PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G09C	A2	(11) International Publication Number: **WO 00/28508**
		(43) International Publication Date: 18 May 2000 (18.05.00)

(21) International Application Number: PCT/IL99/00603

(22) International Filing Date: 10 November 1999 (10.11.99)

(30) Priority Data:
126988 10 November 1998 (10.11.98) IL

(71)(72) Applicant and Inventor: BARKAN, Elad [IL/IL]; Brande Street 24, 49600 Petah Tikva (IL).

(74) Agent: ZUTA, Mark; Ben Yehuda Street 19, 49373 Petah Tikva (IL).

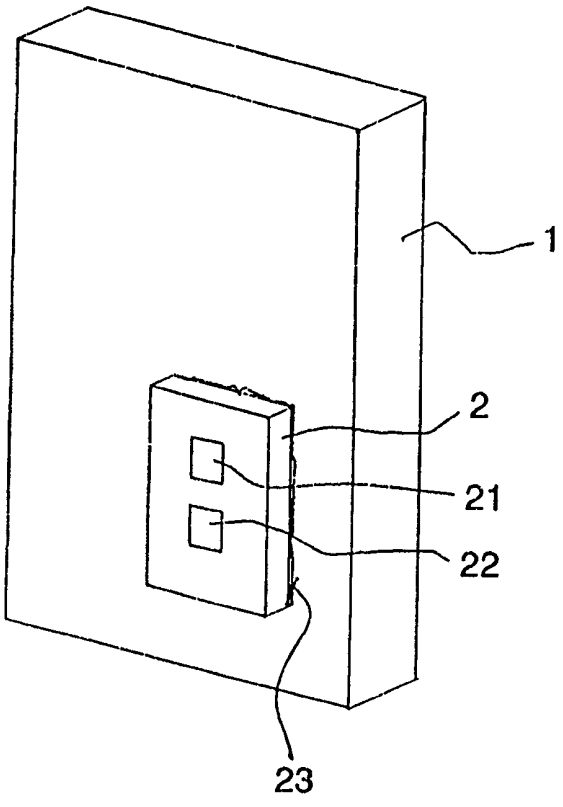
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: MAKING SYSTEM AND METHOD

(57) Abstract

A device for marking a product, comprising: an input/output channel for accepting an inquiry and for answering with marking information stored in the device; means to securely attach the device to the marked product; a digital storage for storing the marking information; a controller for receiving an inquiry through the input/output channel. A method for marking a product comprising the steps of: A) manufacturing an electronic marking device including an input/output channel, means to securely attach the device to the marked product, digital storage means for storing the marking information and additional information, and controller means; B) attaching the marking device to a product to be marked; C) writing product marking information into the storage means.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Marking System and Method

Technical Field

This invention concerns systems for marking objects, and more particularly such systems which include electronic means for holding digital documents and are attachable to an object to be marked, and methods for secure interface with the object.

Background Art

Heretofore, various systems and methods were used to mark objects with desired information. One purpose of marking is to identify the source or manufacturer of a product. Presently used methods to indicate the source of a product are not so effective, this allowing illegitimate manufacturers to sell counterfeits.

For example, a major producer of software packages decided to attach a hologram to its products to prevent the marketing of counterfeit products. The hologram did not help, as competitors succeeded in illegally copying the hologram.

Counterfeit products cause much damage to the legitimate manufacturer. One factor to damage is direct loss of sales to unfair competitors.

Another factor is a damage to the legitimate manufacturer's reputation, as counterfeit products may be of lower quality. Lower quality products may cause damage to users, which may result in lawsuits.

Thus, a problem at present is to mark products, to reliably indicate their source.

Another purpose of marking is to reliably describe the product. For example, assuming that a valuable original painting was identified by experts as such, it is desirable to mark the painting with that information. It is important to prevent, or at least to make it difficult for unauthorized persons to change the description of the product.

Providing a reliable product description allows to use or sell the product, for example. At present, it is difficult to reliably mark a product in a way that will make it difficult for unauthorized people to change that marking.

Another problem with marking products is to indicate ownership. A gun, for example, must have an owner. Ownership may change from the manufacturer to an authorized dealer to a licensed user. It is of paramount importance to achieve a reliable marking of that ownership. At present, labels or paper documents can be easily falsified, this making crime control more difficult.

Another example of ownership marking is in vehicles. Vehicles are stolen, and their parts are sold on the black market. Moreover, complete vehicles are assembled of stolen parts, with the offense very difficult to detect.

The parts in a vehicle are anonymous, without an identity.

Yet another problem with objects marking is to indicate changes in ownership or other important events in the lifetime of a product. For example, a buyer of a car may be interested in prior ownership information, as well as accidents information, tickets and other relevant information relating to the history of that car.

At present, paper documents may be used to indicate part of the above information, however paper documents can be falsified using advanced digital technology like scanners, digital picture processing, color laser printing and more. Thus, paper documents or labels on the product may not provide a reliable indication as to the history of a product.

In the contemporary high tech environment, the traditional methods of marking products are no longer appropriate. New methods for reliable product marking are required, to protect the manufacturers of these products as well as the users of and the business people trading in the products.

It is an object of the present invention to address the problems of the reliable marking of products.

Furthermore, at present there is no secure means to control the operation of various objects. A person who has no authorization may operate a gun or some other's personal objects.

Disclosure of Invention

It is an object of the present invention to provide for a system and method for reliable marking of products.

This object is achieved by a system for reliable marking of products, as disclosed in claim 1. Use of electronic hardware means and digital documents achieves marking means that are more difficult to tamper with than existing marking means.

According to one aspect of the present invention, a product is marked with an electronic device attached to the product. The device includes an input/output channel for accepting an inquiry and for answering with the marking information stored in the device.

Moreover, the device includes means to securely attach it to the marked product, thus addressing a possible danger that the device may be deliberately removed from the legitimate product and attached to a fake. If the marking device is removed from the marked product, it will cease to function as a marking device and cannot be tampered with.

According to a second aspect of the invention, each marking device is devised to include a unique identity, that may include, for example, a unique public/private key pair embedded in the device. The unique identity may be contained in a certificate.

A certificate is a digital document signed with a private key, that is associated with a known public key. The document links the identification of the marking device with that public key.

Moreover, each marking device is equipped with a basic set of instructions or rules and parameters that govern its operation, to achieve a secure and reliable marking device.

According to another aspect of the present invention, the marking device may hold three types of digital documents that define its operation: a certificate to identify the device, one or more permits to define permissible operations and relevant parameters, and one or more permits from certified authorities that the marking device operates according to predefined rules and a required standard.
A permit is a digital document issued and signed by an entity having an unique identification, the document including some piece of information.

According to yet another aspect of the invention, the marking device includes means for accepting additional information, operating rules and parameters which govern its subsequent operation. When required to store additional information and/or rules, the marking device checks the validity of each requirement, according to information and rules already stored therein. Only valid requests will be honored.

After the initial marking of the device, others may write additional permits into the marking device, provided these latter permits are not in conflict with the conditions and/or rules in previously written permits.

A multi-level permit structure is disclosed, with decisions at each level being linked to decisions at adjacent lower and higher levels. Complex decisions can be implemented using logic rules at each level in a multi-level hierarchical structure.

A marking system according to the present invention may include two hierarchical structures: a first hierarchy corresponding to the decision levels in a permit (before marking) and a second hierarchy relating to information and/or other features added after marking.

The marking device may be programmed to respond only after a self-test, so that a response will be issued only if the device has not been tampered with. Moreover, the answer may be conditional upon a specific inquiry, according to predefined rules programmed into the marking device.

The decision of whether a mark is valid or not, is done by the user according to the information displayed to him by the marking device, taking into account additional information the user has at his disposal (information actually held by the user and/or information the user may access). Furthermore, a secure channel is established with various objects, to perform a secure method of control over their operation by a legitimate user.

Further objects, advantages and other features of the present invention will become obvious to those skilled in the art upon reading the disclosure set forth hereinafter.

Brief Description of Drawings

Fig. 1 illustrates an object with electronic marking means attached thereto.

Fig. 2 details the structure of a marking means attached to an object.

Figs. 3A, 3B and 3C detail a method for attaching certificates and permits to a marking device and for their subsequent use, with Fig. 3A detailing the writing of the initial certificate and first permits, Fig. 3B illustrating the process of writing additional information into the marking device, and Fig. 3C illustrating the process of reading the marking information stored in the device.

Fig. 4 details a method for answering inquiries relating to the marking information for a marked object.

Fig. 5 illustrates a multi-level decision structure in a MOL permit.

Figs. 6A and 6B illustrate an example of a multi-level structure, with Fig. 6A detailing the hierarchical issuance of permits, and Fig. 6B detailing part of the vector relating to ownership information.

Modes for Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Fig. 1 illustrates an object 1 to be marked, with an electronic marking device 2 attached thereto. The marking device 2 includes an input/output channel 21 for reading inquiries and for sending out the marking information, an optional power supply input 22 for receiving electrical energy for its operation from an external source, and attaching means 23 to secure device 2 to the marked object 1.

Thus, marking of an object 1 is implemented using electronic hardware means 2 holding the marking information therein. The marking information is stored as one or a plurality of digital documents, as detailed below.

