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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 March 2016 (10.03.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/035012 A1

(51) International Patent Classification:
G06Q 30/00 (2012.01) *G06Q 10/08* (2012.01)

(21) International Application Number:
PCT/IB2015/056637

(22) International Filing Date:
1 September 2015 (01.09.2015)

(25) Filing Language: Italian

(26) Publication Language: English

(30) Priority Data:
102014902290027(BL2014A000012)
2 September 2014 (02.09.2014) IT

(71) Applicant: **DIGICANDO S.r.l.** [IT/IT]; Via Privata Dodiciville 12/C, 39100 Bolzano (IT).

(72) Inventors: **DA CORTE, Mirko**; c/o Digicando S.r.l., Via Privata Dodiciville 12/C, I-39100 Bolzano (IT). **POTO, Manlio**; c/o Digicando S.r.l., Via Privata Dodiciville 12/C, I-39100 Bolzano (IT).

(74) Agents: **FAGGIONI, Carlo Maria** et al.; c/o Fumero S.r.l., Via S. Agnese 12, I-20123 Milano (IT).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: ROBUST ANTI-COUNTERFEIT METHOD WITH DYNAMIC CODES AND CORRESPONDING SYSTEM

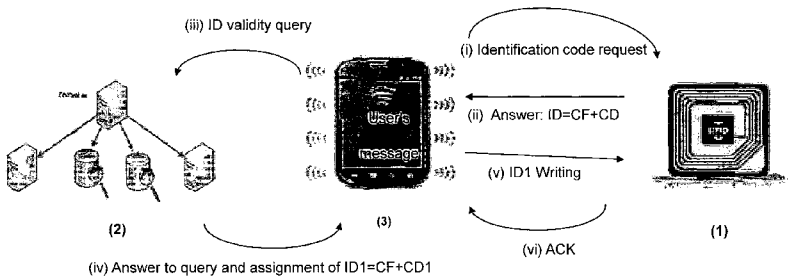

Fig. 1

(57) Abstract: An anti-counterfeit method and system for consumer products is disclosed comprising at least a marker (1) to be associated, in a manner to make tampering evident, with a relative product and provided with at least an identification code (ID), a remote IT management and control infrastructure (2) provided with a database wherein said identification code (ID) is stored in relation to identification data of said product, and at least an interface apparatus between said marker (1) and said remote IT management and control infrastructure (2), wherein said marker (1) comprises at least a rewritable RFID/NFC TAG, said identification code (ID) comprises at least a dynamically variable part (CD) which is changed upon a reading access for verification purposes, and in that said interface apparatus is a personal IT device (3) provided with a reading/writing unit of RFID/NFC TAGs through wireless proximity interface and with a unit communicating with a data transmission network to said remote IT infrastructure (2), on said personal IT device (3) an application software (APP) being installed which provides to transfer data from and to said marker (1) through said wireless proximity interface and from and to said remote IT infrastructure (2) through said communication unit, and it provides to supply first verification information, upon a comparison between said identification code (ID) read from the marker (1) and said database, and a second product information.

WO 2016/035012 A1

ROBUST ANTI-COUNTERFEIT METHOD WITH DYNAMIC CODES AND CORRESPONDING SYSTEM

Technical field

The technical field of the proposed invention is that of the anti-counterfeit methods and systems for movable or circulating goods and it relates all commercial sectors in which there is a demand for control of the genuinity of a product, such as an item of clothing, eyewear products, food, drugs, etc.

Definitions and names nomenclature used

In the present description and in the attached claims the following terms should be understood according to the definitions given here in the following.

Anti-cointerfeit marking: it is a marking mode of objects, in production or in a step in which full control thereof is still had, such as to be able to "certify" and distinguish in a certain way the products from unauthorised copies. This marking allows to establish if the products are genuine, that is, coming from a certain authorised entity.

Marker: object exogenous to the marked product, used for recognising the product through signs or codes associated with the marker.

CF: fixed code, a code which is not changed during the lifetime cycle of the product.

CD: dynamic code, a code which is changed during the lifetime cycle of the product.

TAG: identifies the physical object which acts as label, identifier or support on which the one or more codes reside which define the "marker" and allow to certify authenticity.

RFID: ("radio-frequency identification", in Italian "identificazione a radio frequenza") a technology for identifying and/or automatically storing data through radio-frequency exchange is understood. It is based on the ability to store and remotely read data in special electronic devices (called transponders) with the use of suitable fixed or portable apparatuses called for simplicity's sake readers (however, having also writing capabilities).

NFC: ("Near Field Communication"; in Italian literally "Comunicazione in prossimità") a technology which allows to store and read data in special devices, fully similar to the RFID one, but with protocols and technology which allows only short-radius (up to 10 cm) bidirectional wireless connectivity is understood.

APP: a variant of the IT applications dedicated mainly to mobile-type devices , such as smartphones and tablets.

Remote management and control system: an assembly of hardware and software exogenous to the marker, which allows to remotely interface with the single marker and to manage the data and the data flows to and from the same.

Consumer products: movable products or goods, marketed for a large number of consumers.

