** MACHINE TRANSLATED DOCUMENT **

** TRADUZIONE AUTOMATICA **

Description

"PROCESS ANTI-CONTRAFFAZIONE on BASE Collaborative"

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention relates to a method for verifying the originality of a product or batch of products.

[0002] In particular, the process is essentially based on the generation, management and verification of codes based on digital signatures to identity and a condition/state vector, said authentication codes material or physical Authentication Code (PAC) .

STATE OF THE ART

[0003] The anti-counterfeit methods may essentially be divided in two large categories, first to second employing discriminating techniques of analogue or digital type. In the category of methods based on analog fall all the conventional methods, consisting in the production of labels, trademarks and reproduction difficult seals, possibly combined wrappers equally difficult to tamper. These methods are certainly the currently most widely used to protect both the electronic exchange means not that of some commercially available products. In particular, the techniques used to counter the counterfeit banknotes are numerous and together represent anti-counterfeit system based on analog quintessential. For example, currently the Euro bank notes are printed with a watermark of which represents a particular architectural style present thereon together to the nominal value. The watermark is visible by placing the banknote backlighting. In addition to the banknotes can be inserted watermark, holograms and iridescent, strips and the banknotes from the 50 euro the nominal value present in the corner at the bottom of the right side of the back of the banknote and printed with an ink changing (or optically variable), i.e. that changes color according to the angle of inclination. However all these techniques are sophisticated, do not allow to obtain a complete protection from false. This has made it necessary, on the one hand, the institution of suitable processes performed by monitoring the counterfeiting dedicated organisms (e.g. central office Payment means of fraud; counterfeit Monitoring System)and, on the other hand, the use of

dedicated equipment able to distinguish effectively a false from an original. The evolution of industrial manufacturing techniques and the use of an increasing number of materials, if on the one hand, they allow to provide mechanisms always more sophisticated anti-counterfeit, constitute factors-organisms enabling to perform reduced times and costs less and less easily distinguishable from the original reproductions. Therefore, with the passing of time the traditional techniques are experiencing anti-counterfeit ever greater extent the following two disadvantages:

. require production and materials sufficiently complex and expensive in order to be able to provide good safety standards, whose cost is not turned down in production of scalar. For these reasons, these techniques can not be applied to products of low cost;

. it may not be easy for a user to an operator for sale or distribution or an agent controlling comprise if a given trademark or object is original or counterfeited, unless they are not of apparatuses dedicated auxiliary.

[0004] Therefore anticounterfeiting systems have been developed alternative to the conventional systems that are based on techniques of digital type. These digital systems using specific means or channels for representing the value of coding, suitable algorithms for the generation of codes, and specific processes for the control and the validation of the latter. As regards the type of medium or channel, different are the proposed technologies which use radio frequency (RFID) , or based on the use of two dimensional bar codes. In the Italian patent for example fall into this category the designs Trace cheese" and "and-spumante tracing . The first face to the exploitation of cheeses of double mattress with, comprises the application of RFID technologies for the traceability of products while the second one allows to make available the information of die relative to a bottle of wine thanks to significant amount of information that may be encoded with a two dimensional bar code. Recently have also been developed RFID tag very thin, so that it can be inserted the banknotes so that they are more difficult to be counterfeited. As regards the coding algorithms many proposals involve the use of simple alphanumeric codes, while other make use of cryptographic techniques. Finally, as regards the

process of management and verification of said codes, in some cases it is contemplated the comparison with a database server side which takes into account the codes generated so as to ensure that each code emitted is unique.

[0005] In any case, an analysis of anti-counterfeiting systems based on digital so far proposed shows both the need that the possibility of solutions more effective in terms of pracabilita implementation that of practicality of use and reliability.

[0006] Object of the present invention is to propose an alternative solution to the problem of checking the authenticity of a product originality/with respect to the current state of the art.

