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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2014 (23.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/014401 A2

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

(21) International Application Number:
PCT/SE2013/050902

(22) International Filing Date:
15 July 2013 (15.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1200443-8 16 July 2012 (16.07.2012) SE

(71) Applicant: **QURE AB** [SE/SE]; Resedavägen 57, S-232 53 Åkarp (SE).

(72) Inventor: **SJÖDIN, Tor**; Resedavägen 57, S-232 57 Åkarp (SE).

(74) Agents: **ÅKESSON, Jan-Åke** et al.; Box 1066, S-251 10 Helsingborg (SE).

(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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: AUTHENTICATION OF A PRODUCT

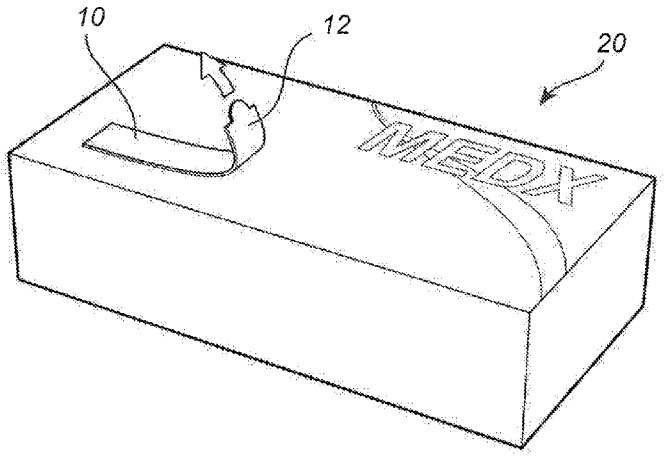

Fig. 2

(57) Abstract: This application relates to a set of authentication labels for being arranged on a physical product (20), the set of authentication labels comprising: a first label (10) provided with a first set of symbols (11); and a second label (12) provided with a second set of symbols (13); wherein at least the second label (12) is adapted to be, when provided on the physical product (20), unreadable and irreversibly exposable for reading; wherein the first set of symbols (11), the second set of symbols (13) or the combination of the first set of symbols (11) and the second set of symbols (13) is unique; and wherein the first set of symbols (11) and the second set of symbols (13) are chosen such that, when input to a predetermined algorithm, an authentic output is obtained. The application also relates to a corresponding single authentication label.

WO 2014/014401 A2

AUTHENTICATION OF A PRODUCT

TECHNICAL FIELD

The present application relates to the field of authentication, and in particular to a authentication label for authentication of a physical product.

BACKGROUND OF THE INVENTION

Many kinds of physical products are manufactured and spread in distribution channels all over the world. This spread renders the traceability of the manufacturing and distribution channel difficult, thus facilitating the possibility for ill-intentioned players to produce and sell forgeries of such physical products. These players are often very innovative when it comes to finding new ways to falsify products.

It can be very difficult for the end customer to separate a forgery from the authentic original product. Thus, many end customers, or other players in a distribution chain, buys forgeries without knowing it. In order to provide the buyer with a possibility to authenticate a product, i.e. verify that the product is authentic and not a pirated copy, there exist authentication methods based on verification codes which are read and sent to a server for verification. The verification codes may be for example be printed on a product package or included in an RFID tag. However, such labels and tags are easy to copy by reading the code comprised therein, for example by photographing a printed label or by reading an RFID tags by a conventional RFID reader. One copied code may be used for producing a great number of forgeries provided with the single copied code.

Thus, there is a need for an improved method and system for authentication of a physical product.

SUMMARY OF THE INVENTION

An object of the present invention is to alleviate the above mentioned drawbacks and problems. A further object is to provide an authentication label for a more secure authentication which also is more difficult to copy.

According to a first aspect of the invention, this and other objects are achieved by a set of authentication labels for being arranged on a physical product, the set of authentication labels comprising:

a first label provided with a first set of symbols; and

a second label provided with a second set of symbols;

wherein at least the second label is adapted to be, when provided on the physical product, unreadable and irreversibly exposable for reading;

wherein the first set of symbols, the second set of symbols or the combination of the first set of symbols and the second set of symbols is unique; and

wherein the first set of symbols and the second set of symbols are chosen such that, when input to a predetermined algorithm, an authentic output is obtained.

A number of advantages are achieved by this aspect of the invention. Firstly, the irreversibly exposure of the second label makes copying of the set of symbols required for reproducing the set of authentication labels difficult. The second label must be exposed if the set of authentication labels is to be copied. It is also detectable that a set of authentication labels has been opened and possible copied. In order to produce an credible copy, the copier must produce new copies of the labels which are non-exposed, thus rendering the copying more cumbersome and costly and thereby less attractive.

Secondly, the use of unique set of symbols, or a unique combination of set of symbols, provides the possibility to uniquely link a the set of symbols to a single product. A database may be provided in which information pertaining to the product corresponding to the unique set of authentication labels. In connection to an authentication of the product, such information may be provided from the database to a person performing the authentication.