TAG types

- *with READ/WRITE or READ ONLY memory:* in the former variety data rewriting is admitted, in the latter the data may be written once only (typically during production)
    * 128-512-bit (or above) memory;
    * 32-128-bit memory, cheaper and generally suited for labels for consumer products
    * very low cost
- with low processing power
    * processing power not sufficient for cryptography or digital signature
    * higher cost (high cost for disposable, consumer-type markings)
- with high processing power
    * high cost (fully unusable for disposable, consumer-type markings)

A robust (secure) anti-counterfeit system may be defined as a marking, control and verification system meeting the following four requirements:

Verifiability: it implies being able to recognise/verify that an item has originated from one's production chain:

Non-generability: it implies that an ill-meaning person

cannot easily generate a mark which passes the authenticity test;

Non-replicability: it implies that, given a mark, it is not possible to create a series of useful copies undistinguishable from the original;

Verifiability of tampering: it means that it must be possible to identify if a mark has been tampered with or if the protection system is altered in some way.

Background

The anti-counterfeit systems currently on the market can be divided into two subgroups:

"low relative cost", that is, those systems the industrial cost of which has a low incidence on the product cost, for example in relation with the cost and/or with the operating margin of the product;

"high relative cost", that is, all the other systems.

Among the main low-cost systems used so far for example barcodes, QR codes, laser codes, holographic labels, philigrane, special inks, etc. can be listed; all these known systems guarantee manufacturing inexpensiveness, however, to the detriment of system robustness/security. In particular each of the known methods does not guarantee the requirement of the "non replicability" of the marker.

Among low-cost systems, up until today also simple passive-type NFC TAGs are found on the market, which TAGs exploit a unique identification code registered within them by manufacturers through suitable security procedures (not fully invulnerable).

Among high-cost systems instead markers using RFID technology with processing power can be found.

Problems of the Prior Art

At the state of the art of the current solutions present on the market, no low-cost solution capable of guaranteeing system robustness is detected.

In particular any method economically advantageous for the manufacturer, which adopts product markers, does not guarantee

marker non-reproducibility.

The main processes/arrangements currently present on the market, capable of actually guaranteeing the security of the anti-counterfeit system are based on microcontroller technology or RFID technology with high-processing-power TAGs, that is, systems capable of processing the possibly received message supplying a reply resulting from message processing. Many of these use "pre" and "post" processing even on remote systems, but the main problem unsolved until now is the need to have a complex and costly marker together with the product and a device capable of actively processing the data. The systems known up until today make the marking and control process industrially burdensome and impracticable for all consumer products.

Solutions using low-cost and medium or low-processing-power NFC TAGs are also being proposed on the market, which are economically more advantageous; in these cases solutions with data cryptography or the use of a special unique identification code (UID) are proposed, the code beingentered in the TAGs by TAG manufacturers.

However, cryptography is not fully devoid of possible attacks, which makes it necessary to implement continuous updates of the systems and relative management of the "releases"; moreover, the Wi-Fi communications have the peculiarity of being vulnerable to attacks called "man in the middle", which simplify the illicit intercepting, activity to be able to decrypt the communications and the codes to create copies; on the other hand, the use of the UID does not offer a certainty on the "non replicability" requirement, since it can be reproduced by a different manufacturer (by the way, using *mirroring* techniques of the NFC microchip codes which have become market standard).

RFID TAGs have also already been proposed on the market containing a double code, at least one of the two rewritable. Examples of markers with two codes, one of which variable, are disclosed in JP2007/328567, US 2002/125997, JP2001/005931.

An application which has been proposed for these markers in

combination with a remote management and control system is that of identifying the TAG (through a first static code) and to authorise or inhibit the reading thereof, through the second variable code which stores a kind of univocal "historical signature" of that TAG of which it is kept track in the remote control system. An example of this application is disclosed in "Dirk Henrici and Paul Mueller, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers", in the Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), PISCATANAY, NJ, USA,IEEE", in which a system is introduced meant to prevent the product marker from being read by unauthorised third parties, which would represent privacy issues.

Summary of the Invention

Object of the Invention

The object of the present invention is to provide an anti-counterfeit system and method for consumer goods which is inexpensive, both in the construction and in the management thereof, and which allows to dramatically reduce other costs connected to the verification of parallel productions.

As a matter of fact, a problem existing in product distribution chains is that of parallel productions. On the market, some wholesalers or retailers can purchase, in addition to a certain number of genuine products, also some fake products, to be offered to the end purchaser illegally but with higher profit margins. In order to avoid these counterfeit phenomena, which cause important economic damages to manufacturers, said manufacturers are forced to define an investigation service, sending trained operators to their own wholesalers/retailers and carry out burdensome investigations on stocked products to verify any stock of fakes of parallel productions.

Up until today there is no methodology which enables manufacturers to remotely monitor the presence of parallel fakes in their own distribution chains.

The method and the system of the invention simultaneously solve the security (robustness) and inexpensiveness demands of the anti-counterfeit system, using the low-cost technologies present on the market, and the surveillance requirements of the remote distribution chain without having to resort to burdensome and invasive investigation techniques.

Concept of the Invention

The system provides the use of:

1. a marker manufactured according to the RFID (TAG) technology, provided with at least one rewritable unique identification code;

2. a remote management and control system which deals with input and output data verification and management, relative to the marker;

3. an interface apparatus between the marker, the remote management and control system and a user.