SUMMARY OF THE INVENTION

[0007] The present invention concerns, as already indicated, to a method for verifying the originality or in any case the reliability of a product or batch of products. In particular, the process is essentially based on the generation, management and verification of codes based on digital signatures to identity and a condition/state vector, said authentication codes material or physical Authentication Code (PAC) .

[0008] The invention described herein consists of a process in which, in the specific, is combined with substantially to a digital coding virtually unalterable, which allows to identify product and manufacturer, a step of controlling and managing the codes emitted to which contribute both the final users of the product that the elements designed to control, such as for example the customs.

[0009] The main advantages of the process of the invention with respect to current solutions consist of the following.

[0010] By virtue of the digital signature mechanism implemented in them the PAC enjoy first properties of authenticity of inalterability and nonrepudiation services. Authenticity: for each product or batch, the relative PAC can be generated only by authorized producer, so that products or different lots correspond different codes. Inalterability: a PAC modified in any part of the unauthorized from a subject is not able to overcome the check test, therefore being not valid. nonrepudiation services: in case of dispute

pronounce a third part can check whether or not a given code is relative to a given manufacturer.

[0011] Moreover, the use of a scheme based on identity allows to avoid the use of the certificates to public key and to use such as identification for checking the authenticity of a product name or trademark of the product itself or the name of the manufacturer or legal.

[0012] Finally, the process of controlling and managing the codes generated, strong of the participation of different figures between which the final users in addition to the one of the elements meant to control, offers the guarantee of codes of duplicate and ensuring a one to one corresponding between active codes and individual products or lots.

[0013] In general, therefore, the method described herein is a highly effective solution to the problem of the counterfeiting of products, ensuring a safety to the originality of the product or batch to the purchaser and control of illicit activity to the detriment of the manufacturer. It is therefore subject of the present description is a method for verifying the originality of a product or batch as defined in independent claim 1.

[0014] In particular, The process comprises the following steps:

-- generating a secret key and the corresponding public key that will act as an identifier of the service and of its version;

- generating a signature key related to the product/Manufacturer on the basis of the following data

(a) first data related to said product or Manufacturer;

(b) and the said secret key ;

- generating an authentication code of the product or material batch comprising

(i) fields in clear comprising second data related to said product or batch

(ii) identifying said code;

(iii) a field obtained by digital signature fields (i)and (ii)by virtue of said key;

- attributing to said signature code a state that is a data structure suitable to manage at least the activated Active conditions (Usable)is

used, for example by means of a pair of Boolean variables state being univocally associated with digital certificate composed of the fields (i) - (iii) thanks to the identification code (ii);

-apply said code on said product or batch in such a manner that it can be read by means of controllo;l'

originality of the product or batch being verified by:

- reading and comparison between the data present in said fields in the clear and said field signature via said control means; and

- control of the state attributed to the code by means of said control means and connection to the service state can be modified by Active (Usable)a used when the product is sold or smerciato ;

wherein said product or batch and counterfeit or not can be sold/smerciabile

- if there is no correspondence between at least one of said fields in the clear and said field of signature code PAC, and/or

the code is activated in the state or in the used.

[0015] In one embodiment of the invention, said product or batch and counterfeit or not sold/smerciabile PAC when the code is not more current that is given when the expiry date of the product/batch or of said code, as better explained in the following is exceeded.

[0016] In another form of embodiment of the invention , said product or batch when the code is counterfeited PAC and multiple i.e. when said code is located in more than one point on the territory.

[0017] Preferred characteristics of the object of the present invention are set forth in the dependent claims.

[0018] Further advantages, as well as the features and the modes of employ of the present invention will become apparent from the following detailed description relating to the possible embodiments thereof, presented by way of example and not for limitative purposes.