By unique is the context of this application meant that the first set of symbols, the second set of symbols or the combination thereof is chosen such that no other set of authentication labels is provided with the same set of

symbols or combination of set of symbols. One way to achieve unique set of symbols is by generating them by a random symbol generator.

By that the set of authentication labels has unique set of symbols, or a unique combination thereof, provides for one-time-authentication of each set of authentication labels. By one-time-authentications is meant that each set of authentication labels is permitted to be authenticated only once. Any further authentication may be blocked. Thus, a specific set of authentication labels cannot be copied and applied on multiple copied and fake products. The copier must copy and reproduce one set of authentication labels for each copied product, thus making the copying time-consuming and costly.

Thirdly, the use of multiple labels renders the copying further difficult. If the copier does not copy the labels directly, he can try to guess correct set of symbols which will work for the authentication. However, by use of a combination of set of symbols instead of a single label the guessing is much more difficult. Further, the copier must also have knowledge about which set of symbols is to be combined in order to achieve a working set of authentication labels. The information of which set of symbols that is intended to be combined may be kept separate from the actual set of symbols, i.e. the set of labels. Thus , if a copier gets hold of the set of symbols, e.g. for a whole batch of products, he would still need the information about how to combine the labels.

A user may authenticate the product by the set of authentication provided thereon, combined with the knowledge of the predetermined algorithm and the authentic output. The algorithm and the authentic output may be stored in a database on a authentication server, together with a connection to a specific set of symbols or a specific combination of set of symbols. By an authentication device, such as a smart phone, the product may be authenticated. The authentication device may have access to the authentication server by means of e.g. wireless communication, and thus have access to the algorithm and the authentic output for the set of symbols which is to be verified. Alternatively, the authentication device may have the algorithm and the authentic output stored on a local memory, thus enabling

off-line authentication. The authentication device may connect to the authentication server when possible or at predetermined frequency for updating the local information, in particular information pertaining to which set of authentication labels that has been blocked for further authentications.

The first set of symbols and/or the second set of symbols may be presented in the form of one or a combination of the following: a barcode, a QR code, an NFC code, an RFID tag, or a transcription.

The second set of symbols may be presented as a print on the second label, the second label being arranged on a backside of the first label. The first label may be attached by its backside to the product such that second label is unreadable. Further, the first label may be irreversible removable in order to expose the second label to reading. Thus, the first label and the second label forms one label unit. This feature may facilitate the attaching of the set of authentication labels on the product. This feature also makes it easier for the person who performs the authentication to locate the position of the second label.

At least one of the first set of symbol and the second set of symbols may be a serial number.

The second label may be irreversibly exposable by scratching or pulling off a cover layer from the second label. Other techniques for making the second label irreversibly exposable are known to the skilled person.

According to a second aspect of the invention, the above mentioned and other objects are achieved by an authentication label for being arranged on a physical product, wherein:

the authentication label is provided with a unique set of symbols;

the authentication label is adapted to be, when arranged on the physical product, unreadable and irreversibly exposable for reading; and

wherein the unique set of symbols is chosen such that, when input to a predetermined algorithm, an authentic output is obtained.

A number of advantages are obtained by this aspect of the invention.

Firstly, the irreversibly exposure of the authentication label makes copying of the set of symbols required for reproducing the authentication label

difficult. The authentication label must be exposed if the label is to be copied. It is also detectable that a authentication label has been opened and possible copied. In order to produce an credible copy, the copier must produce a new copy of the label which is non-exposed, thus rendering the copying more cumbersome and costly and thereby less attractive.

Secondly, the use of unique set of symbols provides the possibility to uniquely link a the set of symbols to a single product. A database may be provided in which information pertaining to the product corresponding to the unique authentication label. In connection to an authentication of the product, such information may be provided from the database to a person performing the authentication.

By that the authentication label has unique set of symbols provides for one-time-authentication of each authentication label. By one-time-authentications is meant that each authentication label is permitted to be authenticated only once. Any further authentication may be blocked. Thus, a specific authentication label cannot be copied and applied on multiple copied and fake products. The copier must copy one authentication label for each copied product, thus making the copying time-consuming and costly.

The set of symbols may be presented in the form of one or a combination of the following: a barcode, a QR code, an NFC code, an RFID tag, or a transcription.

The set of symbols may be a serial number.

The authentication label may be irreversibly exposable by scratching or pulling off a cover layer from the authentication label.

It is noted that the invention relates to all possible combinations of features recited in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

This and other aspects of the present invention will now be described in more detail, with reference to the enclosed drawings showing embodiments of the invention.

Figure 1 illustrates a set of authentication labels.

Figure 2 illustrates a product package comprising the set of authentication labels.

Figure 3 illustrates an embodiment of the structure of an authentication device and an authentication server.

Figure 4 illustrates another embodiment of the structure of the authentication device.

