authorization of access to the secured data the capacity W_1 of the unoccupied memory part of the authorisation memory having the total capacity R_1 of the device to authorize access to the secured data is used, wherein the total memory capacity R_1 of the authorization memory is the

sum of the capacity D_1 of the memory of the data stored in the authorization memory and the capacity W_1 of the unoccupied memory part of the authorization memory.

54. A method of reading the secured data according to any claim from 50 through 53, characterised in that a unique memory is used for authentication of the device for authorization of access to the secured data.

55. A method of reading the secured data according to any claim from 42 through 48, characterised in that:

- the memory of the total capacity R_2 of the device for authorization of access to the secured data in which the secured data are stored is identified, wherein:
- the parameter to identify the device to authorize access to the secured data is the total capacity R_2 of the memory in which the secured data are stored, wherein the total capacity R_2 of the memory in which the secured data are stored is the sum of the capacity D_2 of the memory in which the secured data are stored and the capacity W_2 of the unoccupied memory part of this memory.

56. A method of reading the secured data according to any claim from 42 through 48 and 55, characterised in that:

- the memory of the total capacity R_2 of the device for authorization of access to the secured data, in which the secured data are stored, is identified, wherein:
- a parameter used to identify the device for authorization of access to the secured data is the capacity D_2 of the memory of the secured data , wherein the total capacity R_2 of the memory, in which the

secured data are stored, is the sum of the capacity D_2 of the memory, in which the secured data are stored, and the capacity W_2 of the unoccupied memory part of this memory.

57. A method of reading the secured data according to any claim from 42 through 48 and 55 or 56, characterised in that:

- the memory having the total capacity R_2 of the device for authorization of access to the secured data in which the secured data are stored is identified, wherein:
- the parameter used to identify the device for authorization of access to the secured data is the capacity of the unoccupied memory part W_2 of this memory, wherein the total capacity R_2 of the memory in which the secured data are stored is the sum of the capacity D_2 of the memory part, in which the secured data are stored, and the capacity W_2 of the unoccupied memory part of this memory.

58. A method of reading the secured data according to any claim from 42 through 57, characterised in that the parameter values of the verification key, which were used for securing the data and sent from the data securing system to the device for authorization of access to the secured data authorization, are deciphered.

59. A method of authorization of access to the secured device, characterised in that:

- it makes it possible for the secured device to communicate with the information carrier, which authorizes access to the secured device;
- the technical means for authorization of access to the secured device is activated;
- at least one parameter of the verification key is determined;
- the verification key parameter values are determined against the parameters of the information carrier, which authorizes access to the secured device;
- the access to the secured device is authorized.

60. A method of authorisation of access to the secured device according to claim 59, characterised in that:

- the data contained in the information carrier, which authorizes access to the secured device, are decoded against the verification key parameter values;
- using the decoded data the access to the secured device is authorized.

61. A method of authorisation of access to the secured device according to claim 59, characterised in that:

- the authorization parameter values of the secured device are determined;
- the parameter values of the verification key as determined against the parameters of the information carrier, which is used to authorize access to the secured device, are compared to the authorization parameters of the secured device.

62. A method of authorization of access to the secured device according to any claim from 59 through 61 ,

characterised in that the encoded data contained in the information carrier for authorization of access to the secured device are deciphered.

63. A method of authorisation of access to the secured device according to claim 62, characterised in that the data contained in the information carrier for authorization of access to the secured device are deciphered with the verification key parameter values.

64. A method of authorisation of access to the secured device according to claim 62, characterised in that the encoded data contained in the information carrier for authorization of access to the secured device are deciphered with the parameter values for authorization of the secured device.

65. A method of authorization of access to the secured device according to any claim from 59 through 64, characterised in that the encoded parameters for authorisation of the secured device are deciphered.

66. A method of authorization of access to the secured device according to claim 65, characterised in that the encoded parameters for authorisation of the secured device are deciphered with the verification key parameter values.

67. A method of authorization of access to the secured device according to any claim from 59 through 66, characterised in that the parameter of the verification key is a sequence of digits.

68. A method of authorization of access to the secured device according to any claim from 59 through 66,

characterised in that that as the parameter of the verification key a physically measurable parameter is used.

69. A method of authorization of access to the secured device according to any claim from 59 through 68, characterised in that the verification key parameter is a memory parameter of the information carrier for authorization of access to the secured device.