BRIEF DESCRIPTION OF THE FIGURES

[0019] Figure 2 shows the cryptographic methods related to the phase of activation of the service provided by the supplier F and recording of the producer P or the product. In particular, SetUp=algoritmo for the

calculation of the public key encryption of the service provided by the Supplier; secKeyF=chiave secret; sysPar=parametri public service offered by the Provider of the system; pubKeyF=chiave public KeyGen=algoritmo encryption of the service provided by the Supplier; for the generation of the key of signature; prodId = denominazione of the Manufacturer and/or the product; codeEx =data expiration date of; sgnKeyP=chiave signature code related to the product/Manufacturer ; .

[0020] Figure 3 schematically illustrates the cryptographic procedures relating to the generation of an app and a code PAC in accordance with an embodiment of the present invention. In particular: SgnGen=algoritmo encryption of generation of digital signatures; secKeyF=chiave secret appId=identificativo unique; of the service offered by the Provider of app; sysPar=parametri public of the system; appSgnF= firma the app affixed by the Supplier; prodNum= numero product or batch; codeId= identificativo unique code of PAC; fields opzionali= zero or more of the following fields ProdEx=scadenza product or batch; prodCer= certificazioni product; prodUpc= codifica Universal Product Code (UPC) or sgnKeyP= chiave signature; equivalent relative to the product/Manufacturer; codeSgnP=campo digital signature of the code PAC relating to the product/Manufacturer; ;

[0021] Figure 4 shows a diagram of the verification of a app is a code PAC by a producer P of a handler G or a user U. In particular: SgnVrf=algoritmo cryptographic signature verification; for the pubKeyF=chiave public of the service offered by the Provider appSgnF=firma of the app affixed by the Supplier; sysPar=parametri public of the system; appId=identificativo unique codeSgnP= campo code of app; digital signature of PAC relating to the product/Manufacturer; prodId = denominazione of the Manufacturer and/or the product; codeEx =data expiration date of the code; {0,1 } = possible values returned by verification algorithm: 0=firma valid 1=firma nullifies.

DETAILED DESCRIPTION OF THE INVENTION

[0022] The present invention which relates to a method for verifying the originality of a product or batch of products.

[0023] In particular, the process is essentially based on the generation, management and verification of codes based on digital signatures to identity and a condition/state vector, said authentication codes material or physical Authentication Code (PAC) .

[0024] A product in which it is desired to check the originality can be either a well of consumption and also a document, a work of art, checks, credit cards, good meal, banknotes but also a payment method. In other words, the term product is used herein to indicate in any type of object concrete that can be reproduced in a manner that is illicit without authorization of the manufacturer and which therefore represents a false.

[0025] In one embodiment of the invention the method essentially comprises four types of main figures that is a service provider F, a producer P, a user U and the handler G.

[0026] In particular, the service provider F and the figure responsible for the generation of secret chiava and of the corresponding public key corresponding to the service and to its version and of all the codes PAC. The producer P is instead an organization or company that is directed to the service provider in order to provide a system for combating the counterfeiting of its products and therefore allows, to anyone has interest to check the originality of the products or batches manufactured by or for its company. A user U is a purchaser of the product or batch marketed or a user of the document or payment means and is the one who needs, preferably by means of a dedicated application or a web interface, information about the originality of a product or batch of products. Finally, the role of the handler G, whose main function is, as better specified in the activation of codes PAC, is coated with one or more of the following figures: supplier, producer and assigned to the control and/or distribution and/or sale of the product or batch.

[0027] The process described herein is configured substantially as a service which can be used preferably by Web or by applications (app)for mobile devices to which it is possible to access, for example, upon recording. By way of example , under a commercial profile recording can be free for the operators and users, while the Manufacturers may be subject to a cost.

[0028] The first step of the method of the invention and therefore the generation of a secret key and of the corresponding public key, that are uniquely associated to the offered service by F and to the version of it. The subsequent step is instead the generation by F of a key for a signature producer P or for a given type of product of P. This key of signature corresponds univocally to the first data relating to the product or batch and to the public key of the service. Specifically, the key of signature can be generated on the basis of the name and/or brand of the product and/or denomination of P. The key of signature is managed by the Supplier with properties of absolute confidentiality and integrity.