The system provides the use of a dyamic code, generated by the remote management and control system and associated with the single product through a respective RFID TAG, during the manufacturing step, or possibly distribution or possibly sales process, or possibly in a phase in which one still has control thereof. Such dynamic code is in parallel registered within the remote management and control system and there continuously updated based on the historical events which occur on the single product; in other words, code dynamicity is determined by the product life: the code is changed in connection with controls or updates carried out on the product - that is, on the marker of the RFID TAG thereof - and such change remains registered within the remote management and control system, hence providing at any time a unique identification code for the product and different each time. Thereby the marked product will be identified by a different code at each verification and there does not exist only one single code, clonable, by which one can manage to reproduce in a fraudulent way the marker to apply it on a parallel fake. Due to the action of the same users on the product markers, on the terminal part of the distribution chain

- that is, at the sales point - the products remain associated with unique markers of which it is possible to keep track: that allows, conversely, to immediately identify a possible cloned marker, so as to put it immediately outside the circuit of genuine markers/products (giving suitable information thereof to the user/purchaser) and to identify the retailer which has stocked up on parallel products without having to carry out any investigation activity on site. From an operating point of view, the system can be implemented through a marker with a single variable code, preferably consisting of a fixed part CF and of a dynamic part CD, or with a pair of codes of which a fixed one CF and a dynamically variable one CD.

Advantageously, the CF allows to detect the case in which a CD is replaced with an existing CD attributed to another product, and in case of tampering it allows through various policies to restore the correct CD code. In such case the system hence provides the use of a pair of codes associated with the product: a fixed code and a dynamic code. Considering that at a certain time, to a valid CF code one and only one CD code corresponds, it is possible to detect and correct any tampering. The fact of using the pair CF+CD does not necessarily imply that the CF code must be used to perform each test.

The CF codes can be represented in various ways, provided they cannot be altered by the user. As an example: a barcode, a QR Code, a read-only NFC TAG, the UID code of a TAG, etc.

Furthermore, both codes are associated with the product during the manufacturing process or in a phase in which full control thereon is still had, and they are in parallel registered within a database. While the first fixed code CF does not undergo changes in the product lifetime, the second dynamic code CD is changed in connection with controls or updates carried out on the product, that is, on the product marker. Such change remains registered within the remote database providing hence at any time a unique identification code for the product similarly to the preceding method.

Moreover, operating in the way described, the marked

product is identified by a different code at each verification instance; thereby there does not exist a reproducible univocal code by which one can create a clone of the verified product. Even though a copy of the assembly of the two codes CF+CD was made, at a certain time of the lifetime of the marker associated with the product, this would cease being recognised as valid upon the subsequent verification instance on the marker associated with the original product which, in virtue of such verification, would be immediately changed and tracked in the database of the management system. The generation of the new CD depending on a remote system which generates and associates the new code with that product at each verification request only when it is completed successfully, it is not possible to change in parallel any copies created with the closed code. Thereby, each possible cloned marker copy would be made immediately recognisable as non-genuine copy.

Should the marker instead be verified with the cloned CD associated with a fake, the dynamic code CD on the genuine marker would automatically cease being recognised as valid: the situation would thus arise in which, due to a falsified sample /marker which is recognised as genuine, it will be obtained that the genuine product/marker is recognised as fake: this situation makes cloning economically not convenient, because in the distribution chain only one product considered genuine can circulate, while any other product (whether cloned or genuine at the beginning), is excluded from the circuit of genuine products: the method thus prevents the actual opportunity of serial generation of copies. It is positively impossible to create more than one copy of the single piece of the product-original-marker assembly and the manufacture of a single copy is not an advantageous process.

It is thereby proved that the method according to the invention provides the best solution reachable through markers exogenous to the object.

Brief Description of the Drawings

Further features and advantages of the system and method

according to the invention will in any case be more evident from the following detailed description of preferred embodiments of the same, given as an example and illustrated in the attached drawings, wherein:

Fig. 1 is a schematic view which represents the interactions in a system according to a first embodiment of the invention;

Fig. 2 is a schematic view which represents the interactions in a system according to a second embodiment of the invention; and

Fig. 3 is a schematic view which represents the interactions in a system according to a third embodiment of the invention.

Description of Preferred Embodiments

Purely as a non-exhaustive example, here in the following a possible implementation of the system and method of the invention will be given.

As represented in fig. 1, the system is based on marker 1, to be applied to a product, an IT infrastructure 2, which acts as remote management and control system, and of a personal IT device 3 capable of communicating with the marker in reading/writing mode and with the IT infrastructure for data exchange.

In particular, marker 1 is in the shape of an RFID TAG, precisely a TAG with NFC technology which requires a greater proximity between reading/writing device and TAG. Marker 1 must preferably be applied onto the product of interest in a way which makes evident any tampering or removal (tamper evident), so as to make substantially univocal the association between marker 1 and the relative product to be protected from counterfeiting. IT infrastructure 2, as represented in fig. 1, essentially consists of a server communicating with a remotely accessible network, for example the Internet network, on which a proprietary database resides, the management of which is entrusted to a certifying body, typically (but not necessarily) a third party with respect to consumer good manufacturers, to

the subjects involved in the distribution chain and to the purchasers. Personal IT device 3 has a unit communicating with IT infrastructure 2 and a reading/writing unit of marker 1; it typically consists of a smartphone or tablet or other IT support provided with said communication and reading/writing units and of an operating system on which software applications can be installed.