The combination of digital documents and an electronic device securely attached to an object achieves a reliable means for marking the product 1. Thus, the electronic marking device may be better trusted to indicate that the information presented about the product is true, and that it refers to the product the marking device is attached thereto.

In another embodiment of the present invention, the marking device 2 is an integral part of the product to be marked. A product may be manufactured with the marking device included therein.

Furthermore, the marking device 2 may also be used to control an object it is attached to. To this purpose, the marking device 2 may be connected to control inputs in a product. For example, the marked product may be a tape recorder. The marking device 2 then controls the functions of the tape (rewind, play, record) responsive to user's commands.

Only the legitimate user can communicate with the marking device, since the channel is protected with encryption procedures. Similarly, the user can receive information regarding the status of the tape recorder or read information recorded on the tape, through the marking device 2.

Various electrical appliances may be thus controlled through a secure channel using the marking device 2.

In another implementation, a marking device 2 attached to a gun will only allow operation of the gun when the legitimate user is identified by the device 2.

Thus, the marking device 2, when attached to an object, may be used as a secure interface with that object .

In a modular structure, the marking device 2 provides basic services: a reliable indication who is the owner of the device, presentation of certificates, optional addition of information. These are generic functions of the marking device according to the present invention.

The device 2 may also provide extended services, that are adapted to the properties of each object being marked. These may include audio controls in a stereo system, play/record/rewind functions in a tape recorder, immobilizer functions in a gun, etc.

The user may be provided with a remote control unit that can communicate with the marking device over a secure channel.
The extended functions may be either performed with controls on a remote panel, or using controls on the object itself, with the remote control only used to enable those functions.

A simple implementation of the latter implementation is a remote control of the ON/OFF function of a device. When the device is OFF, then all its local controls are inactive. When the device is turned ON through the secure channel and the marking device 2, then the local controls on the object itself may be used .

This achieves a simple implementation, since no special-purpose controls are required on the remote control unit, just means to set the controlled object ON or OFF.

Thus, one control unit may be used to control a plurality of objects, each with a marking device attached thereto. Each device may have a different channel parameters.

A secure channel with the marking device may be achieved using encryption means.

Fig. 2 details the structure of a marking device 2 attached to an object 1 to be marked. The marking device 2 includes an input/output channel 21 for receiving requests for information and for outputting the response with the marking information for the product 1. The information concerning the identity of the product as well as various parameters, the history of the product and operating rules are stored as digital documents in storage means 25.

In the example illustrated in Fig. 3A, the marking device 2 may hold three types of digital documents that define its operation: a certificate 251 to identify the device, a permit 252 from a certified authority to attest that the marking device operates according to predefined rules and a specific standard, and one or more permits 253, 254 to define permissible operations and relevant parameters.

In one embodiment of the invention, each marking device 2 is devised to include a unique identity indicated in certificate 251, that may be include for example a unique public/private key pair embedded in the device.

In another embodiment, the ID is unique but the encryption key is random. Thus, an encryption pair may be generated locally using for example a random numbers generator. In this embodiment, each key needs not be unique.

The certificate 251 is a digital document that may be signed with a private key associated with a known public key, the document linking the identification of the marking device with that public key.

In another implementation, the document may be encrypted with the private key. A digital signature or encryption may be implemented as known in the art.

Throughout the present disclosure, it is to be understood that either a digital signature or encryption may be used to sign a document.

A permit is a digital document issued and signed by an entity having a unique identification. The permit includes some piece of information. Thus, permit 252 indicates that the marking device 2 operates according to predefined rules and a specific standard pertaining to marking devices.

The marking device may be equipped with a basic set of instructions or rules and parameters that govern its operation, to achieve a secure and reliable marking device which are contained, in the example as illustrated, in permits 253 and 254. These are implemented in the software and/or hardware of the marking device.
Similarly, permits 253 or 254 may be used to give the credentials of the ID holder and/or for other information.

Moreover, a permit like 254 may include authorization to issue additional permits. This may be used to achieve a permits hierarchy, where entities at various levels may issue permits, being authorized to do so by entities at higher levels in the hierarchy.

A controller 24 may accept a request from the channel 21, and decide whether to honor that request according to rules and/or parameters stored for example in permits 252, 253 and/or 254. If the decision is positive (to honor the request), then controller 24 assembles a response with predefined parts of the information stored in means 25, and sends the answer out through channel 21. More details on this process are to be found in a later part of the present disclosure.

Controller 24 may be implemented using digital circuits as known in the art to implement devices capable of reading and writing digital data and making decisions according to a predefined computer program.

Microcontrolled logic may be used or a central processing unit with adequate peripheral components.

In another embodiment, device 2 is implemented as a smart card processing unit SCPU that can be attached to an object 1 to be marked. The SCPU may include means to remove all its memory if someone is tampering with the device.

The marking device 2 is secured to the object to be marked 1 using attaching means 23. Means 23 are so devised that removal of device 2 will disable the marking device, to prevent its unauthorized removal from the correct object 1 and its subsequent attachment to another object, which may mislead a user. Thus, if marking device 2 is removed from the object 1 it is intended to mark, then the attaching means 23 causes it to cease its operation.

One possible embodiment of means 23 is a strong glue attached to the microchip itself on the side the electronic circuit is etched thereon, so that the removal by force of device 2 will damage the chip.
Another embodiment may include a glue with a plurality of fine wires (not shown) immersed therein, so that removal of marking device 2 breaks the wires and device 2 becomes permanently damaged.

Thus, the marking device 2 may be securely attached to the marked product 1, to address a possible danger of the device being deliberately removed from the legitimate product and attached to a fake.

In another embodiment, the marking device may be attached during the manufacture of the product 1, or may be made an integral part thereof.

Since the marking device 2 is an electronic device, it needs a source of electrical power to operate. In one embodiment, a battery (not shown) may be used for that purpose. This may have disadvantages, like a higher cost, larger size and/or the need to periodically replace the battery.
In another implementation, the device includes a power supply input 22 for the application of power when a user desires to read the marking information, or to program additional information like permits into it.

Power supply input 22 may include (not shown) electrical contacts for the direct connection to an external electrical source, or a radiation receiver means for the noncontact application of power.

For example, a solar cell may be used to convert light energy into electrical power. In another example, a coil may be used to transfer energy to the device 2 through an alternating magnetic field.

In another embodiment, power supply 22 may include energy storage means like a capacitor (not shown), that may be charged from an external source. When the capacitor is charged to a suitable level, sensor means in the device activate the device to communicate with the outside. In this state, the marking device 2 has enough energy to complete its task, and is thus independent of external energy sources.

The energy already stored in the device prevents tampering with the marking device by way of interrupting its power supply, since the marking device starts operating only when it has stored enough energy to allow its independent operation. A capacitor may be otherwise used together with an internal battery or an external energy source.

In yet another embodiment (not shown), one device may implement both the input/output channel 21 and the power supply input 22, using a common channel for both conveying the information to/from the marking device and applying electrical energy to the device.

The marking device 2 may include means for communicating with other marking devices. This may be used to exchange information and/or permits between marking devices, or to achieve a hierarchical marking structure.

For example, various parts in a vehicle may each have its separate marking device. All these marking devices may be connected to each other in a network and to a marking device that communicates with the outside, for example with the vehicle computer. This allows the vehicle computer to ensure the integrity of the car, without the user need to communicate with each marking device for each part in the car.

A case 26 may be used to contain all the parts of the marking device 2, to provide mechanical protection.

Figs. 3A, 3B and 3C detail a method for attaching certificates and/or permits to a marking device and for their subsequent use, with Fig. 3A detailing the writing of the initial certificate 251 and first permits 252 and 253. The marking device 2 may be implemented as a monolithic integrated circuit IC, a module or another implementation of an electronic circuit.

The device 2 is produced by a marking device manufacturer 31. A certificate C1 251, which includes unique identification information for each device 2, is permanently written into the marking device 2. The certificate 251 may be written during the production of the chip, using for example a mask in the IC or a Read Only Memory ROM. In another implementation, the certificate may be programmed in the field, using for example a Programmable Read Only Memory PROM, an EPROM, EEPROM or flash memory as known in the art. In a preferred embodiment, the certificate is written by the manufacturer 31 of the device 2, to ensure that each marking device 2 has an unique identification.

The manufacturer 31 receives from a standards institute 315 a digital document attesting to the compliance of marking device 2 with predefined rules and a required standard. The manufacturer issues a digital document under that one which is written into device 2 as permit 252. The document may be read by users, to ensure that the marking device may be trusted to act in a reliable way.

A certificate authority 316 may create a certificate for the device. Alternately, the certificate may be created by one of the manufacturers 31 or 32.

A manufacturer of products 32 attaches the marking device 2 to a product and writes additional information relating to that manufacturer and the product the marking device 2 is attached thereto.
The manufacturer 32 may receive marking authorization as a permit called "Marker Operating License" or MOL, from a marking authority 325.

That authorization may be included in the permit written into device 2 by manufacturer 32, so that the permit in device 2 may be traced to authority 325 to allow users to verify that the marking was indeed authorized.