70. A method of authorization of access to the secured device according to claim 69, characterised in that the memory parameter of the information carrier for authorization of access to the secured device is a unique parameter.

71. A method of authorization of access to the secured device according to claim 69 or 70, characterised in that the verification key parameter is the total capacity R_1 of the information carrier for authorization of access to the secured device.

72. A method of authorization of access to the secured device according to claim 69 or 70 or 71, characterised in that the verification key parameter is the capacity D_1 of the data stored in the information carrier for authorization of access to the secured device.

73. A method of authorization of access to the secured device according to claim 69 or 70 or 71 or 72, characterised in that the verification key parameter is the capacity W_1 of the unoccupied memory part of the information carrier for authorization of access to the secured device.

74. A method of authorization of access to the secured device according to any claim from 61 through 66, characterised in that the parameter for authorization of the secured device is a sequence of digits.

75. A method of authorization of access to the secured device according to any claim from 61 through 66, characterised in that the parameter for authorization of the secured device is a physically measurable parameter.

76. A method of authorization of access to the secured device according to any claim from 61 through 66 and 74 or 75, characterised in that the memory to authorize the secured device is identified, herein a parameter for authorization of the secured device is the parameter of the memory for authorization of the secured device.

77. A method of authorization of access to the secured device according to claim 76, characterised in that the parameter of the memory for authorization of the secured device is a unique parameter.

78. A method of authorization of access to the secured device according to claim 76 or 77, characterised in that the parameter to authorize the secured device is the total authorization memory capacity R_2 for authorization of the secured device.

79. A method of authorization of access to the secured device according to claim 76 or 77 or 78, characterised in that the parameter to authorize the secured device is the capacity D_2 of the data saved in the memory for authorization of the secured device.

80. A method of authorization of access to the secured device according to claim 76 or 77 or 78 or 79, characterised in that the parameter to authorize the secured device is the unoccupied memory part capacity W_2 of the memory for authorization of the secured device.

81. The information carrier containing the secured data, characterised in that it has a total capacity and an occupied memory part capacity of the information carrier, herein the total memory capacity R is a sum of the occupied memory part capacity D and the unoccupied memory part capacity W, wherein the data secured in the information carrier can be read with the help of the technical device serving to authorize access to the data and the verification key, wherein the verification key contains information on the memory of the information carrier.

82. The information carrier containing the secured data according to claim 81, characterised in that the verification key contains information on the occupied memory part capacity W of the information carrier.

83. The information carrier containing the secured data according to claim 81 or 82, characterised in that the verification key contains information on the occupied memory part capacity D of the information carrier.

84. The information carrier containing the secured data according to claim 81 or 82 or 83, characterised in that the verification key contains information on the total capacity R of the information carrier memory.

85. The information carrier containing the secured data according to claim 81 or 82 or 83 or 84, characterised

in that the verification key is saved on the information carrier.

86. The information carrier containing the secured data according to claim 81 or 82 or 83 or 84 or 85, characterised in that the technical device which serves for authorisation of the data access is saved on the information carrier.

87. The information carrier containing the secured data, characterised in that it has the data memory capacity D and the information carrier memory total capacity R, wherein the total capacity of the information carrier memory R is the sum of data memory capacity D and the unoccupied memory part capacity W, and the data secured on the information carrier can be read with the technical means, which is used for the authorization of the data access, and the encoding-verifying key, wherein the parameter of the said key is at least one of the parameters determined by: the total capacity of the information carrier memory R or the data memory capacity D or the capacity W of the unoccupied part of the information carrier memory.

88. The information carrier containing the secured data according to claim 87, characterised in that the parameter of the encoding-verifying key is the parameter determined by the total memory capacity R of the information carrier.

89. The information carrier containing the secured data according to claim 87 or 88, characterised in that the parameter of the encoding-verifying key is the parameter determined by the data memory capacity D.

90. The information carrier containing the secured data according to claim 87 or 88 or 89, characterised in that the parameter of the encoding-verifying key is the parameter determined by the capacity W of the unoccupied part of the memory of the information carrier.

91. The information carrier which authorizes access to the secured device, characterised in that it has at least one parameter of the information carrier, which determines the verification key parameter values, wherein the verification key parameter values serve to authorize access to the secured device.

92. The information carrier which authorizes access to the secured device according to claim 91, characterised in that the parameter of the information carrier serving to authorize the access to the secured device is the parameter of the memory of the information carrier serving to authorize access to the secured device.