Figure 5 illustrates a method for authentication of a physical product.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which currently preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided for thoroughness and completeness, and for fully conveying the scope of the invention to the skilled person.

In the following, the invention will be disclosed with reference to a set of authentication labels. It is understood that inventive concept is applicable to a single authentication label as well.

A set of authentication labels comprising a first label 10 and a second label 12 is illustrated in figure 1. The first label 10 is a sticker made in e.g. paper or plastics. The first label 10 comprises a first set of symbols presented in the form of a barcode 11. The second label 12 is also a sticker and comprises a second set of symbols in the form of a transcription 13. By transcription is in the context of this application meant that the set of symbol is written out or typed out in full without altering the appearance by e.g. the use of a QR code or a barcode, or by encryption.

The set of symbols on the labels may comprise uncoded information, such as a product name in plain text, or may comprise a randomly selected number which is connected to information relating to the product in the database. In this embodiment, the second set of symbols comprises a combination of randomly selected numbers and letter as a first portion 14 and

as a third portion 16 of the transcription 13. The second portion 15 of the transcription is formed by readable information in plain text, in this case the product name "MEDX".

The first set of symbols and the second set of symbols are chosen in view of a predetermined algorithm. When the set of symbols are input to the predetermined algorithm, an authentic output is obtained. The predetermined algorithm compares or combines the input set of symbols. There exist many types of feasible algorithm which may be used, for example check-sum algorithms. A person skilled in the art of authentication and encryption has the knowledge of determining a suitable algorithm depending on desired security level and prevailing circumstances.

The purpose of the set of authentication labels is to provide a possibility to authenticate a physical product on which the first label 10 and the second label 12 are provided. In this embodiment, the first label 10 and the second label 12 do not function for authentication alone. Information from both labels are necessary in order to perform the authentication. Thus, an ill-intentioned person who wants to produce copies of the labels would have to copy both labels.

The second label 12 is arranged to be unreadable and irreversible exposable for reading. By unreadable is meant that, when the second label 12 is arranged on a product package, the second set of symbols cannot be read from the label.

The action required for making the second label 12 unreadable depends on the type of label. For example, a second label 12 in the form of a paper sticker, as in this case, may be attached with the transcript side (comprising the transcript 13) against a non-transparent package. Thus, the sticker needs to be separated from the package in order to make the transcript 13 visible such that it may be read.

As another example, if the second label 12 is in the form of a NFC tag, the tag may be arranged within a shielding enclosure which needs to be removed in order to read the NFC tag. Further examples of irreversible exposable labels are a label provided with a cover layer to be scratched off,

similar to a scratch card, or with a cover layer to be pulled off; a sticker provided with a seal, similar to entrance bands to concerts or amusement parks; or a label attached with non-reusable adhesive.

Labels comprising visible information may easily be copied, by e.g. photographing one or more labels. Ill-intentioned persons could thus get hold of copies of codes or set of symbols without leaving a trace. According to the present invention, this type of copying is prevented by the use of the irreversible exposable second label 12. The second label 12, and thus the second set of symbols 13, must be exposed for enabling copying of the required information for performing a successful authentication. Hence, it will be apparent that a set of authentication labels has been exposed and possible copied. Further, each second label 12 in a plurality of set of authentication labels has to be exposed thus rendering the copying cumbersome.

The set of symbols is unique. By unique is in the context of this application meant that the first set of symbols, the second set of symbols or the combination between the first set of symbols and the second set of symbols are chosen such that no other set of authentication labels are provided with the same set of symbols. One way to achieve unique set of symbols is by generating them by a random symbol generator, such as a random number generator. Another advantage of using a random symbol generator is that the generated set of symbols are non-predictable, thus rendering it more difficult to copy the set of authentication labels.

Examples of systems for performing the authentication of a product provided with a set of authentication labels according to the above will now be disclosed with reference to figures 2–4.

A medicament package 20 provided with the set of authentication labels according to figure 1 is illustrated in figure 2. In this embodiment, the second label 12 is arranged on the backside of the first label 10. Thus, the first label and the second label forms one label unit. The second label 12, and thus the second set of symbols thereon, are exposed by pulling the first label 10 so as to expose its backside.

The inventive concept is applicable to any physical product, in particular products which are manufactured, distributed and sold to an end customer. Examples of product categories are medicaments, clothes, toys, furniture, fabrics, jewelry, and shoes.

The set of authentication labels may be attached to the product package 20 in connection to the production or packaging of the product. Alternatively, the set of authentication labels may be arranged on the package 20 before packaging the product. The set of authentication labels may be activated by a manufacturer by scanning the labels.

Figure 3 illustrates a first embodiment of the system comprising an authentication device 30 which is connected to an authentication server 34. Figure 4 illustrates a second embodiment of the system comprising only an authentication device 30.

Figures 3 and 4 illustrate components which are used during the authentication process. It is to be understood that the system may comprise further components for providing further functions.