The marking device 2 includes means (not shown) for only allowing a single session of certificate or encryption keys programming therein. After the unique identification of the marking device 2 is written in, the device 2 will not allow subsequent changes in the identification information.

For example, if the identification information is written in a mask ROM by the device manufacturer, the inherent structure of this memory prevents subsequent changes therein. If the identification is programmed in the field in an EPROM for example, that EPROM may include an additional bit, the enable bit. After entering the identification information for the device 2, the enable bit is programmed into a state that prevents (disables) further programming of the marking device 2.

In still another embodiment of the invention, the certificate or identification information is written into a programmable memory according to information received from outside, however the controller in device 2 is so programmed as to prevent such writing if a certificate or identification information was already written into device 2.

In yet another embodiment, device 2 includes means for creating an encryption key pair comprising a public and a private key. The private key is written into the internal memory of device 2 and is not available outside. The public key is sent out, to be encrypted or signed digitally by an outside authority like a manufacturer, importer, a government agency or another certificate-issuing authority. The resulting digital document or certificate is transferred back to device 2 and is written therein as part of its identification.

Alternately, a manufacturer may create locally the encryption key pair using a random generator and write these keys in the marking device 2.

In another embodiment, the private/public keys are allowed to be changed, as long as there is an ID that remains unchanged. After a change, a new certificate may be needed.

A possible problem with marking devices is false marking.
If all the information in the marking device may be read by a user,
there is the danger of the private key and the ID being read as well.
The private key and the ID can then be written to another, false product
or to a plurality of false products.
Thus, false marking may be performed.

The above problem may be solved using the abovedetailed methods. In one method, the private key may only be generated by a certified manufacturer. In another method, the private key is generated in the marking device itself. The private key in the marking device cannot be read by users.

In a preferred embodiment, after writing the certificate 251 to define the unique identity of device 2 and permit 252 indicating the SCPU's conformance to permit standards, a third digital document is written in device 2, that is the permit P2 253. The permit 253 may define the basic mode of operation of the device 2. For example, it may define the use of the certificate 251 and the encryption keys therein. It may define a marking authority, that is an authority to mark various products, for example the Government of a country or a specific Governmental Department or Ministry. Permit 253 may actually mark the product, to indicate that it is an object of a specific kind.

In one embodiment of the invention, after receiving a permit indicating the type of product, the marking device 2 will not accept another permit claiming the product to be different than that initial marking.
Certificates and permits may be attested to by the issuing authority (the authority that prepared these digital documents) using one of two possible methods: either the document is encrypted with the private key of the issuer, or a digital signature is added to the document, with the document itself not being encrypted.

Throughout the present disclosure it should be understood that either encryption or digital signature of these documents is possible.

In one embodiment of the invention, only authorized parties may mark a device 2, as indicated in a permit called "Marker Operating License" or MOL. When device 2 receives a request by an objects manufacturer 32 to mark the device, manufacturer 32 has to present a permit or MOL signed by that marking authority, indicating that manufacturer 32 indeed has the right to mark products.

It is assumed that the digital ID of the Government or the designated marking authority will be known to all the citizens, so that the permit issued by that authority, which is encrypted or signed with their private key, can be verified by anyone using the corresponding public key or ID.

A permit may be transferable in a predefined hierarchical structure, that is a marking authority may empower others to mark products as well. Thus, an authorized party may present a plurality of permits, which may be used to track their authorization to an ultimate, publicly known marking authority.

If the permit presented by manufacturer 32 is acceptable, according to certificate 251 and permit 252 in the device 2, then device 2 will accept a digital document or permit P2 253 and will write that permit in the permanent, nonvolatile memory of device 2.

In another embodiment of the invention, anyone can mark the device 2 by writing a digital document therein. The first permit will be accepted without check of originator ID. A digital document may include information, rules and/or parameters, all signed by the marking entity.

Additionally, the document includes any permit or permits attesting to the authority of that entity to perform that marking. When the document is read by others, the reliability of the information therein may be evaluated based on those permits, so the reader may decide for himself whether that marking is acceptable.

For example, let's assume that vehicle marking can be only performed or authorized to be done by the Ministry of Transportation. If a car marking device contains information signed by a person without authorization from the Ministry of Transportation, that information will be simply ignored, as if the marking was not correct.

The marking device includes means for accepting additional information and operating rules, which govern its subsequent operation, in the form of digital documents like MOLs in a specific marking format.

When required to store additional information and/or rules, the marking device checks the validity of each requirement, according to information and rules already stored therein. Only valid requests will be honored.

The permit 253 is encrypted or signed by manufacturer 32, for example using their private encryption key. This enables each manufacturer 32 of products to reliably mark their products and be responsible for the product and its marking.

The permit presented by manufacturer 32 (the MOL) may also state whether the permit is transferable, that is whether manufacturer 32 may empower others to write marking information into device 2.

In one embodiment of the invention, the highest marking authority may be the Government of a country where the marking device is used. The Government may issue permits or a Marker Operating License MOL to the people or firms or organizations that perform the actual marking of products. The actual marking may be done by importers and/or manufacturers of the relevant products.

A marking device 2 may be devised to accept either a single mark or a plurality of marks. In the former case, device 2 is programmed to accept only a single permit or marking information. It may also accept updates to the information stored therein, for example the same information signed with another digital key, or an enlarged package containing the previous information with additions that are in compliance with that prior information. The device may be programmed to accept an update, even if it contains new information, from the same source, that is a completely new permit may be issued by the same authority that issued the original permit.

In the latter case, the marking device 2 will accept a plurality of permits, rules and/or parameters and will store all the information in the marking device, to be presented to users (readers of the marking).
For example, a marking device in a car may include an original description from the manufacturer of that car. When the car is imported to another country, the vehicle registration authority there may add another permit reflecting the authorization/registration of the vehicle in that country.
That second permit may be written into the marking device by the importer of the car.

The marking device may allow cancellation of marks therein by an authorized entity, if the initial permit stored therein permits it.

In the above description, a certificate was used to reliably link the unique identification of the marking device 2 with a known public key.

Thus, a known authority with a known public key attests as to the correctness of the identity or public key of the device 2. There is no need that all marking devices be issued certificates directly by that known authority. Others may be granted authorization to issue certificates by that authority, using certificates signed by that authority for that purpose.

A hierarchy of certificates may thus be formed, wherein for example a first person who is marking devices 2 has a certificate from a second person to do so, with that second person, among others, having a certificate from a third person.

When the first person marks a product, he also attaches to the document written therein the certificates from the second and third person. Thus, anyone reading the certificate in device 2 can verify all the certificates to ensure that the issuing authority (the first person) indeed has authorization ultimately derived from the third person.

A certificate or permit may be updated, subject to predefined rules written therein. For example, a new certificate will be accepted as long as it contains the same information (the same identity number or public key for the marking device).
An update may reflect, for example, a new public key used by the known authority, the third person. In a hierarchical certificates structure, when a center or member of that structure changes its encryption keys, it may be necessary for all certificates to update so as to use the new keys.

The marking device supports the hierarchical certificates structure with the means for updating certificates contained therein.

The mechanism for certificates updating may be used to achieve a dynamic marking device, which is capable of multiple updates. A marking device may include means for automatically updating a certificate to an updated version. For example, when the device is presented with a certificate issued at a later date than that of a corresponding certificate stored in the device, the marking device may automatically replace the stored certificate with the new, updated certificate.

One of the parameters written into the marking device indicates whether a permit or certificate may be updated or not. Various change limitations may be included, relating to the various digital documents in the marking device. Another parameter indicates whether the marking device will accept just one permit or a plurality thereof.

Method for use of marking device

The life cycle of a marked product thus may include the following stages:

A. Manufacture of marking device. The device includes a controller or computer.

Writing an identification digital information package into the storage means in the device. The information uniquely identifies each marking device. This may include, for example, the programming of an ID or certificate into the marking device. Only one identification information may be programmed, however that information may be later updated if the device is programmed to accept updates.

A permit indicating the device operates according to specific standards for permits, and basic rules or code that govern its operation are then written into the marking device.

B. Attachment of the marking device to a product to be marked.

C. Writing product marking information into the storage means in the marking device. This may include, for example, a marking permit written into the device. In single marking mode, the device will accept only one permit, but may allow later updates to it, if the device is programmed to accept updates.

D. Use of the marking device, including presenting the marking information to the public and/or authorized persons, and/or updating the permit or certificate therein. This stage may be performed many times.
End of method.

In another embodiment, in step (A) the marking device will generate an encryption key pair, as detailed elsewhere in the present disclosure.

In yet another embodiment, step (D) also includes writing additional permits into the device, as well as updates of each permit.

It is possible to change the order of performing the above stages, without departing from the scope of the present invention.

A "Marker Operating License" or MOL may include the following information:

1. Receiver identification

a) Issuer identification (ID corresponding, for example to Government or a designated Department or Agency, having a specific ID)

b) Receiver identification (Marker's ID)

c) Permit type: MOL for example

d) Serial number

2. Marking propagation

A single layer of marking authorities may be defined, or a hierarchical structure (tree-like for example) may be implemented by forbidding or permitting propagation, respectively. Date control may be implemented.