On personal IT device 3 an application APP is installed which is capable of exchanging data with IT infrastructure 2 and of reading/writing data from and to said NFC TAG 1 through said reading/writing unit.

On NFC TAG 1 there is registered, in ways known per se in the RFID sector, at least one variable code, possibly with a fixed part CF and a dynamically variable part CD, or a first fixed code CF and a second dynamically variable code CD.

The system can also be accomplished using a code consisting of a fixed part CF, which corresponds to the same code associated with the type of product and to the manufacturer, and of a dynamically variable part CD which is a simple random code generated by the remote system (with the constraint of never being able to assign a code already previously assigned). The two marker codes can both be stored in the same TAG or they can be of an heterogeneous nature: for example, fixed code CF can be a barcode applied to the product label or a code registered in the memory of a READ-ONLY TAG, while variable code CD is registered within a rewritable TAG in a certain step of the manufacturing (or distribution or sales) process.

The data relating to the product (for example product name, owner, CF, CD,...) are registered within the database implemented in the server of IT infrastructure 2, suitably protected from access and wherein the correlation between variable code CD and the other data of the specific product is maintained, or between fixed code CF and the data, or between fixed code CF and variable code CD, or all the correlations indicated.

Since dynamically variable code CD is changed at each verification instance of the assembly of the two codes CD+CF

concluded with a positive outcome, in parallel the database data are changed accordingly. Preferably in the database it is not simply preformed a change of the single record relating to that product into the new variable code CD, but the entire sequence of variable codes CD used with that corresponding fixed code CF and the further additional marker data is stored in a respective number of records, the time sequence of the various records allows to keep track of the marker lifetime and of the product associated therewith, so as to be able to detect also - in case cloning attempts were detected, upon an unsuccessful verification of a variable code CD - the distribution chain and the retailer involved in the circulation of the counterfeited product.

The genuine verification instance is performed, for example, using a smartphone in which an application software APP is installed which interacts with the fixed and variable codes contained in the RFID TAG 1 and it communicates with the database of IT infrastructure 2 through secure data transmission protocols.

According to a first embodiment of the invention (fig. 1), the application software on device 3 provides to perform a data exchange procedure which provides storage of the new identification code upon the positive outcome of the verification instance. That is, the application initially provides (i) to query the marker (with techniques known per se) to (ii) obtain the identification code ID present on the marker (the single code stored in the RFID TAG, or the two codes stored in the RFID TAG, or the heterogeneous codes partly in the TAG and partly visible externally in form of QR Code or barcode, for example) and (iii) it communicates said code to the database of certifying infrastructure 2, checking the validity thereof. If the check on the database gives a positive outcome, that is, the current composition of the identification code matches to what is stored in the database, the IT infrastructure 2 provides to generate a new identification code ID1 - or better, the dynamically variable part thereof CD1 - which is also

associated in the database with the data of the respective product and transmits it (iv) to the application of device 3 so that (v) it is retransmitted to the marker and stored there as a substitute to the previous one. If the procedure ends regularly, with the storage of the new identification code ID1 in the RFID TAG 1, a positive outcome acknowledgement ACK is determined (vi) - for example through a number of sequential marker readings, until it is detected that old code CD has been actually replaced with the new one CD1 - which closes the data exchange procedure.

According to an alternative embodiment (fig. 2), the data exchange procedure provides a storage of the new identification code as preliminary operation. That is, the application on device 3 initially provides (i) to request to IT infrastructure 2 to generate and associate a new identification code ID1 - or better, the dynamically variable part thereof CD1 - to that product and then (ii) to send it to device 3 which then proceeds (iii) to transmit it to the marker to store it, as a substitute to the previous identification code ID which (iv) is transmitted back to device 3. After the confirmation that the storage of new code ID1 has been completed successfully, the application of device 3 provides (v) to communicate the identification code ID, which was found resident on marker 1, to the database of certifying infrastructure 2 to check the validity thereof. If the check on the database returns a positive outcome, that is, the current composition of the identification code matches to what has been stored in the database, infrastructure 2 completes the association of the new code ID1 with the product and returns (vi) to device 3 a successful completion acknowledgement which closes the data exchange procedure.

This second embodiment has the advantage of limiting the time window which remains open for data exchange with the RFID TAG, since the reading and the storage of the new data occur in rapid sequence: that is advantageous to avoid irregular information exchanges in the fractions of second in which the user approaches his/her mobile device to the product marker. Vice versa, the first embodiment has a longer time window -

because between the reading and the storage/writing of the TAG the querying of IT system 2 occurs as well as the generation of the new code - but it has the advantage of generating a new code (with what it implies in terms of resources employed) only in the cases in which the validity check has had a positive outcome.

According to a third alternative embodiment represented in fig. 3, the process occurs in a fully similar way to the first embodiment described, up to the point (vi) in which an positive outcome acknowledgement (ACK) is determined from the marker 1. At this point, however, unlike the first embodiment, portable IT device 3 in turn sends (vii) an acknowledgement message (of positive or negative outcome of the writing operation in the marker 1) to infrastructure 2, which replies (viii) with the conclusive outcome of the operation with a positive or negative outcome acknowledgement which closes the data exchange.