The authentication device 30 in figure 3 comprises a reader 31, a processor 32 and a display 33. The reader 31 may be for example a camera, a NFC reader, a barcode reader, or an RFID reader. The type of reader 31 required depends on how the first set of symbols and the second set of symbols are presented.

In this embodiment, the authentication device 30 is provided in the form of a smart phone. Non-limiting examples of other feasible authentication devices 30 are a personal digital assistant (PDA), a laptop or other computer device, and a barcode scanner device.

The authentication device 30 comprises a software, so called applications for smart phones, for performing the authentication. Smart phones are commonly provided with a camera and/or a NFC reader. By the camera in combination with suitable software/applications, codes such as barcodes, QR codes or uncoded set of symbols may be read and the set of symbol therein may be interpreted to read out the set of symbols.

When the first set of symbols and/or the second set of symbols are presented uncoded, i.e. as a transcript of the set of symbol(s), the set of symbols may alternatively be read by manually reading and inputting the symbols into the authentication device 30 by use of a keyboard or similar input means.

In an alternative embodiment, the authentication device 30 may be a computer device located in a specific store selling the products. An end customer may thus authenticate the product in the store before purchase. The computer device may be sealed and/or be verified by an authority or a trusted manufacturer.

By the display 33 of the authentication device 30, the user may be provided with feedback during the authentication process, such as read set of symbols and authentication conclusion.

The authentication device 30 is connected to the authentication server 34. The authentication server 34 comprises a database 35 and a processor 36. In this embodiment, the authentication of the product is performed by the authentication device 30 being online, i.e. being in communication with the authentication server 34 during the authentication process. The communication may be performed through wired or wireless communication, such as through a GPRS network or a Wi-Fi network.

The database 35 comprises information connected to specific sets of symbols or specific combinations of sets of symbols. In other words, the database 35 comprises information relating to each product which has been provided with a set of authentication labels. Since the first set of symbols, second set of symbols or the combination of the first set of symbols and the second set of symbols are unique, the set of symbols may be uniquely linked to a single product package.

The database 35 comprises the authentic output and the predetermined algorithm connected to the set of symbols in a set of labels. Thus, by reading the set of symbols on the set of labels and inputting in into the predetermined algorithm, it may be concluded that, if the output from the predetermined

algorithm is equal to the authentic output, the set of labels are authentic and thus also the product.

Other information stored the database may for example be information relating to ingredients, recipe, batch, responsible manufacturer, date of manufacture, best-before date, distribution date, land code, regional code, etc.

The authentication device 30 may access the authentication server 34 via the Internet, such as via a web site. The access to the authentication server 34 may be controlled by the use of login. The web site may be available for different user groups such as producers, distributors, retailers and end customers. The database and/or web site may be configured such that different user groups has access to different information in the database 35 or different amount of information or access on different permission levels. For example, a manufacturer may have permission to add information to the database 35 of the authentication server 34 regarding which product are packed in a package provided on beforehand with a set of authentication labels.

A first embodiment of an authentication process which may be performed by the system in figure 3 will now be disclosed. In this example, the product to be authenticated is the medicament package 20 illustrated in figure 2.

The barcode 11 representing the first set of symbols on the first label 10 is read by means of the reader 31.

Next, the second label 12 is exposed for reading, i.e. the transcription 13 on the second label 12 is made visible. The second label 12 is exposed by removing the combination of the first label 10 and the second label 12, being arranged on the backside of the first label 10, from the package 20. The first label 10 is attached to the packaged 20 by an non-reusable adhesive, whereby the second label 12 cannot be unreadably arranged on the package again.

Next, the transcript 13 representing the second set of symbols on the second label 12 is read by means of the reader 31.

Next, the read first set of symbols and the read second set of symbols are input to a predetermined algorithm. The algorithm is decided when selecting the first set of symbols and the second set of symbols, i.e. in connection to the manufacturing of an authentic set of authentication labels, and stored in the database 35.

The algorithm is in this embodiment stored only in the database 35, and thus known only to the authentication server 34. The read first set of symbols and the second set of symbols are communicated to the authentication server 34 where they are input to the algorithm. The processor 36 in the authentication server 34 retrieves the predetermined algorithm and authentic output corresponding to the read set of symbols from the database 35.

If the set of symbols does not exist in the database 35, the processor 36 may conclude that the set of authentic labels are false and return this information to the authentication device 30 which notifies the user.

Depending on the type of algorithm, the read first set of symbols and the read second set of symbols are compared or combined, or both, with each other. The algorithm generates a verification output as a result.

Next, the verification output is compared to a predetermined authentic output.

Next, if the verification output is equal to the authentic output, it is concluded that the product is authentic. Else, if the verification output is not equal to the authentic output, it is concluded that the product is not authentic. The conclusion is communicated to the authentication device 30 which notifies the user.