3. On expiration activities

The MOL may include an expiry date, in which case its validity has a limited time interval. Additional information in the MOL may specify what is to be done when that expiry date is met. One possibility is to kill the permit, that is to destroy all the information therein.
Another possibility is to "vegetate" , that is do nothing until a specific event happens. This may allow for "revival" of the MOL under certain terms, or to allow only specific activities. For example, the device may only report its identity, without additional information.

4. Marking limitations – a set of rules for specific activities, together with various limitations, for example relating to specific products or types of products, or referring to specific lists. These lists may be included in the device or may appear in other permits.
Additions to and exclusions from a list may be included as well. Various timing limitations may be set, for example timing limits between the various markings. A limit to the number and/or types of products that can be marked may be set as well. Other limitations may be included.

The above information may be stored in predefined fields in a digital document or permit.

Fig. 3B illustrates a possible process of writing additional information into the marking device 2. A request from marking authority 33 to add to the information in device 2 will be evaluated according to the certificate 251 and permits 252, 253 already written in device 2. If the permit presented by authority 33 is acceptable, that is the permit is traceable to the higher marking authority indicated in the digital documents in device 2, then device 2 will accept a permit P3 254 and will write it in the digital nonvolatile memory of the device.

Otherwise, if device 2 is presented with an updated version of a permit stored therein, the new permit will be used to automatically replace the old permit in device 2.

Authority 33 may write information regarding changes in ownership, for example. Only information that does not contradict the information and/or rules already written into the marking device 2 will be accepted.
Thus, if device 2 is used to mark a car, then an authorized change in ownership may be recorded therein, together with additional relevant information like the date, name of new owner and more.
If the car was involved in an accident, the Police or insurance company may write details regarding that accident in device 2.

In another setup, authorization from the current owner and possibly future owners, in the form of a permit, may be required or enough to perform a change in ownership. In a possible setup, there may be no need for an authority's involvement in the transaction.

Thus, the present invention gives an "identity" and "history" to an object that previously was indistinguishable and without a readily available record of past events. Although objects are being marked at present, the marking may be tampered with relative ease. Although some records on objects are kept at present in various locations, these records may not be readily accessible and/or may be tampered with. The present disclosure relates to electronic marking means that reliably assign an identity and a history to various objects or products.

Additionally, device 2 may include a list of allowed and/or forbidden activities as stated in the MOL. When the marked product is required to perform a task, a controller in the product may check that list in the marking device to decide whether to allow that activity. For example, the marking device in a car may only permit its use by the registered owner.

The car computer may connect to the marking device, check the operation rules/permits and operate the car accordingly. In another embodiment, a communication link between the marking device and the car computer allows the transmission of a question or inquiry to the marking device. If the requested operation is permitted, then the marking device will issue a permit to the car computer.
In still another embodiment, all the requests to a car may pass through the marking device.

In another embodiment, the marking device may contain a list of permissible operations/information to disclose, together with an indication of the person or persons allowed to do each one. A request to the marking device will include the desired operation together with the identification of the person requiring it. The marking device will present the information or perform as required if the request and ID of inquirer are compatible with that list. The dialog with the marking device may include a challenge as known in the art.

The list of permissible operations may be hierarchical, as detailed below.

A permit may include various rules and/or parameters, as well as pointers to other permits or locations where other permits may be found. Thus a multi-level, interdepartmental permit may be achieved, allowing a product to receive several permits from several authorities, without the need to actually contact all those authorities personally each time. This may lessen the bureaucratic burden associated with the issuance of multiple permits for a product.
The MOL companion may include the required additional permits, to allow a reader to evaluate the MOL.

Fig. 3C illustrates the process of reading the marking information stored in device 2. A user communicates with device 2 and, if predefined conditions are met, then device 2 presents all or part of the marking information stored therein.

The predefined conditions are optional – in another embodiment the device will unconditionally present the marking information .

The presented information may include, for example, a permit or permits together with the permits and/or certificate of the marking party.

User 34 may thus obtain information relating to the marked product, like the identity of that product, details on the manufacturer of the product and production date, as well as various events in the past of the product like changes in ownership, accidents, repairs etc.

Fig. 4 details an example of a method for answering inquiries relating to the marking information relating to a marked object and for writing additional information in the device.
This relates, for example, to the processes illustrated in Figs. 3B and 3C, referring to the method implemented in marking device 2 (see Fig. 2) by controller 24 therein.

Method for answering marking inquiries

A. The marking device becomes active when power is applied to the device (state 41), that is when the device is to be read or additional information is to be written therein.

The state 41 is not necessary when the device is continuously connected to a source of electrical power, however this may not be a practical solution.

B. The device enters a waiting state 42, waiting for an input signal from an external source, indicating a request for information or a request to write new information into the device. When such a request is received, then the device steps to state 43 (step C).

C. The device checks for its integrity and the attachment to an object being marked in state 43. If the device functions OK and no tampering with was detected, then go to step E (state 45), otherwise go to step D (state 44).

D. The device ceases all its activities and will communicate no longer with any external device (state 44). No marking information will be presented any longer, this preventing the attachment of the device to a false product .

Optionally, the controller in the marking device may write in an internal nonvolatile memory the fact that the device was tampered with. This may be subsequently read in step (C) the next time, so even if an unauthorized person may later overcome the protection means of the marking device, the marking device will cease to function as such.
In a preferred embodiment, the memory of the device is erased or destroyed in an irreversible operation.

E. The information from the external source is evaluated against the information stored in the marking device, including the certificate and permits, in state 45.

If the received request is legitimate, then the marking device answers by sending out the marking information stored therein.
In one embodiment of the invention, the request is only checked for its being a request for information, so that practically the device responds to anyone.
In another embodiment, the marking device only responds to legitimate users, that is users who can present a predefined permit signed by a specific authority.

The above conditions may be part of the marking license or operating permit (MOL).

In yet another embodiment of the invention, the information in the device is compartmentalized, with various parts of the information being made available to authorized users. For example, the identification of a car including its manufacturer and date of production may be presented to anyone. Information relating to present ownership may be presented only to police officers. Still more sensitive information relating for example to past owners, accidents or traffic offenses may be only presented to persons authorized to receive this information.

F. The device next checks (state 46) whether new information is to be written into the marking device. If yes, then go to step G, else go to step H (state 48) to go back to the waiting state 42 (step B).

G. The device receives information to be written therein, as digital documents or permits. If the new information corresponds to the permits in the device (that is, the information is written by a marking authority having the right permit to do so), then the new information is written in the marking device (state 47).

H. (state 48) go back to the waiting state 42 (step B).

End of method.

Notes:

1. Steps (C), (D) provide the protection against tampering with the device if the device does not include means for self-destruction when it is being removed from the marked product. Even when such means are present as detailed above, the software protection achieved in these steps provide an additional layer of protection.

2. The marking device may be programmed to respond only after a self-test, so that a response will be issued only if the device has not been tampered with. Moreover, the answer may be conditional, according to predefined rules programmed into the marking device in a permit.

A Government or other highest marking authority may issue permits or a Marker Operating License (MOL) to the people or firms or organizations that perform the actual marking of products. The actual marking may be done by importers and/or manufacturers of the relevant products. The MOL may be self-contained, or may indicate other permits that are to be included as attachments or may be found elsewhere. A web of permits may thus be formed, with a permit indicating other permit or permits that are to be included in the device or are to be found elsewhere.

A permit may indicate the properties of a marked product, and may include all or part of the following items:

1. Marking propagation
   a) Can the marker allow other entities to mark in his name and, if so, what are the limitations for that propagation.
   b) Is the marker limited in the number of marks he can create.
   c) Is the marker operation limited in time and, if so, the date of expiry of their authorization.

2. Marking limitations
   a) What type of object or product can be marked, and what are the actions and rules to follow. A list of products or product types may be included. A standard list may be referenced, possibly with additions and/or exclusions. The list may be made of object limitations.

3. Object limitations

a) Object ownership limitations

1) Can the object be owned? It is possible that an object is owned by anyone who presently holds it, in case the object cannot be registered as owned by a specific user. The present holder may control the object. Otherwise, an ownership in an object may be registered.

2) Must the object be owned? There are objects, for example hand guns, that must have a specific ownership at any time, and be registered as such.

3) Can the ownership be changed? Some products like a toothbrush or a shaving razor cannot change ownership.

4) Are there limitations for changing ownership? Some products require a special license of a new owner. For example, a car may require a driving license, or a gun may require a license to hold it.

5) Owner anonymity limitations. An object may be required to report its ownership when asked to do so, or may not report ownership, or may report ownership under certain conditions. For example, an object may not report its ownership to anyone but a police officer.

6) Owner traceability. The marking device for an object may optionally store and report a list of prior owners of the marked object.

b) Temporal usage information. Specific criteria may be defined and checked, referring to services beyond the basic services being requested by someone who is not the present owner of the object.

These services refer to control or use of the object without an ownership thereto.

1) Is temporal use allowed? For example, a gun owner is not allowed to permit others to use it.