93. The information carrier, which authorizes access to the secured device according to claim 92, characterised in that the parameter of the information carrier serving to authorize access to the secured device is a unique parameter.

94. The information carrier, which authorizes access to the secured device according to claim 91 or 92 or 93, characterised in that the parameter of the verification key is the total capacity R_1 of the information carrier, which authorizes access to the secured device.

95. The information carrier, which authorizes access to the secured device according to claim 91 or 92 or 93 or 94, characterised in that the parameter of the

verification key is the capacity D_1 of the data saved in the information carrier which authorizes access to the secured device.

96. The information carrier, which authorizes access to the secured device according to claim 91 or 92 or 93 or 94 or 95, characterised in that the parameter of the verification key is the capacity W_1 of the unoccupied part of the information carrier memory, which authorizes access to the secured device.

97. The technical means for authorization of data access, characterized in that it makes possible:

- to identify the verification key;
- to determine the information concerning the information carrier memory contained in the verification key;
- to determine the actual parameters of the information carrier;
- to verify the information contained in the verification key against the actual parameters of the information carrier;
- if the verification is positive, to authorize access to the data secured on the information carrier.

98. The technical means for authorization of the data access according to claim 97, characterized in that it is a computer program.

99. The technical means for authorization of the data access according to claim 97, characterized in that the technical means is a device.

100. The technical means serving for securing of data, characterised in that it makes it possible:

- to determine the parameters of the encoding-verification key;
- to determine the parameter values of the encoding-verifying key;
- to encode the data with the values of the encoding-verification key parameters.

101. The technical means for securing of data according to claim 100, characterized in that it makes possible to determine the total memory capacity R_1 of the information carrier.

102. The technical means for securing of data according to claim 100 or 101, characterized in that that before encoding it enables to determine the memory capacity D_1 for data to be saved on the information carrier.

103. The technical means for securing of data according to claim 100 or 101 or 102, characterized in that that before encoding it enables to determine the capacity W_1 of the unoccupied part of the information carrier memory which after having saved the data will remain unoccupied.

104. The technical means for securing of data according to claim 100 or 101 or 102 or 103, characterised in that the technical means is a computer program.

105. The technical means for securing of data according to claim 100 or 101 o4 102 or 103, characterised in that the technical means is a device.

106. The technical means serving for authorization of the data access, characterized in that it makes it possible:

- to identify the encoding-verifying key;
- to determine the encoding-verifying key parameters;
- to determine the encoding-verifying key parameter values;
- to decipher the data secured in the information carrier with the values of the encoding-verifying key parameters;
- to authorise access to the data secured in the information carrier with the values of the encoding-verifying key parameters if the values of the encoding-verifying key parameters comply with the encoding-verifying key parameter values, which were used for encoding the data.

107. The technical means for securing of data according to claim 106, characterised in that it makes it possible to determine the total memory capacity R_2 of the information carrier.

108. The technical means for securing of data according to claim 106 or 107, characterised in that it makes it possible to determine the data memory capacity D_2 of the information carrier.

109. The technical means for securing of data according to claim 106 or 107 or 109, characterised in that it makes it possible to determine the capacity W_2 of the unoccupied part of the information carrier memory.

110. The technical means for securing of data according to claim 106 or 107 or 108 or 109, characterised in that the technical means is a computer program.

111. The technical means for securing of data according to claim 107 or 108 or 109 or 111, characterised in that the technical means is a device.

112. The technical means serving for authorization of the data access, characterized in that it makes it possible:

- to determine at least one parameter of the verifying key, wherein the parameter of the verifying key is the parameter of identification of the device designed to authorise access to the secured data;
- to determine the value of the verifying key parameters;
- to secure the data against the value of the verifying key parameters;

113. The technical means for securing of data according to claim 112, characterised in that it enables:

- for the device for authorization of access to the secured data to communicate with the data security system;
- to send information enabling to determine the value of the verification key parameters from the device for authorizing access to the secured data to the data security system;

114. The technical means for securing of data according to claim 112 or 113, characterised in that it enables to encode the data against the values of the verification key parameters.

115. The technical means for securing of data according to any claim from 112 through 114, characterised in that it enables to determine the authorization memory of the device designed for authorization of access to the secured data, wherein the parameter for identification of the device designed to authorize access to the secured data is the authorization memory parameter of the device to authorize access to the secured data.