Next, any further authentication relating to the same set of symbols is blocked. The blocking may be executed in many different forms which are apparent to the skilled person. For example, the authentication server 34 may block, in the database 35, any further retrieval corresponding to a particular transmitted read first set of symbols and/or read second set of symbols. Thus, a specific authentic output is allowed to be retrieved only once. Since the set of symbols of a set of authentication labels are unique, this means that the set of authentication labels on a product may be authenticated only once. This

one-time-authentication approach has many advantages. For example, a copier cannot copy a single set of labels and use on multiple copies. After one authentication, the set of symbols on the authenticated set of labels are used. The copies must thus provide each copy with a working set of authentication labels. As another example, if it is suspected, by for example a salesclerk, that a set of authentication labels has been copied by that the second labels is exposed, the salesclerk may block the use of any copy of the set of authentication labels by performing a single authentication.

It is understood that the steps may be performed in a different order, such as exposing the second label 12 before reading the first set of symbols.

Many alterations of the above method is possible within the inventive concept. The skilled person is competent in how the system and method may be altered while still achieving the authentication according to the inventive concept.

For example, the step of inputting the read set of symbols, the step of comparing the verification output with a predetermined authentic output and concluding the authenticity may be performed by the authentication device 30. The predetermined algorithm may be stored in the authentication device 30 or be requested from the authentication server 34.

Another example is that the authentic output may be requested by the authentication device 30 by transmitting the read first set of symbols and/or the read second set of symbols to the database 35 of the authentication server 34. By using request, the authentication server 34 may gather information about which authentication devices 30 are used.

The authentication device 30 in figure 4 is arranged to performed the authentication off-line, i.e. without any communication with the authentication server 34 during the authentication. The authentication device 30 in this embodiment also comprises a memory 40 in which one or more predetermined authentication algorithms and one or more predetermined authentication outputs are stored.

A second embodiment of an authentication process may be performed by the system in figure 4. Also in this example, the product to be authenticated is the medicament package 20 illustrated in figure 2.

The authentication process comprises the same steps as for the previous example, disclosed with reference to figure 3. However, in the present embodiment, the step of inputting the read first set of symbols with the read second set of symbols and the step of comparing the verification output with the predetermined authentic output are performed in the authentication device 30.

By that the predetermined algorithm and the authentic output is stored in the authentication device 30, the authentication process may be performed without exchanging any information with the authentication server 34. Thus, the authentication of a product is simplified.

The blocking of any further authentication may be stored in the authentication device 30 and communicated to the authentication server 34 at a convenient time, for example the next time the authentication device 30 is connected to the Internet. When connected to the authentication server 34, the locally stored algorithms and authentic outputs in the memory 40 of the authentication device 30 may be updated. Further, the information about which set of symbols are blocked may also be updated.

A system of authentication devices may be connected, at least now and then, to a single authentication server 34. Information about which sets of authentication labels that has been authentication, and thereby blocked, may thus be shared between the authentication devices via the authentication server 34.

The above disclosed authentication method is generally illustrated in figure 5. The method comprises:

- providing 501 the product 20 with a first label 10 and a second label 12
- reading 502 the first label 10
- irreversibly exposing 503 the second label 12
- reading 504 the second label 12

- inputting 505 the read set of symbols in an algorithm to obtain a verification output
- comparing 506 the verification output with an authentic output
- concluding 507 if the product 20 is authentic or not
- blocking 508 any further authentication of the set of authentication labels

In one embodiment, a product may be provided with a plurality of sets of authentication labels. Thus, the product may be authenticated by different players in a distribution channel. Since the authentication is blocked after the first authentication process thereof, a single set of labels would only suffice for a single player.

Within a distribution channel, the product may thus be arranged to be authenticated multiple times. In particular, a product may be authenticated in each distribution step. Thus, a plurality of authentications may be performed within the distribution channel for the product.

For example, a product package, may be authenticated for each of the following events: a) when a product arrives to a distributor from the manufacturer, b) when the product arrives at a retailer c) when the product is sold to an end customer, and d) when the end customer wants to authenticate the product after the purchase.

The system for authentication may be designed such that the authentication may be repeated using the same labels as long as the product is located at the specific player. This feature may be achieved by postponing the blocking for a specific set of labels until it has been concluded that the set of labels has been relocated to the next step in the distribution channel. The same or a plurality of linked authentication devices may be utilized for the authentication at a specific player.

The relocating of the product to another player in the distribution channel may be detected by the authentication server by that an authentic output is requested by a new authentication device or a authentication device that is not registered to the preceding player.

The system may be designed such that the authentication is achievable only with an approved authentication device. For example, the authentication server may perform a check if the authentication is approved before responding to a request of a authentic output. The database of the authentication server may comprise information about which authentication devices that are approved, for example by a list comprising serial numbers of approved such devices.

For each authentication, a receipt may be issued as a proof of a successful authentication. The receipt may be issued by the authentication server.

It is to be understood that the set of authentication labels does not need to relate to a single product, but could be attached to a freight box or a container comprising a plurality of product packages. Thus, a distributor or the like does not need to unpack the box or container in order to perform an authentication for the products.