This third method allows to eliminate a vulnerability present in the case in which the procedure should be accidentally interrupted (for example due to a fault of the writing unit or of the marker) between the steps (iv) and (v) of the first embodiment, in which case an inconsistent situation would be obtained between the information maintained within marker 1 and the information contained within infrastructure 2.

In any case, the outcome of the verification instance is shown to the user on portable IT device 3, together with other information on the product (for example type, quality, way of use, suggested price and other) which are sufficiently interesting for the user, so much so as to induce him/her to approach their device to the marker and to carry out the verification process, regardless of the conclusion of a purchase action. As a matter of fact, it is advantageous for system robustness that one of more verificaton operations on the product marker are carried out, so that the univocal identification code be changed and tracked on the database of IT infrastructure 2 and marker cloning opportunities are substantially eliminated.

Operatively, the anti-counterfeit method according to the invention works as follows.

During manufacturing, the genuine products are associated, in ways which make evident any tampering, with respective markers provided with a univocal code ID of the type described above. Simultaneously, in the database of IT infrastructure 2 the data of each genuine product (such as type, colour, size and other) are stored in connection with the marker identification code ID.

The users are provided with an application software APP, to be installed in a personal IT device, which is capable of reading/writing from and to the marker, as well as of communicating remotely with the IT management and control infrastructure 2.

The marker identification code, or better, the dynamically variable part thereof, is hence changed over time at each verification operation, carried out along the chain of distribution and/or by the final users/purchasers through the application software APP, so as to make the code virtually unreproducible. As a matter of fact, at each verification operation, unique code ID is replaced by a new unique, code ID1 generated randomly or with other virtually unpredictable criteria (for example connected to the credentials of the personal IT device which connects to IT infrastructure 2). Changed unique code ID1 is stored in the database and is considered the new genuine code.

At each verification operation, the unique code read in the marker is compared against the latest one stored as genuine in the database and, if the comparison provides a positive match, a positive-outcome acknowledgement of the validity instance is supplied to the user. In the same validity operation other useful information on the product is also supplied to the user.

If the comparison provides a negative outcome, that is, there is no match between the unique code just read from the marker and the one stored as genuine in the database, the user is supplied with a corresponding information and an alert signal

is generated in the IT management and control infrastructure 2. Following this event, it is possible to trace the retailer who has the product considered fake, through information which the user has deliberately chosen to supply through the application software APP (for example relying on compensation approach) or through tracing of the product codes carried out by the manufacturer.

As can be understood from the description reported above, with the system and method according to the invention the objects set forth in the premises are perfectly achieved.

As a matter of fact, the anti-counterfeit method is configurable at a very low cost, using rewritable RFID TAGs (but without processing power) of a modest cost, a standard IT infrastructure and a verification device already available to users. Furthermore, exploiting the user verification operations, the unique identification code of the markers is made virtually unreproducible precisely in correspondence of the terminal part of the distribution line, which makes it possible to detect the retailers involved in the purchase of parallel products without the need of unpleasant investigative operations.

With the system according to the invention the likelihood of randomly detecting the correct code, for each time of the product lifetime, is reduced to a value next to zero; as a result the opportunity of generating a series of copies of the variable code CD which are verifiable with a positive match is impossible, each variable code CD remaining valid exclusively until the subsequent verification instance carried out with positive outcome and resulting hence impossible to clone the new code on any copies created.

Furthermore, it is possible to correlate in a univocal manner an object with the relative owner. When the ownership of an object is univocally identified, it is also possible to associate therewith personal information which may be useful to other people or which may be used in the most disparate uses. It is possible for example to add text to a verifications message resulting from the control, for example: "if you find this

object, please call number xxx-xxxxx. Reward".

The concept of owner is functional: for example should a person find the object, unless the marker is removed and hence tampering the genuinity sign, he/she would own an original object, but not of his/her property.

With markers a social use of the TAGs may also be encouraged, which goes well beyond the simple genuinity verification, but which may expose to potentially complex social dynamics, both online and offline.

A possible application of the system is also that of supplying an alternative to purchase proofs.

Moreover, it often happens that for some products, for example foodstuff or drugs, the expiry date is recycled, for example applying a label on top of the original one. Advantageously, with the proposed system, if a company decides that their own product has an expiry date, it is possible to warn the purchaser - upon registration at the IT infrastructure - when that specific product is due to expire.

Furthermore, with this system, being able to successfully certify the actual ownership of an object attributing it to a person or company, it is advantageously possible to provide a warranty service for online purchases between private entities or stores and private entities, certifying that such person or company really owns the products it states it is selling, and that such product is genuine and not counterfeited. Advantageously, that may help to fight the phenomenon of scams relating to the online sale of goods.