116. The technical means for securing of data according to any claim from 112 through 115, characterised in that it enables to determine the total capacity R_1 of the authorization memory of the device designed for authorization of access to the secured data.

117. The technical means for securing of data according to any claim from 112 through 116, characterised in that it enables to determine the data memory capacity D_1, wherein the said data are saved in the authorization memory of the device used for authorization of access to the secured data.

118. The technical means for securing of data according to any claim from 112 through 117, characterised in that it enables to determine the capacity W_1 of the

unoccupied part of the authorization memory of the device designed to authorize access to the secured data.

119. The technical means for securing the data according to any claim from 112 through 118, characterised in that it enables to determine the total capacity R_2 of the memory designed save the secured data.

120. The technical means for securing of data according to any claim from 112 through 119, characterised in that it enables to determine the capacity D_2 of the memory designed to save the secured data.

121. The technical means for securing of data according to any claim from 112 through 120, characterised in that it enables to determine the capacity W_2 of the unoccupied memory part designed to save the secured data.

122. The technical means serving for authorization of the data access, characterized in that it makes it possible:

- to determine at least one parameter of the verifying key, wherein the parameter of the verifying key is the parameter for identification of the device designed to authorise access to the secured data;
- to determine the values of the verifying key parameters;
- to decode the data with the values of the verifying key parameters;

123. The technical means for authorisation of access to the secured data according to claim 122, characterised in that it enables to read the values of the verification key parameters sent from the data security system to the device designed to authorize access to the secured data.

124. The technical means for securing of data according to claim 122 or 123, characterised in that it enables to compare the determined values of the verification key parameters with the values of the verification key parameters being sent over from the data security system to the device for authorization of access to the secured data.

125. The technical means for authorisation of access to the data according to claim 122 or 123, characterised in that it enables to decipher the encoded data.

126. The technical means for authorisation of access to the data according to any claim from 121 through 124, characterised in that it enables to decipher the encoded data with the values of the verification key parameters.

127. The technical means for securing of data according to any claim from 122 through 126, characterised in that it enables to determine the authorization memory of the device designed for authorization of access to the secured data, wherein the parameter for identification of the device for authorization of

access to the secured data is the authorization memory parameter of the device for authorization of access to the secured data.

128. The technical means for securing of data according to any claim from 122 through 127, characterised in that it enables to determine the total capacity R_1 of the authorization memory of the device designed for authorization of access to the secured data.

129. The technical means for securing of data according to any claim from 122 through 128, characterised in that it enables to determine the capacity D_1 of the data memory of the data saved in the authorization memory of the device designed for authorization of access to the secured data.

130. The technical means for securing of data according to any claim from 122 through 129, characterised in that it enables to determine the capacity W_1 of the unoccupied memory part of the authorization memory of the device designed for authorization of access to the secured data.

131. The technical means for securing of data according to any claim from 122 through 130, characterised in that it enables to determine the total capacity R_2 of the memory designed for saving the secured data.

132. The technical means for securing of data according to any claim from 122 through 131, characterised in

that it enables to determine the capacity D_2 of the memory of data, which will be saved in the memory designed for storing secured data.

133. The technical means for securing of data according to any claim from 122 through 132, characterised in that it enables to determine the capacity W_2 of the memory designed for saving the secured data.

134. A secured device, characterised in that that during the process of authorization of access to the secured device the values of the verification key parameters are used, wherein the values of the verification key parameters are determined against the parameters of the information carrier, which authorizes access to the secured device.

135. A secured device according to claim 134, characterised in that it has an authorization memory.

136. A secured device according to claim 134 or 135, characterised in that the authorisation memory of the secured device is provided with authorization parameters, wherein the parameter for authorization of the secured device is the parameter of the authorization memory of the secured device.

137. A secured device according to claim 134 or 135 or 136, characterised in that the authorisation memory of the secured device is a unique parameter.

138. A secured device according to claim 134 or 135 or 136 or 137, characterised in that the parameter for authorization of the secured device is the total capacity R_2 of the authorization memory for the secured device.

139. A secured device according to claim 134 or 135 or 136 or 137 or 138, characterised in that the authorisation parameter for the secured device is the capacity D_2 of the memory of data saved in the authorization memory for the secured device.

140. A secured device according to claim 134 or 135 or 136 or 137 or 138 or 139, characterised in that the authorisation parameter for the secured device is the capacity W_2 of the unoccupied memory part of the authorization memory for the secured device.