2) Temporal usage limitations. Maybe a specific license is required, for example a driving license.

c) Usage limitations. The following are example of criteria that may be checked for services beyond the basic services: A driver's license; a license or statement that that person is not drunk, like that issued by an alcohol vapor detecting machine.

d) Service usage limitations vector. Several criteria may be checked when a service is asked, for example:

1) Limitations of use – a car may not be allowed to exceed a predefined speed, however a special license may permit that. To open the engine head, another license may be required, like a technician license.

e) Optional additional information.

The possible services that the marking device may perform for an external user or authority may be divided into two groups, that is basic services and extended services.

Basic services may include, for example:

1. Request ID, when someone asks for the unique identification of the marking device.

2. Request owner, when someone asks about the present ownership on the device or product.

3. Ownership changes request, when someone asks for changes in ownership

4. Clear previous ownership, when the marking device is asked to clear the list of prior owners. Such a request may or may not be permissible, according to the initial programming of the marking device.

5. Change properties, when the marking device is required to change certain properties of a service. A request should include information indicating what service to change, and what change is required.
The marking device may initially assign default values to all the properties therein, according to the MOL.
The default properties preferably refer to the extended services.

6. On expiration - this is an optional basic service that is executed when the MOL expires.

7. Add extended service – an optional basic service that allows to add extended services.

8. Remove extended service – an optional basic service that allows to remove extended services.

Extended services are additional services that are application-dependent. Various extended services may be defined, as the need be.
For each service, a vector is defined. The data in the vector may include:

1. Service name
2. Service code
3. Use limitations (Header, footer)
4. Display limitations (Header, footer)
5. MOL external addition limitation (Header, footer)
6. MOL external removal limitation (Header, footer)

In all the above items, specific information may be included, or it may refer to specific lists of products, options and operations.

Where lists are used, a list may be actually included or reference may be made to an external list to be found in another location.
When referring to a list, there may be included additions to the list or items to be excluded therefrom.

Fig. 5 illustrates a multi-level decision structure in a MOL permit.

The list of permissible operations may be hierarchical, including for example levels 51, 52, 53 and 54, each level corresponding to a permit level.
A typical level 52 includes a header 521 and a footer 522.
The header 521 and the footer 522 include logical rules and may include function calls referring to adjacent levels in the hierarchy.
Each set of rules is a Boolean function, with the result being 1 or 0, corresponding to True or False.

Method for multi-level decision

The operation of the multi-level decision structure is as follows:

A. Controller 24 makes an inquiry, for which a decision is required. The inquiry is presented to the header 511 in the first level 51 of the permit.

B. The logic rules in header 511 are evaluated to reach a decision. One of the rules in header 511 indicates whether additions to the rules is allowed. If negative, then the final decision is reached in header 511. If positive, then the rules in the adjacent lower level 521 are evaluated next.

C. The rules in header 521 are evaluated, and the lower adjacent header in level 53 is activated if necessary. Similarly, the decision rules evaluation is passed to headers in lower levels.

If a final decision is reached at in one of the headers, the result is transferred up, from one level to the adjacent higher level, up to the highest level 51 where the result is delivered to controller 24.

D. At the lowest level (level 54 in the example), the inquiry is passed to the footer 542 there.

E. The inquiry is passed from one footer to the next higher footer for rules evaluation there, until a level is reached where a final decision is made. The decision, or result of the Boolean rules, is sent down, that is from one footer to the adjacent lower footer, down to the footer in the lowest level 54. The decision is passed up through adjacent headers, until the decision reaches the header 511 in level 51.
End of method.

As shown in Fig. 5, level 52 includes a header 521 that may call header 531, so that the lower level 53 may participate in the decision taking.
Similarly, level 51 includes header 511 and footer 512; level 54 includes header 541 and footer 542.

The footer 522 includes default rules for the level 52. These rules can call footer 512. The footer at the first level 51 cannot reference a previous footer since there is none.

Each of the illustrated levels 51, 52, 53 and 54 thus includes a header with logic rules and links to adjacent levels.

A vector may be assigned to each operation, including the various rules at a given level in the hierarchy, as well as rules connecting to the two adjacent levels therein.
The rules may be written in the Java language for example.

In a marking system according to the present invention, there may be two hierarchies: One hierarchy corresponding to the decision levels in a permit, and a second hierarchy relating to the limitations after a product has been marked.

A permit called "Marker Operating License" or MOL, may be built of several permit levels. Every entity that receives a MOL can issue a next level permit, under the authorization of the permit it got from the previous level.

For example:

A first (highest) level may be a Government authorizing a car importer to mark a car.

A second level may be the car importer, authorizing a worker to mark a car.
A third level may be the worker authorizing the car to be of a specific kind.

Each next level is issued under the limitations of the previous level.

The whole permit list is called a MOL, and there are levels as described above.

When dealing with a marking device, there is a need to define actions that can be performed.
Examples of actions: Change ownership, display owners, etc.

Note: Throughout the present disclosure, the terms "action" and "service" are used interchangeably and are to be understood to have the same meaning.

The definition of actions may appear in the MOL in object properties of each level. Also, after an object has been marked, there can be addition outside of the MOL (external levels).
If in a MOL level there is a reference to a list, then it may be treated as if that list actually appeared in that level.

For each action a vector may be provided, which may contain the following data:

a. action name

b. action code

c. action use limitations

d. MOL external addition limitations

e. MOL external removal limitations

f. display limitations

An action name is a name for the action to be described.
The action code may be a Java code to be performed when this action is executed. The code may reference other actions to be performed. It is preferably supplied internally or by first level.

Limitations may be implemented as Boolean functions. These functions may be implemented in the Java language for example.

Limitations are evaluated to give a result that is either TRUE or FALSE. According to the result, the requested action will be performed or denied.

Each action's limitations are evaluated when the action is requested.

MOL external levels can be added. They are single level permits from the entity that is issuing to the SCPU, and contain data similar to a MOL level. MOL external addition limitations are evaluated when there is a request to add an external level.

MOL external removal limitations are evaluated when there is a request to remove the last external addition.

The limitations may appear on each level of the MOL.
The first, or highest level, has full freedom of action. On the lower levels, each level may include limitations set by higher levels. Each level may also set a default choice, possibly in the footer, indicative of lower levels it may reference.

In one embodiment of the above method, the limitations are established as detailed below. Each level (either regular or external) has two places to hold limitations, that is a header and a footer.
Each one of the header and footer includes a Boolean (logic) expression that may be evaluated to give either a true or false result. The expression may reference any kind of variables, functions and/or constants in the system.

Each header may reference the next (lower) level header, for example by calling the next level header function which may be generally named "NextLevel" . This function gets a true or false value, depending on the result of the evaluation at the lower level.
The footer may reference the previous (higher) level footer in the same way.
The above applies to all levels except the first (highest level) footer, which is not allowed to reference the previous level, since there is none.

The chaining of the "NextLevel" in this embodiment, therefore, will be in that order:

1. The headers of all levels, starting from the first level header and ending with the last level header. If there are external levels, then the last external level header.
2. The header of the last level is followed by the footer of the last level.
3. The footers of all the levels, starting with the last level up to the first level's footer.

Figs. 6A and 6B illustrate an example of a multi-level decision, with Fig. 6A detailing the hierarchical issuance of permits.
Assuming that the Government 35 allows a car manufacturer 36 to mark cars, then the Government 35 will issue a MOL permit to the car manufacturer 36, that is a first level permit. The car manufacturer 36 may now issue a MOL marking permit under it, to the car 37 itself. This MOL is a second level permit.

In the example as illustrated, the Government 35 demands that a car would reveal its ownership information when asked to by a police officer. Also, the Government allows lower levels in the hierarchy to set other conditions in which a car would reveal the ownership information. The above terms are defined in the Boolean equations in header 551 of level 55 in the permit.
Level 55, see Fig. 6B , details part of the first level MOL permit.
Fig. 6B details part of the vector relating to ownership information.

Since the Government permit allows lower levels to add conditions, the car manufacturer 36 added the second level 56 of the permit, indicating that a car should reveal ownership information to a qualified technician during working hours, that is when the time is between 8:00 and 17:00 .

Method of evaluation of the multi-level permit

A. When a car is asked to display ownership information, the requester is challenged as known in the art to identify himself. The response is used in the subsequent stages of Boolean equations evaluation.

B. The header 551 of the MOL is evaluated. If the requester is a police officer, the Boolean equation will get a True value, indicating that the information can be revealed. End of method.

C. There is a NextLevel reference, indicating that the header 561 of the next level 56 should be evaluated. Therefore, the equation in header 561 is next being evaluated.

D. If the requester is a qualified technician and the time is between 8:00 and 17:00 , then the Boolean equation will get a True value. In this case, the NextLevel variable in the first level header 551 will get a True value, this resulting in a True final value. The information can be revealed. End of method.

E. There is a NextLevel reference, pointing to the footer 562, since level 56 is the lowest level in the permit.
According to the present method, NextLevel references in the lowest level always go to the footer in the same level.

F. The footer 562 references to NextLevel, thus the next footer is evaluated. The next footer is footer 552 in the level 55 that is adjacent to level 56. The value of footer 552 is False, therefore the NextLevel variable receives a False value, and the whole process gives a False result. The final result is that the ownership information will not be revealed in this case. End of method.