Finally, is should be noted that the system of the invention invariably meets the robustness requirements:

1. *Verifiability: at any time*, querying the database of the remote management and control infrastructure 2, using the pair CF+CD it is possible to verify the entire production flow as well as the distribution flow of the product;

2. *Non generability*: the impossibility to generate a correct code by an ill-meaning person is substantially linked to the opportunity of assimilating the codification to a pseudo-

random generation and the management of the codes through remote database. That is, it is not possible to generate a valid code without entering the value thereof in the remote management and control infrastructure 2; in parallel, randomly generating a code which is recognisable as valid has a likelihood of success next to zero (depending on code length);

3. Non replicability: while fixed code CF defines univocally the product, the variable code CD associated with fixed code CF is - for the purposes of generation - a random code: the opportunity of randomly detecting a similar code is so low to be able to define the event as being virtually impossible. Should an existing code be copied onto a different marker, the validity of such code would cease at the subsequent verification instance or status change of the product: the produced copy would hence no longer be a valid and verifiable copy of the code, making *de facto* the product-associated code non reproducible.

4. Verifiability of tampering: the assembly of fixed code CF and variable code CD being a code similar to a random code, any possible tampering of the variable code CD would generate a code not present in the database of valid codes and the absence thereof in the database hence makes evident the tampering of the marker.

However, it is understood that the invention is not limited to the special embodiments illustrated above, which represent only non-limiting examples of the scope of the invention, but that a number of variants are possible, all within the reach of a person skilled in the field, without departing from the scope of the same invention.

CLAIMS

1. Anti-counterfeit system for consumer products comprising at least a marker (1) to be associated, in a manner to make tampering evident, with a relative product and provided with at least one identification code (ID),

a remote IT management and control infrastructure (2) provided with a database wherein said identification code (ID) is stored in relation with identification data of said product, and

at least an interface apparatus between said marker (1) and said remote IT management and control infrastructure (2), characterised in that

said marker (1) comprises at least a rewritable RFID/NFC TAG,

said identification code (ID) comprises at least a dynamically variable part (CD) which is changed upon a reading access for verification purposes, and in that

said interface apparatus is a personal IT device (3) provided with a reading/writing unit of RFID/NFC TAGs through wireless proximity interface and with a unit for communication with a data transmission network to said remote IT infrastructure (2),

on said personal IT device (3) an application software (APP) being installed which provides to transfer data from and to said marker (1) through said wireless proximity interface and from and to said remote IT infrastructure (2) through said communication unit, and it provides to supply first verification information, upon a comparison between said identification codes (ID) read from the marker (1) and from said database, and second product information.

2. Anti-counterfeit system as in 1, characterised in that said dynamically variable part (CD) of the identification code (ID) is changed upon a reading access for verification purposes only upon a positive outcome of said verification.

3. Anti-counterfeit system as in 1, characterised in that said dynamically variable part (CD) of the identification code

(ID) is changed into a new identification code (ID1) upon a reading access for verification purposes of said identification code (ID).

4. Anti-counterfeit system as in 1, 2 o 3, wherein said identification code consists of a fixed part (CF) and of a dynamically variable part (CD).

5. Anti-counterfeit system as in 1, 2 or, in anyone of the preceding claims, characterised in that a part of the dynamically variable code (CD) remains unchanged during product lifetime.

6. Anti-counterfeit system as in any one of the preceding claims, wherein in said remote IT infrastructure (2) a track of a univocal correlation of the data of a product with an owner's data is stored.

7. Anti-counterfeit system as in any one of the preceding claims, wherein in said remote IT infrastructure (2) product information in relation to said identification code (ID) are univocally stored.

8. Anti-counterfeit method for consumer products comprising at least a system as in any one of the preceding claims wherein

a marker (1) comprising at least a rewritable-type RFID/NFC TAG is provided with at least one unique identification code (ID) and is associated, in a manner to make tampering evident, with a relative product,

in a remote IT management and control infrastructure (2) provided with a database, said unique identification code (ID) is stored in relation with identification data of said product,

characterised in that

at least a dynamically variable part (CD) of said unique identification code (ID) is changed upon a reading access for verification purposes to said marker (1) through a personal IT device (3) provided with a reading/writing unit of RFID/NFC TAGs through wireless proximity interface,

said personal IT device (3) exchanging first verification information and second product information with said remote IT infrastructure (2) through a unit communicating with a data

transmission network,

said personal IT device (3) furthermore receiving data generated by said remote IT infrastructure (2) for said change of said dynamically variable part (CD), and wherein

said personal IT device (3) provides on a display said first verification information and said second product information, the verification information being tracked also in said database of the remote IT infrastructure (2).

9. Method as in 8, wherein said unique identification code (ID) is first read from the marker (1) and communicated to said remote IT infrastructure (2) for a validity check, through comparison against data stored in said database, and subsequently, upon a positive outcome of said validity check, said dynamically variable part (CD) of said unique identification code (ID) is changed through respective change data generated by said remote IT infrastructure (2) and transmitted to said personal IT device (3).

10. Method as in 8, wherein change data of said dynamically variable part (CD) are preliminarily generated by said remote IT infrastructure (2) and transmitted to said personal IT device (3), said dynamically variable part (CD) of said unique identification code (ID) being changed upon reading the marker (1) for verification purposes before the subsequent communication of the unique identification code (ID) to said remote IT infrastructure (2) for a validity check through comparison against data stored in said database.

11. Method as in 9 or 10, once completed the change of said dynamically variable part (CD) of said unique identification code (ID), a positive outcome signal (ACK) is generated which is transmitted back from said personal IT device (3) to said remote IT infrastructure (2) for a conclusion of the verification instance.