141. A device designed to authorise access to the secured data, characterized in that it has the authorization memory of a total capacity R_1.

142. A device designed to authorise access to the secured data according to claim 121 or 141, characterised in that the total capacity R_1 is a unique capacity.

143. A device designed to authorise access to the secured data according to any claim from 121 or 141 or 142, characterised in that the authorization memory contains saved data of the data memory capacity D_1.

144. A device for authorized access to the secured data according to any claim from 121 or 141 through 143, characterised in that the data memory capacity D_1 is a unique capacity.

145. An encoding and verifying key, characterised in that the parameter of the encoding-verifying key is at least one of the parameters determined by the total memory capacity R of the information carrier or the data memory capacity D of the information carrier or the capacity W of the unoccupied memory part of the information carrier, wherein the total memory capacity R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the data memory capacity D.

146. An encoding and verifying key according to claim 145, characterised in that the parameter of the encoding and verifying key is a parameter determined by the total memory capacity R of the information carrier.

147. An encoding and verifying key according to claim 145 or 146, characterised in that the parameter of the encoding and verifying key is a parameter determined by the data memory capacity D of the information carrier.

148. An encoding and verifying key according to claim 145 or 146 or 147, characterised in that the parameter of the encoding and verifying key is a parameter determined by the capacity W of the unoccupied memory part of the information carrier.

149. A verifying key, characterised in that it contains information about the memory of the information carrier.

150. A verifying key according to claim 149, characterised in that it contains information about the capacity W of the unoccupied memory part of the information carrier, wherein the total memory capacity R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

151. A verifying key according to claim 149 or 150, characterised in that it contains information about the capacity D of the occupied memory part of the information carrier, wherein the total memory capacity R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

152. A verifying key according to claim 149 or 150 or 151, characterized in that the verification key contains information about the total memory capacity R of the information carrier, wherein the total memory capacity R of the information carrier is the sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier.

153. A system containing the secured data, characterised in that it consists of the information carrier containing the secured data, of the technical device for data access authorization and of the verification key, wherein the information carrier has a total memory and an unoccupied memory part, where the total memory capacity R of the information carrier is a sum of the capacity W of the unoccupied memory part of the information carrier and the capacity D of the occupied memory part of the information carrier and the data secured in the information carrier can be read with the help of the technical device for authorization of data access and using the information contained in the verification key.

154. A system containing the secured data according to claim 153, characterised in that it has additionally an external information carrier in which the verification key containing information on the information carrier memory is saved.

155. A system containing the secured data according to claim 153 or 154, characterised in that it has an additional external information carrier in which a technical device for authorization of data access is saved.

156. A system containing the secured data according to claim 153 or 154 or 155, characterised in that the verification key contains information on the capacity W of the unoccupied memory part of the information carrier.

157. A system containing the secured data according to claim 153 or 154 or 155 or 156, characterised in that the verification key bears information on the capacity D of the occupied memory part of the information carrier.

158. A system containing the secured data according to claim 153 or 154 or 155 or 156 or 157, characterised in that the verification key bears information on the total memory capacity R of the information carrier.

159. A system for securing and reading of the secured information, characterized in that it consists of the data security system and the device for authorization of access to the secured data of the total capacity R_1 it communicates with.

160. A system for authorization of communication between two devices, characterized in that it consists of at least two devices in communication with each other, wherein at least one of these devices has the authorization memory of the total capacity R_1.

161. A system authorising the secured device, characterized in that it consists of at least one secured device and of at least one information carrier, which authorizes access to the secured device.

162. A system authorising the secured device according to claim 161, characterized in that the secure device

can at the same time function as an information carrier, which authorizes access to the secured device.

163. A system authorising the secured device according to claim 161 or 162, characterized in that the information carrier, which authorizes access to the secured device, can at the same time function as a secured device.

164. A system containing secured data, characterised in that it consists of the information carrier containing the secured data, of the technical device for authorization of data access and of the encoding and verification key, wherein the data secured in the information carrier can be read with the help of the technical device for authorization of data access and the encoding-verifying key, while the parameter of the latter key is at least one of the parameters determined by: the total memory capacity R of the information carrier or the capacity D of the information carrier data memory or the capacity W of the unoccupied memory part of the information carrier.