A possible embodiment of the marking device is as a device embedded in a personal computer. The device may be implemented as an integrated circuit, a module or a board. The device may be embedded as a component that is part of the motherboard or other part of the computer. The marking device is electrically connected to the computer to allow communications between the computer and the marking device. Thus, the computer may read the marking information and perform various tasks accordingly.

The device may thus be used to mark a computer, so that computer acquires a unique identity. There may be various uses to such a marked computer, for example to permit software packages to run only on a specific computer. This may help eliminate software piracy and allow elaborate uses such as pay-for-use software.

Moreover, the marking device may be used to mark cellular phones. This is useful to help prevent cloning of cellular phones. A cellular system may identify each wireless phone, to prevent fraud.

Furthermore, the marking device of the present invention may also be used to control an object it is attached to. To this purpose, the marking device may be connected to control inputs in a product.

Only the legitimate user can communicate with the marking device, since the channel is protected with encryption procedures. Similarly, the user can receive information regarding the status of the marked object, through the marking device.

Various electrical appliances may be thus controlled through a secure channel using the marking device.

Thus, the marking device, when attached to an object, may be used as a secure interface with that object .

A simple implementation of the latter implementation is a remote control of the ON/OFF function of a device. When the device is OFF, then all its local controls are inactive. When the device is turned ON through the secure channel and the marking device , then the local controls on the object itself may be used .

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore.

Claims

1. A device for marking a product, comprising:

A. An input/output channel for accepting an inquiry and for answering with marking information stored in the device;

B. means to securely attach the device to the marked product, including means for preventing further answering to inquiries if it detects that the marking device was removed from the product;

C. digital storage means for storing the marking information together with information for uniquely identifying the marking device; and

D. controller means for receiving the inquiry through the input/output channel, for reading the information in the storage means and for transferring the information to the input/output channel according to predefined rules.

2. The device for marking a product according to claim 1, wherein the unique identification information is stored as a digital document which is encrypted or signed by a known authority.

3. The device for marking a product according to claim 2, wherein the digital document includes a public key and wherein the storage means further includes a private key corresponding to the public key in a public encryption scheme.

4. The device for marking a product according to claim 3, wherein the device further includes means for generating or accepting an encryption key pair and for receiving and storing a certificate with the public key, and for storing the encryption keys and the certificate in a nonvolatile storage means.

5. The device for marking a product according to claim 1, wherein the storage means includes a certificate to identify the device, a permit to indicate compliance with permits standards and one or more permits to define permissible operations and relevant parameters.

6. The device for marking a product according to claim 1, wherein the controller means further includes means for accepting additional information, operating rules and/or parameters which govern its subsequent operation.

7. The device for marking a product according to claim 1, wherein the controller means further includes means for accepting updates to the marking information stored therein.

8. The device for marking a product according to claim 5, wherein the controller means further includes means for accepting updates to the certificate and/or permits.

9. The device for marking a product according to claim 7, wherein the controller means further includes means for checking the validity of each requirement to accept an update according to information and rules already stored therein, and wherein only valid requests will result in an information update.

10. The device for marking a product according to claim 8, wherein an update will be accepted only if it will not change the identification of the marking device.

11. The device for marking a product according to claim 1, wherein the controller will present the marking information only when presented with a predefined permit or digital information.

12. The device for marking a product according to claim 11, wherein the marking information comprises several parts each with its required password or key, and wherein the controller will present each of the parts only when presented with a predefined permit or digital information relating to that part.

13. The device for marking a product according to claim 11, further including interface means connected to control inputs or outputs in the marked product to Furthermore, the marking device of the present invention may also be used to control the object through a secure channel.

14. A method for marking a product comprising the following steps:

A. Manufacturing an electronic marking device including an input/output channel for accepting an inquiry and for answering with marking information stored in the device, means to securely attach the device to the marked product with means for preventing further answering to inquiries if the marking device is removed from the product, digital storage means for storing the marking information and additional information, and controller means for receiving an inquiry through the input/output channel, for reading the information in the storage means and for transferring the information to the input/output channel according to predefined rules;

B. attaching the marking device to a product to be marked;

C. writing an identification digital information package into the storage means, that uniquely identifies each marking device, together with a permit indicating compliance with permit standards;

D. writing product marking information into the storage means; and

E. presenting the marking information to the public whenever required to.

15. The method for marking a product according to claim 14, wherein the unique identification information in step (C) is stored as a digital document which is encrypted or signed by a known authority.

16. The method for marking a product according to claim 15, wherein the digital document includes a public key and wherein the storage means further includes a private key corresponding to the public key in a public encryption scheme.

17. The method for marking a product according to claim 16, wherein step (C) further includes the stage of generating or accepting an encryption key pair and for receiving and storing a certificate with the public key, and for storing the encryption keys and the certificate in a nonvolatile storage means.

18. The method for marking a product according to claim 14, wherein the identification digital information written in step (C) comprises a certificate including information to uniquely identify the device, encrypted or signed with the private key of a known authority.

19. The method for marking a product according to claim 14, wherein the product marking information written in step (D) comprises one or a plurality of permits which include information relating to permissible operations and/or relevant parameters.

20. The method for marking a product according to claim 14, wherein the stage (E) further includes the stage of accepting additional information, operating rules and/or parameters which govern its subsequent operation.

21. The method for marking a product according to claim 14, wherein the stage (E) further includes the stage of accepting updates to the marking information stored therein.

22. The method for marking a product according to claim 18, wherein the stage (E) further includes the stage of accepting updates to the certificate.

23. The method for marking a product according to claim 19, wherein the stage (E) further includes the stage of accepting updates to the permits.

24. The method for marking a product according to claim 22, wherein the stage (E) further includes the stage of checking the validity of each requirement to accept an update according to information and rules already stored therein, and wherein only valid requests will result in an information update.

25. A method for marking a product comprising the following steps:

A. Manufacturing an electronic marking device including an input/output channel for accepting an inquiry and for answering with marking information stored in the device, means to securely attach the device to the marked product, including means for preventing further answering to inquiries if it detects that the marking device was removed from the product, digital storage means for storing the marking information and additional information, and controller means for receiving an inquiry through the input/output channel, for reading the information in the storage means and for transferring the information to the input/output channel according to predefined rules;

B. attaching the marking device to a product to be marked;

C. writing product marking information into the storage means as a digital document, and wherein the document has a multi-level hierarchical structure, with decision rules at each level being linked to decisions at adjacent lower and higher levels.

26. In a device for marking a product, a multi-level permit document comprising a plurality of levels, with each level including a header and a footer , each of the header and footer including Boolean rules for evaluating a Boolean value of the permit.

27. The multi-level permit document according to claim 26, wherein a first header may transfer a request to a second header located in an adjacent lower level, if Boolean rules in the first header permit the transfer, and wherein the second header may transfer a result to the first header.

28. The multi-level permit document according to claim 26, wherein a first footer may transfer a request to a second footer located in an adjacent higher level, if Boolean rules in the first footer permit the transfer, and wherein the second footer may transfer a result to the first footer.

29. The multi-level permit document according to claim 26, wherein a header in the lowest level in the permit may transfer a request to a footer located in the same level, and wherein the footer may transfer a result to the header.

30. The multi-level permit document according to claim 26, wherein a first footer located in the highest level may reach a decision unconditionally and may pass that decision to a second footer located in the second level of the permit.