As mentioned earlier, it is understood inventive concept of the above disclosed authentication is applicable to a single authentication label as well. In particular, instead of a set of authentication label, a single authentication label may be used. The authentication label is provided with a unique set of symbols and is adapted to be, when arranged on the physical product, unreadable and irreversibly exposable for reading. Further. the unique set of symbols is chosen such that, when input to a predetermined algorithm, an authentic output is obtained.

The authentication label thus corresponds to the second label in the above disclosed set of authentication labels. However, the set of symbols on the authentication label is not input together with another set of labels into the algorithm. This provides for a more simple way to arrange the authentication label on the product package, and for a more simple authentication.

The principles of the authentication is the same as disclosed above. The skilled person has knowledge in how to modify, if necessary, and apply the above disclosed method and system to a single authentication label.

It is understood that the above disclosed embodiments may be combined or altered within the scope of the claims. For example, in one embodiment, the set of authentication labels comprises further labels. The set of authentication labels may be arranged on top of each other in a multilayered structure such that only one label is readable at a time. In order to authenticate the product, a user reads the set of symbols located on the top label, exposes the next label by removing the top label, thus making the next label the new top label, and reading the set of symbols on the new top label. By the read set of symbols, the product may be authenticated according to the above method. The next authentication of the product is performed by first reading the current top layer, exposing the next layer such that this layer becomes the new top layer and reading the new top label. Thus, a plurality of authentications may be enables by a single set of authentication labels attached to a product.

CLAIMS

1. A set of authentication labels for being arranged on a physical product (20), the set of authentication labels comprising:

a first label (10) provided with a first set of symbols (11); and

a second label (12) provided with a second set of symbols (13);

wherein at least the second label (12) is adapted to be, when provided on the physical product (20), unreadable and irreversibly exposable for reading;

wherein the first set of symbols (11), the second set of symbols (13) or the combination of the first set of symbols (11) and the second set of symbols (13) is unique; and

wherein the first set of symbols (11) and the second set of symbols (13) are chosen such that, when input to a predetermined algorithm, an authentic output is obtained.

2. The set of authentication labels according to claim 1, wherein the first set of symbols (11) and/or the second set of symbols (13) are presented in the form of one or a combination of the following: a barcode, a QR code, an NFC code, an RFID tag, or a transcription.

3. The set of authentication labels according to any of claims 1–2, wherein the second set of symbols (13) is presented as a print on the second label (12), the second label (12) being arranged on a backside of the first label (10).

4. The set of authentication labels according to any of claims 1–3, wherein at least one of the first set of symbol (11) and the second set of symbols (13) is a serial number.

5. The set of authentication labels according to any of claims 4–6, wherein the second label (12) is irreversibly exposable by scratching or pulling off a cover layer from said second label (12).

6. An authentication label for being arranged on a physical product, wherein:

the authentication label is provided with a unique set of symbols;

the authentication label is adapted to be, when arranged on the physical product, unreadable and irreversibly exposable for reading; and

wherein the unique set of symbols is chosen such that, when input to a predetermined algorithm, an authentic output is obtained.

7. The authentication label according to claim 6, wherein the set of symbols is presented in the form of one or a combination of the following: a barcode, a QR code, an NFC code, an RFID tag, or a transcription.

8. The authentication label according to any of claims 6–7, wherein the set of symbols is a serial number.

9. The authentication label according to any of claims 6–8, wherein the authentication label is irreversibly exposable by scratching or pulling off a cover layer from said authentication label.