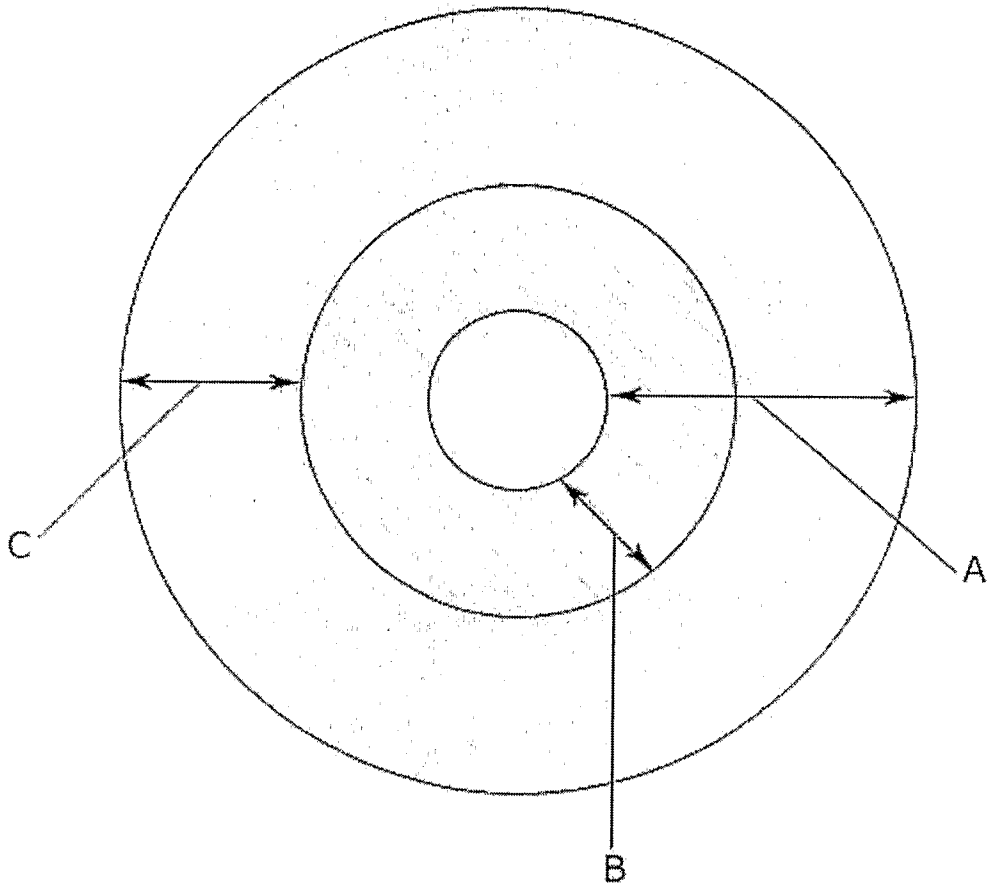

Fig. 1

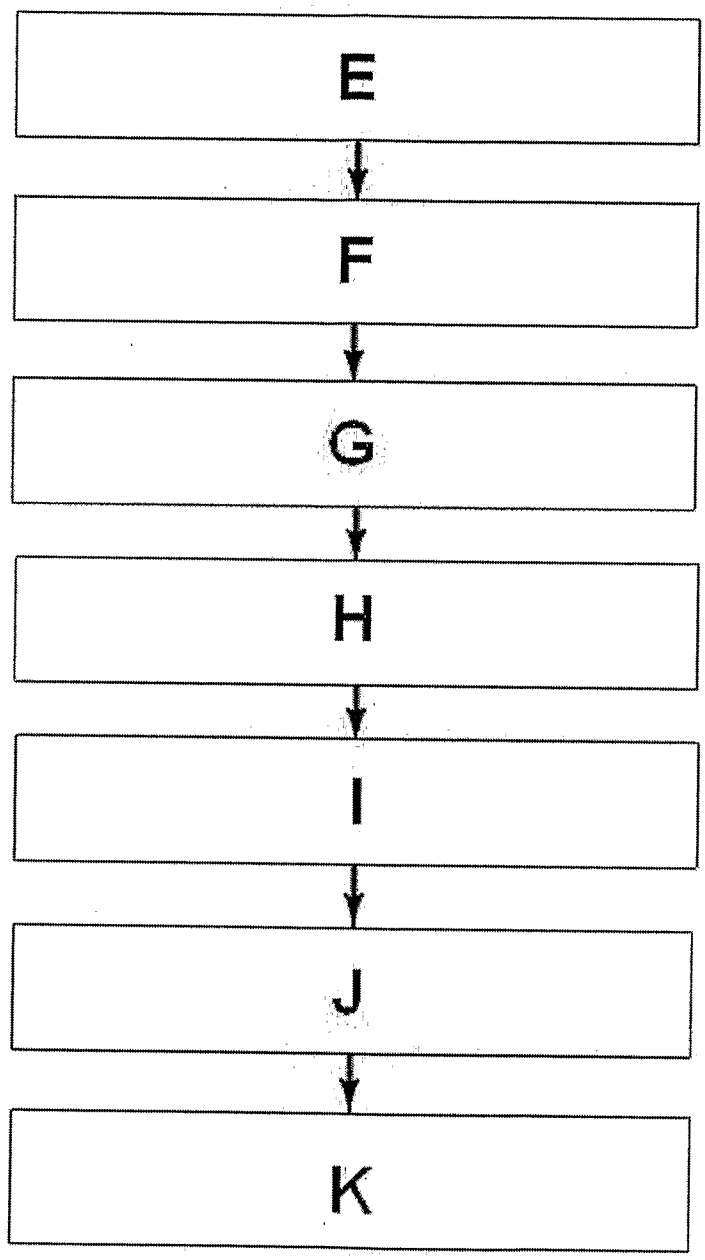

Fig. 2