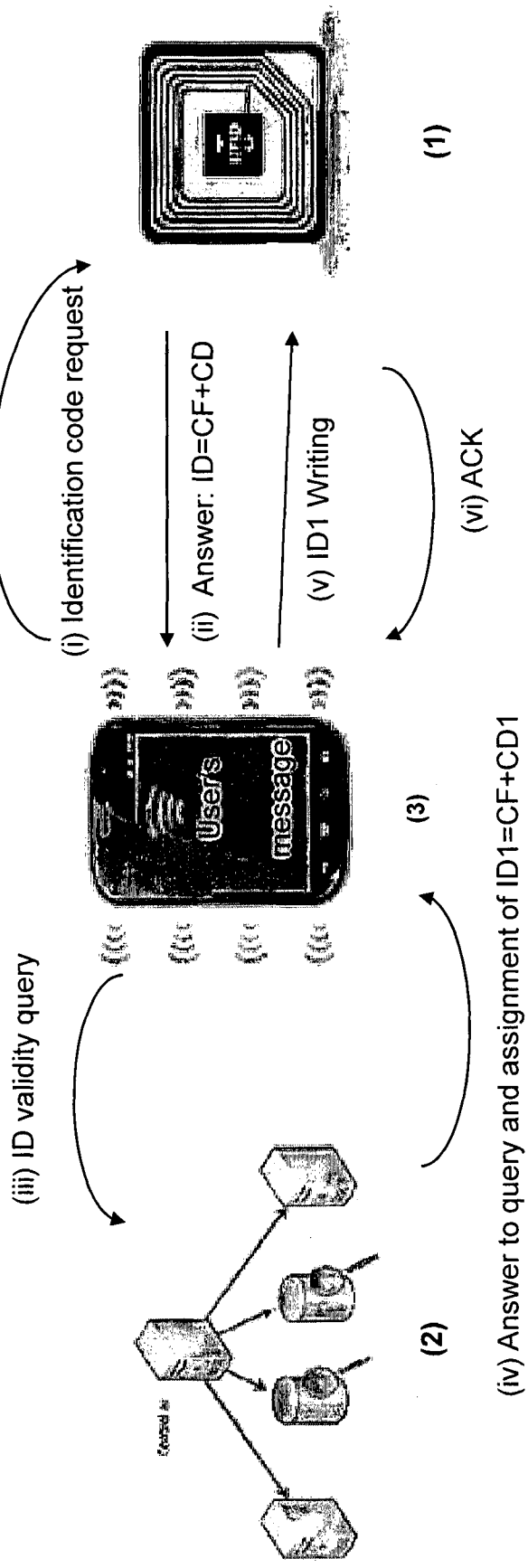
(1)
(i) Identification code request
(ii) Answer: ID=CF+CD
(v) ID1 Writing
(vi) ACK
User's message
(3)
(iii) ID validity query
(2)
(iv) Answer to query and assignment of ID1=CF+CD1

Fig. 1

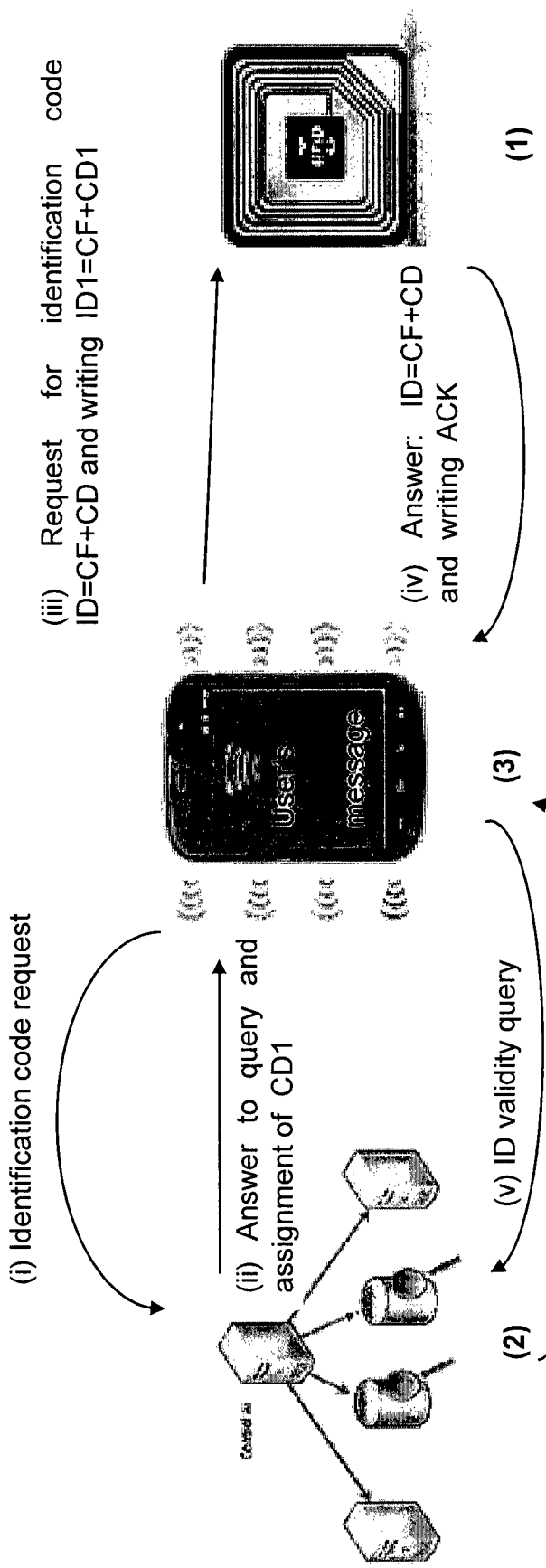
(i) Identification code request
(ii) Answer to query and assignment of CD1
(iii) Request for identification code ID=CF+CD and writing ID1=CF+CD1
(iv) Answer: ID=CF+CD and writing ACK
(v) ID validity query
(vi) Answer to query
(1)
(2)
(3)
User's
message