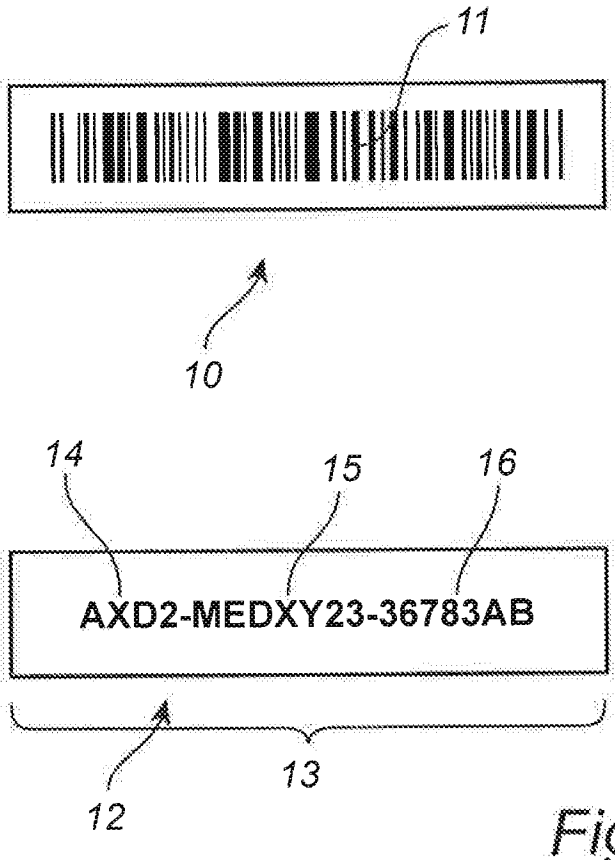

Fig. 1

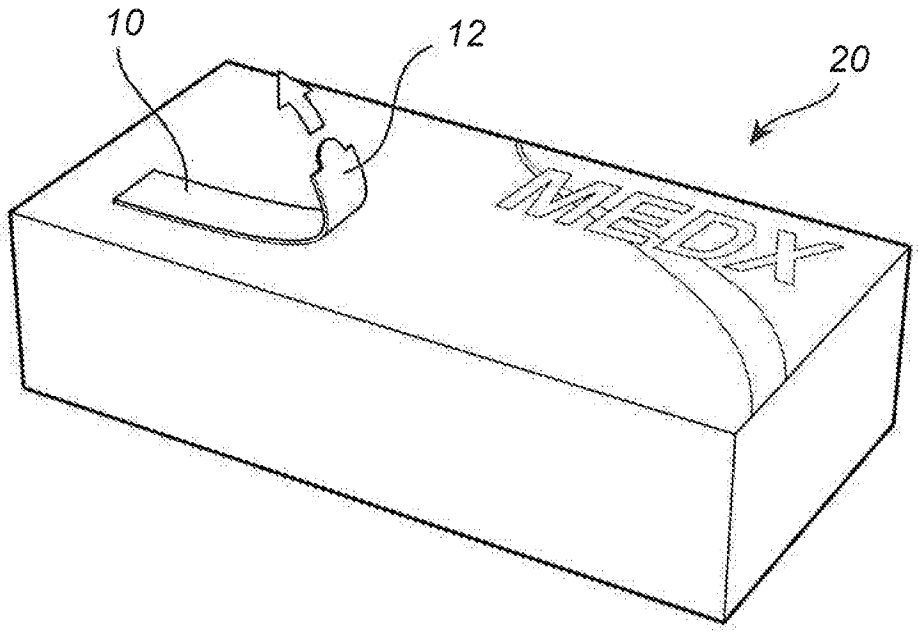

Fig. 2

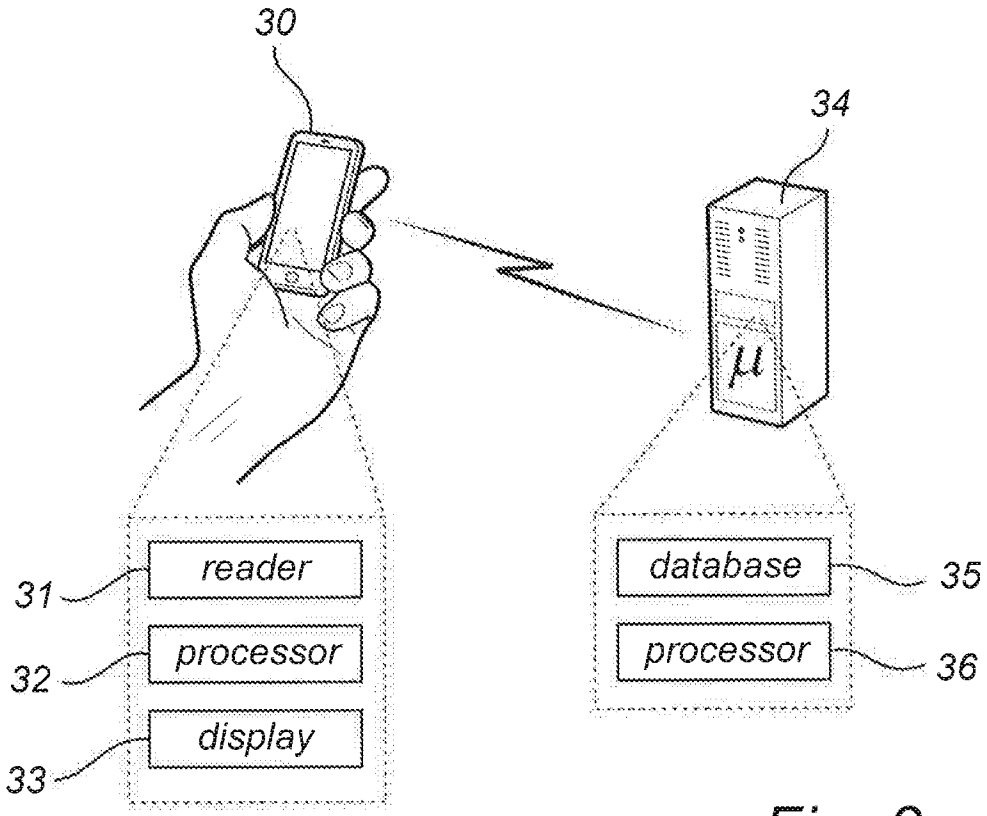
30
34
reader
processor
display
database
processor
31
32
33
35
36