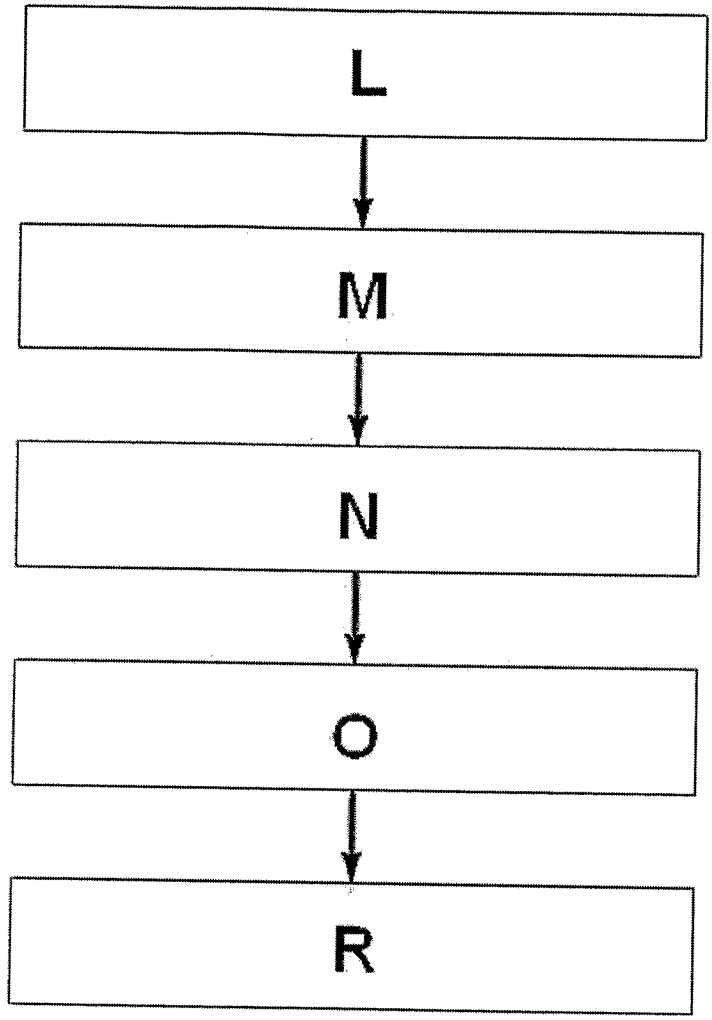

Fig. 3

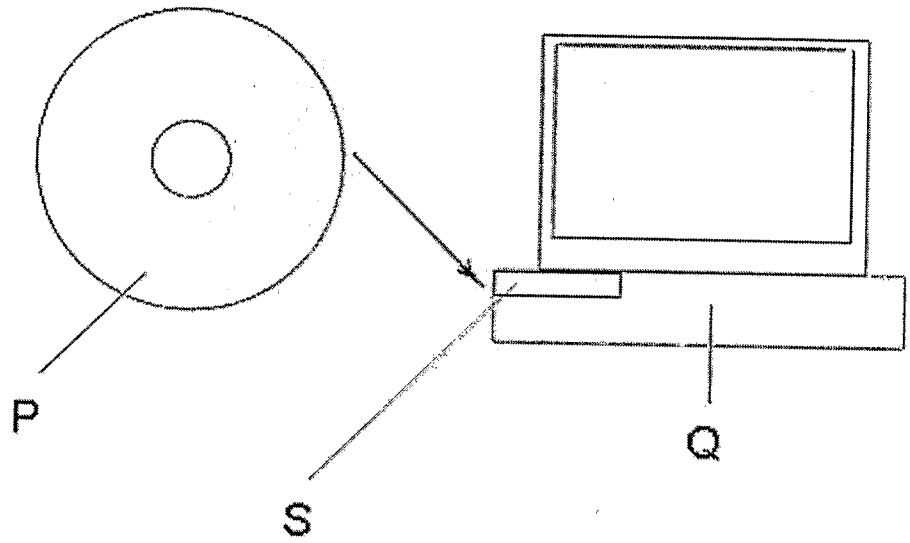

Fig. 4

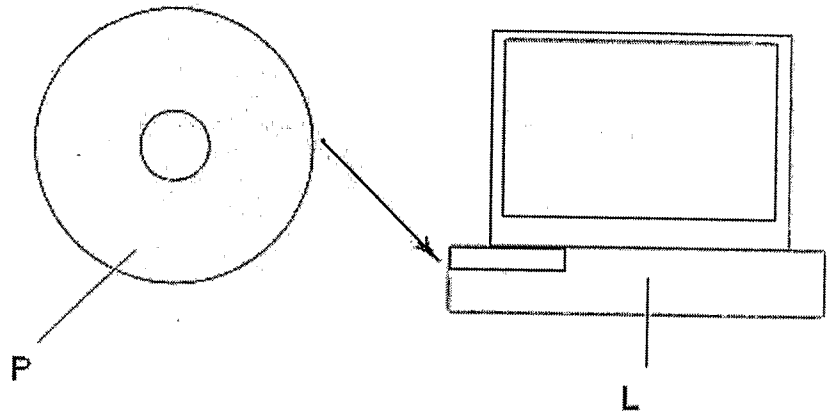