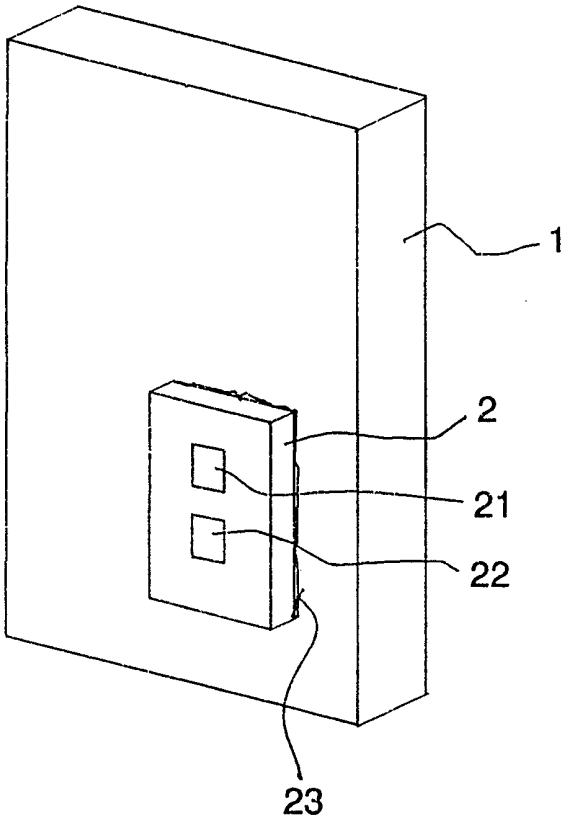


Fig. 1

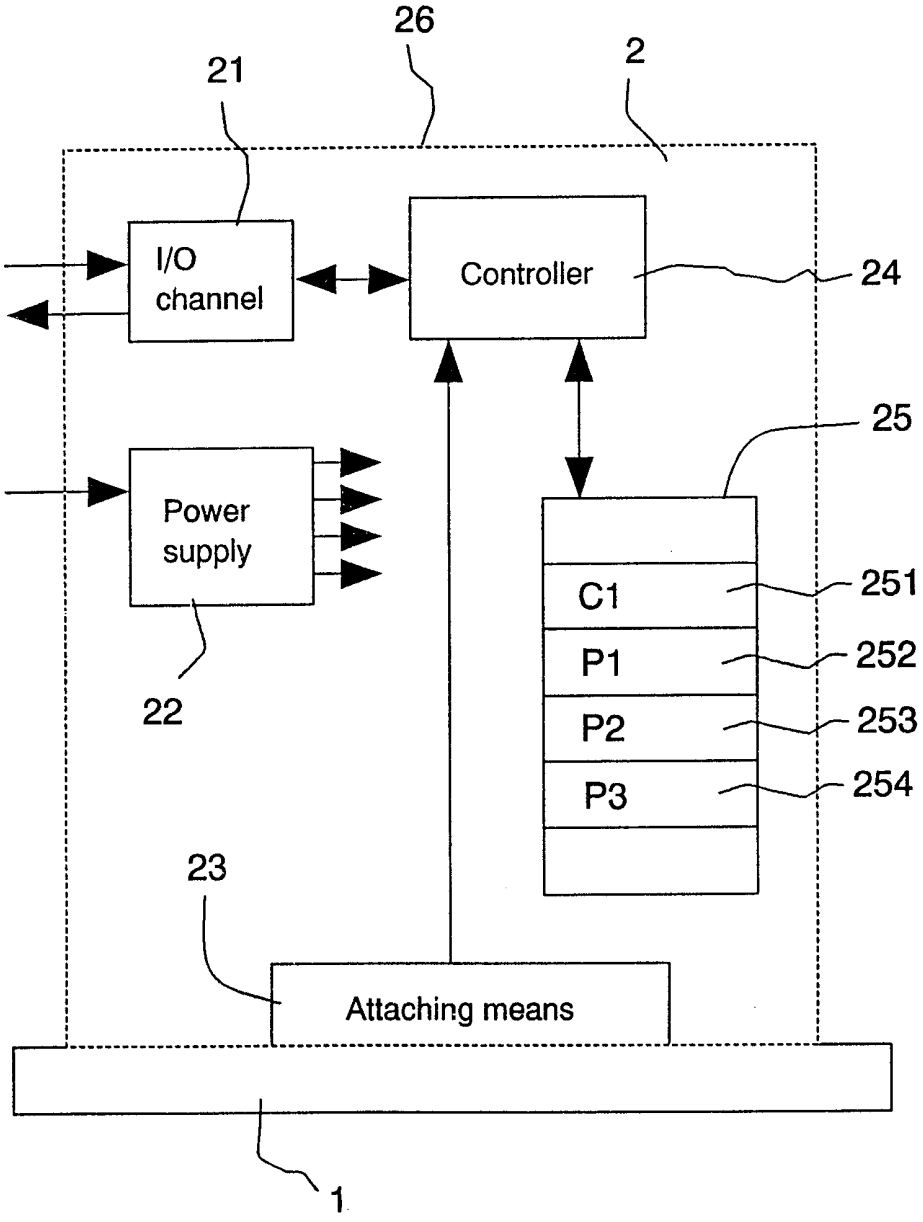

26
21
2
I/O channel
Controller
24
25
Power supply
C1
251
P1
252
P2
253
P3
254
22
23
Attaching means
1