Fig. 3

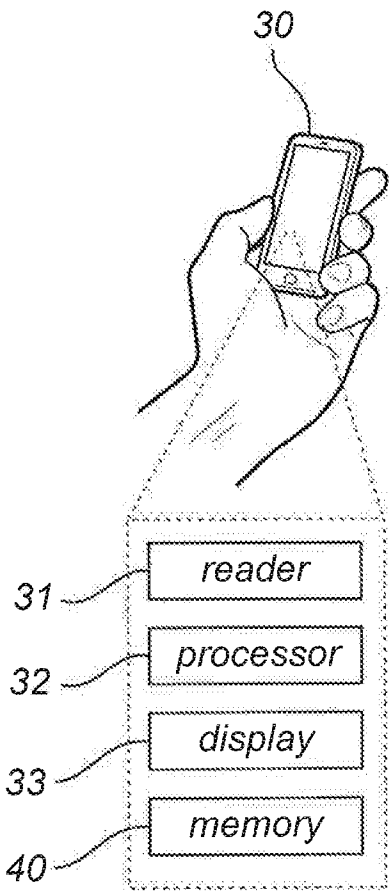
30
reader
processor
display
memory
31
32
33
40

Fig. 4

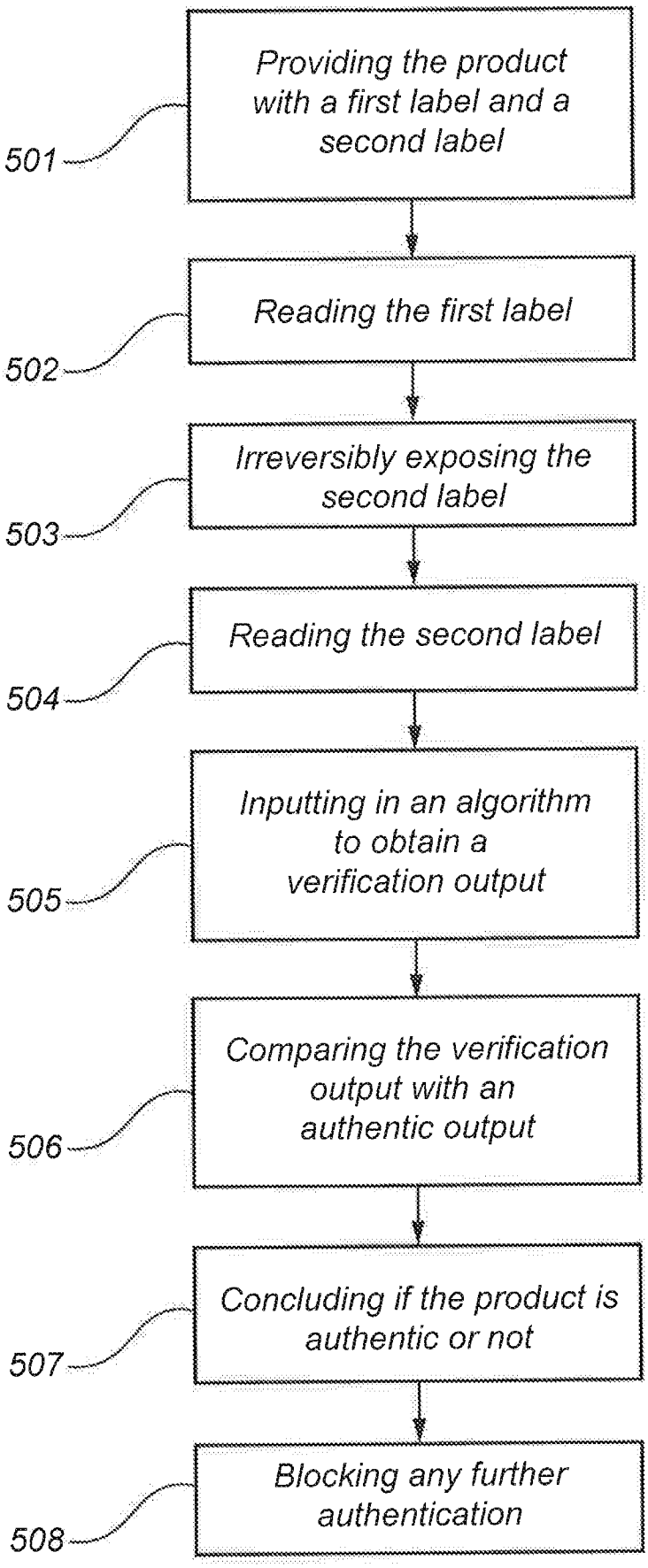
Providing the product with a first label and a second label
501
Reading the first label
502
Irreversibly exposing the second label
503
Reading the second label
504
Inputting in an algorithm to obtain a verification output
505
Comparing the verification output with an authentic output
506
Concluding if the product is authentic or not
507
Blocking any further authentication
508

Fig. 5