Fig. 5

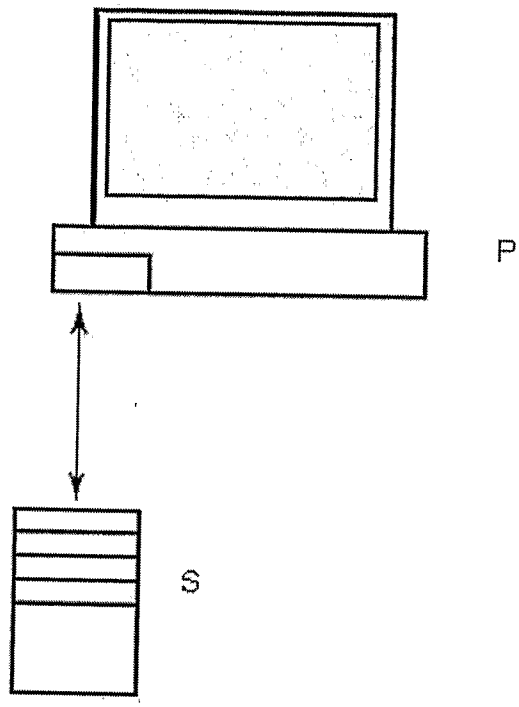

Fig. 6

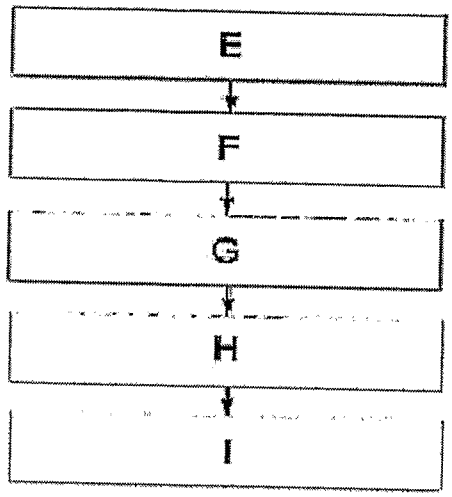

Fig. 7