Fig. 2

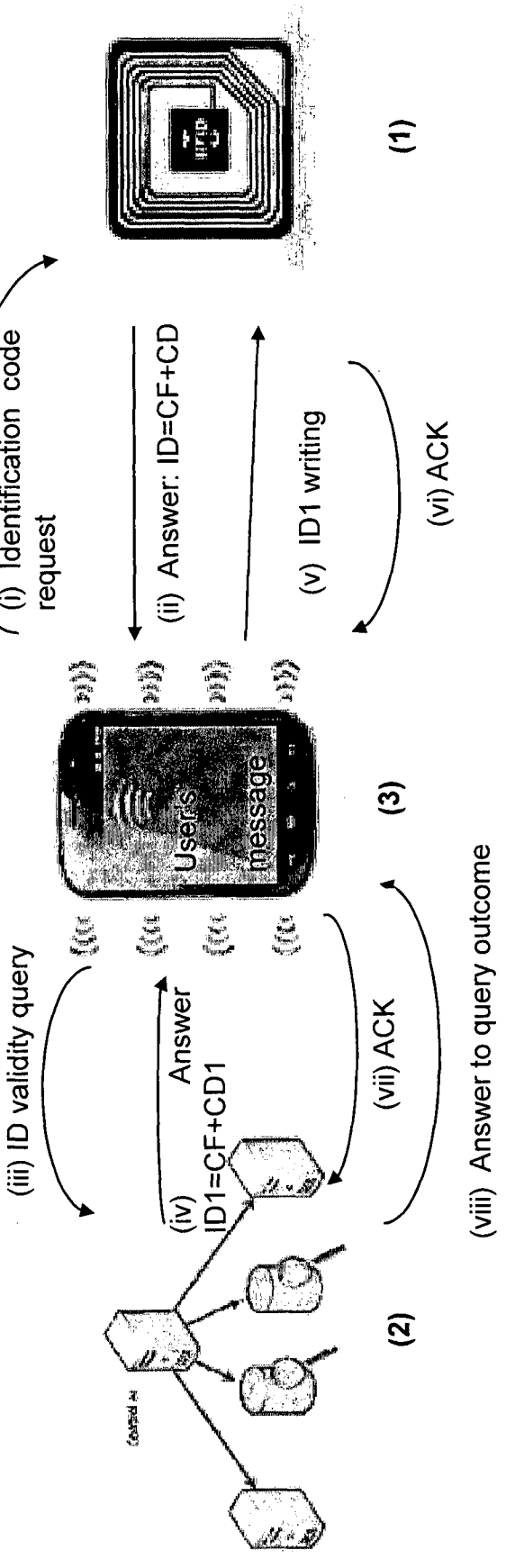
(1)
(i) Identification code request
(ii) Answer: ID=CF+CD
(v) ID1 writing
(vi) ACK
User's message
(3)
(iii) ID validity query
(iv) Answer ID1=CF+CD1
(vii) ACK
(viii) Answer to query outcome
(2)

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2015/056637

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/00
ADD. G06Q10/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2007 328567 A (SEIKO EPSON CORP) 20 December 2007 (2007-12-20) cited in the application page 4, paragraph 12 - page 17, paragraph 125 figures ----- -/--	1-11

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 December 2015	22/12/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Rachkov, Vassil

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HENRICI D ET AL: "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, 2004. PROCEEDINGS OF THE SECOND IEEE ANNUAL CONFERENCE ON, PISCATAWAY, NJ, USA,IEEE, 14 March 2004 (2004-03-14), pages 149-153, XP010689745, DOI: 10.1109/PERCOMW.2004.1276922 ISBN: 978-0-7695-2106-0 cited in the application the whole document	1-11
X	JP 2001 005931 A (TOHKEN CO LTD) 12 January 2001 (2001-01-12) cited in the application page 3, paragraph 8 - page 5, paragraph 25 figures	1-11
A	US 2002/125997 A1 (KASHI MOTOFUMI [JP] ET AL) 12 September 2002 (2002-09-12) cited in the application page 1, paragraph 8 - paragraph 10 page 2, paragraph 17 - page 3, paragraph 26 figures	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2015/056637

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2007328567 A	20-12-2007	NONE	
JP 2001005931 A	12-01-2001	NONE	
US 2002125997 A1	12-09-2002	JP 2000357847 A	26-12-2000
		US 2002125997 A1	12-09-2002