Fig. 2

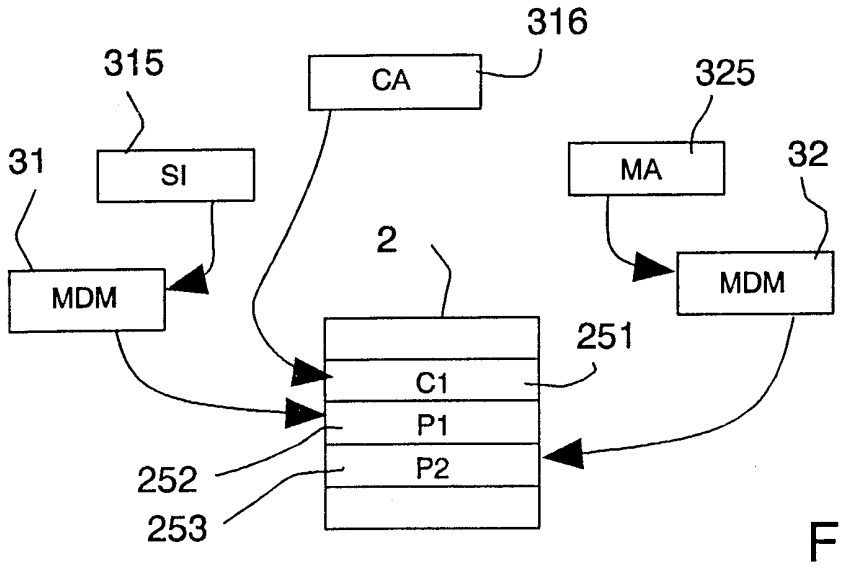


Fig. 3A

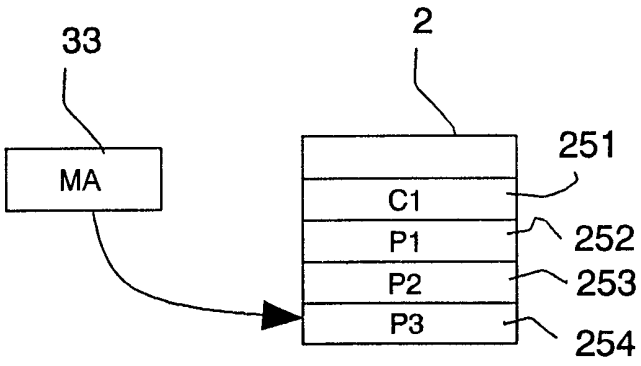


Fig. 3B

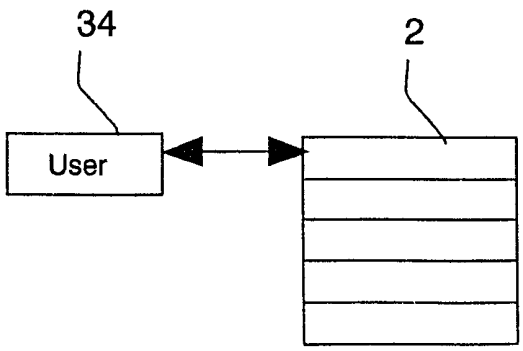


Fig. 3C

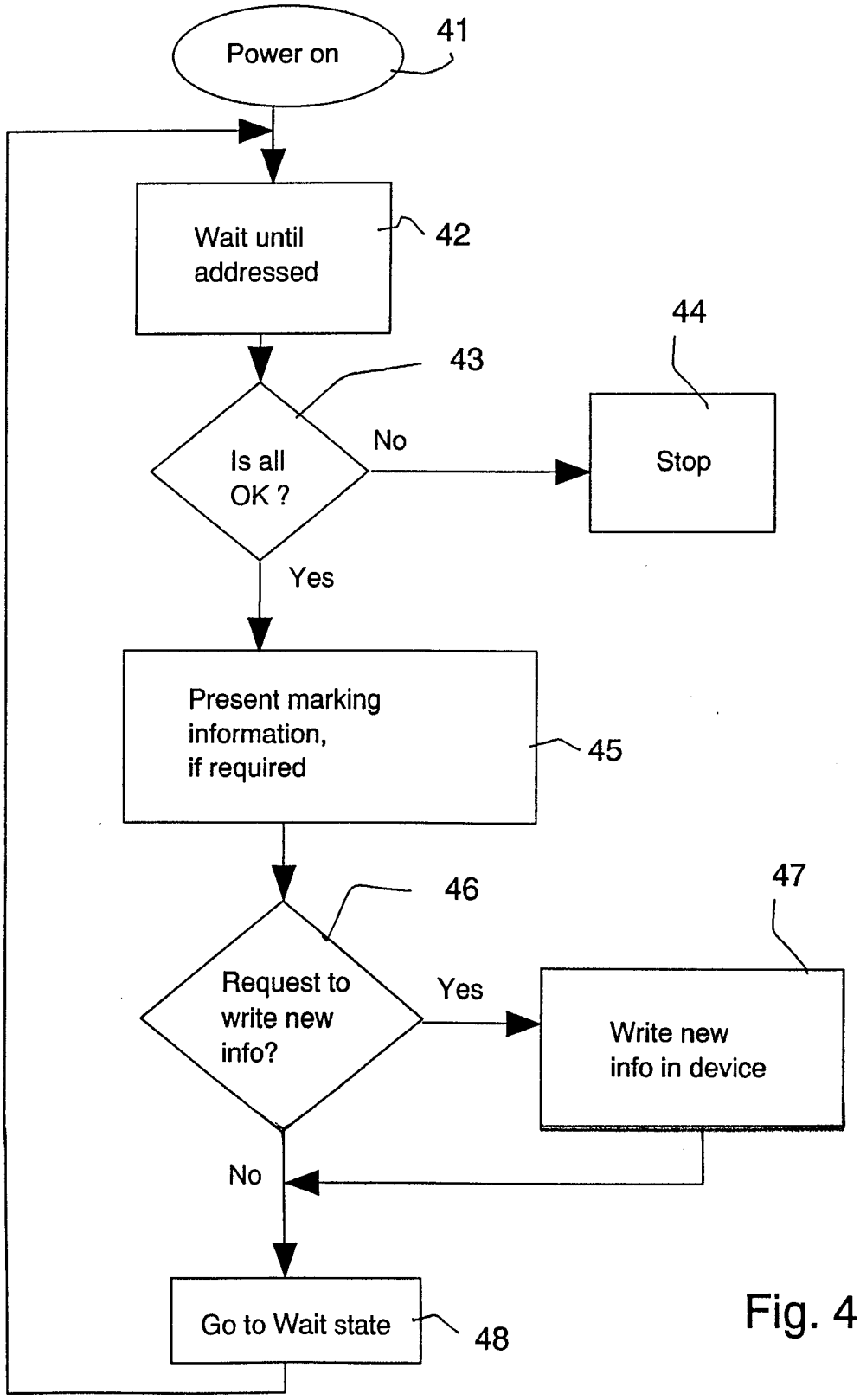

Power on
41
Wait until addressed
42
44
43
Is all OK ?
No
Stop
Yes
Present marking information, if required
45
46
47
Request to write new info?
Yes
Write new info in device
No
Go to Wait state
48

Fig. 4

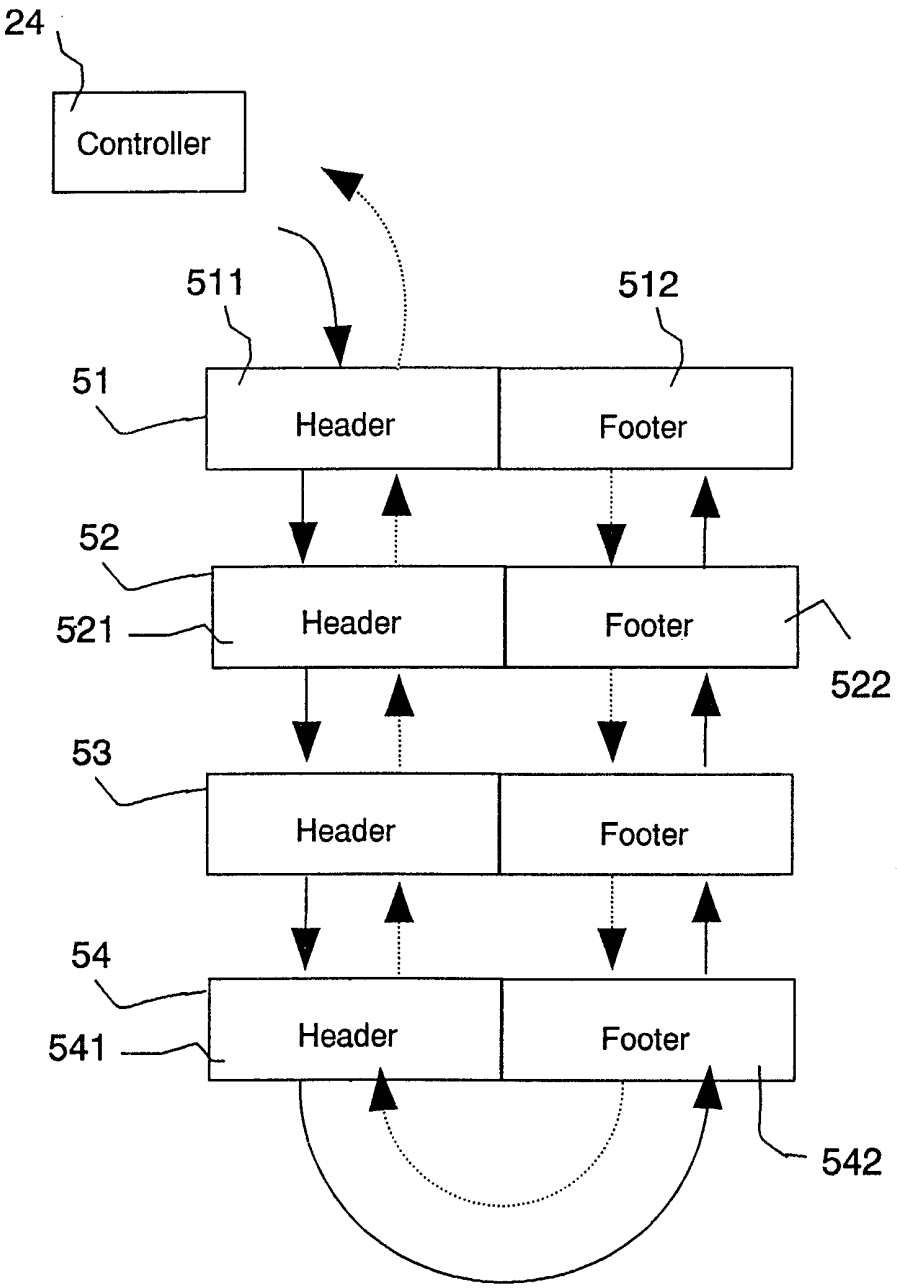

24
Controller
511
512
51
Header
Footer
52
Header
Footer
521
522
53
Header
Footer
54
Header
Footer
541
542

Fig. 5

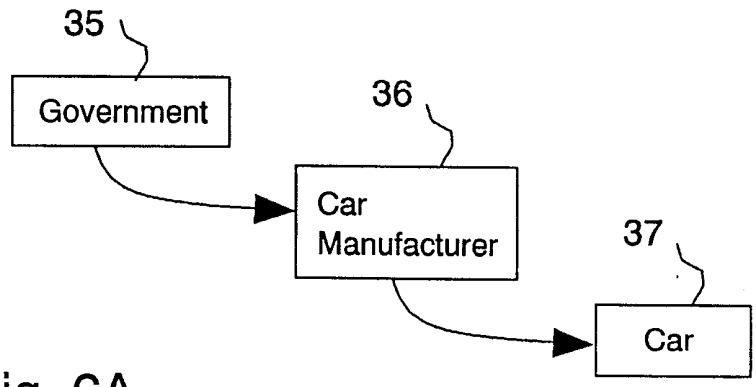

35
Government
36
Car
Manufacturer
37
Car

Fig. 6A

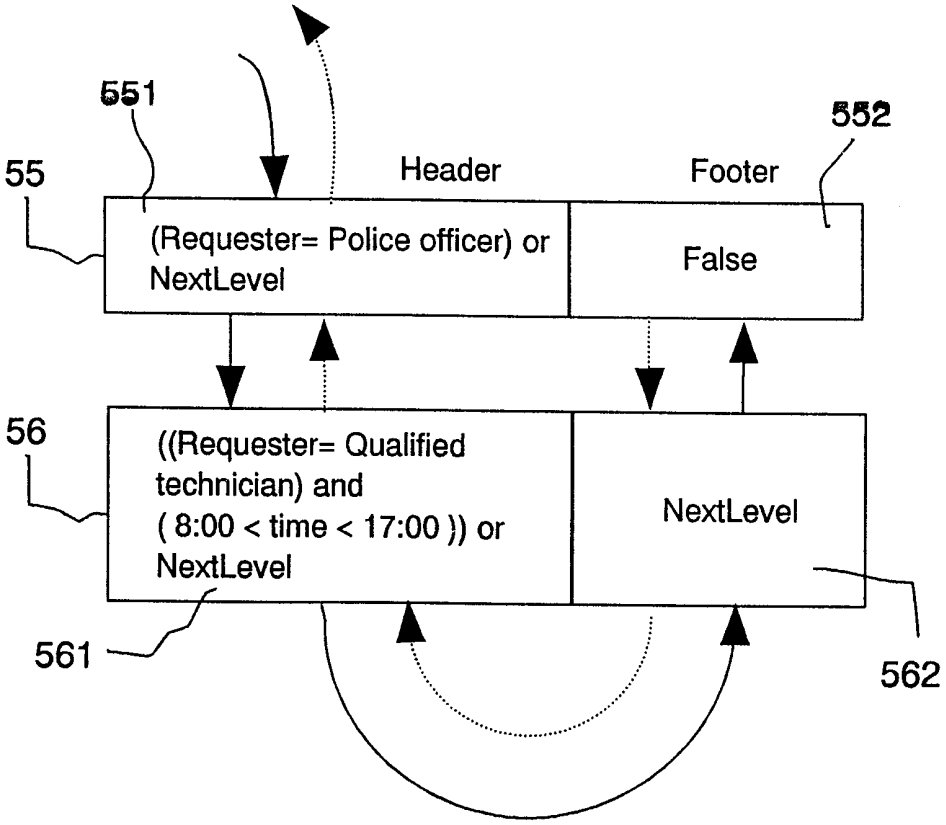

551
552
55
Header
Footer
(Requester= Police officer) or
NextLevel
False
56
((Requester= Qualified
technician) and
(8:00 < time < 17:00)) or
NextLevel
NextLevel
561
562

Fig. 6B