[0029] In the following is generated an authentication code material (Physical Authentication Code; PAC)be associated univocally to each product or batch of products manufactured by the producer P.

[0030] A PAC is obtained by combining a digital signature mechanism appropriate with a process for controlling its state server side. An authentication code material is substantially a document digital generated for the Manufacturers and managed by the Supplier, which contains, as detailed hereinafter, of the fields in clear field and a digital signature, as shown in Figure 1 and to which is associated a data structure composed of at least two bits of information, called state of PAC.

[0031] The authentication code material comprises

(i) fields in clear comprising second data relating to the product or batch and/or manufacturer;

(ii) an identifier of said code

field; (iii) a digital signature obtained by the fields (i)and (ii)thanks to a signature key.

[0032] Also associated to the code and a state of the code, that is to say a data structure suitable to manage at least the conditions activated Active (Usable)

[0033] is used,and optionally the condition single/ultiplo), which is univocally associated with digital certificate composed of the fields (i) - (iii) thanks to the identification code (ii).

[0034] The second data of the product or batch can include the name of the

product and/or the category of the product and/or of the watermark and/or serial number and/or batch number and/or the expiration date of the product or batch and/or at least a certificate relates to the product. In one embodiment of the invention the fields in clear of the code can comprise:

- Name or trademark (prodId)comprising specific adapted to identify univocally the Manufacturer or the product. These specific can consist of a registered trademark and/or in the type of product, or in the denomination and/or business and in road address of the producer P, according to what reported in the registers of the chamber of Commerce of the country in which;
    - expiration date code (codeEx): indicating the expiration date attributed to material authentication code generated and coinciding with the given up to which the key should be considered valid signature relative to the product or
    service Manufacturer; - public key (pubKeyF): public key associated univocally to the service and to its version;
- product or batch (prodNum)comprising specific adapted to identify univocally the product or batch which the code is riferisce.Nel case of a means Payment, such a specification may be, for example, the serial number corresponding. In the case of a consumer product, instead the prodNum can be: a code indicating whether the unit can be sold of product is distinguished by a lot number or a serial number and/or the corresponding alpha-numerical value corresponding. If the unit is sold of product is distinguished by a number of batch which by a serial number, the fields may be reported only those corresponding to the serial number;
- Encoding UPC (prodUpc): field that for example in the case of consumer goods, contains the value Universal Product Code (UPC) which indicates the type of product;
- expiration date product (prodEx): specific for example present for those products or payment reception means that show an expiry date beyond which the quality of the product could not be longer guaranteed;
- Certification product (prodCer): indicating any certifications relative to

the product. For example, in the case of products from organic farming, this field can bring the code of the operator control MiPAAF authorized by the Manufacturer and the number associated subject to control;
- identification code (codeId): indicating a unique identification (e.g. value serial and/or time instant of emission)of the code PAC;

[0035] The field digital signature (codeSgnP)is obtained digitally signing the following fields, if present: product or batch, coding, expiry product, UPC product Certification and identification code.

[0036] In one embodiment, the authentication code can be represented by a bar code, for example a code QR-code.

[0037] In accordance with nature of service offered by the provider F, preferably allowed to the producer and the access to the service request codes with properties, confidentiality and integrity of availability, thanks to which the manufacturer may require, receiving and printing the codes PAC by means of suitable devices. The codes may be sent to the producer as files in formed row (e.g. Unicode)or graph (e.g. JPEG)corresponding, for example, a serial numbers or batch of the product, possibly in files compressed by means of a standard Internet protocol for the transmission of rows. In said light the printing devices in possession of the manufacturer preferably are capable of:(a)acquiring data in one or more digital format suitable and,(b)printed graphic codes digital.

[0038] The authentication code generated material can be placed immediately in the active state, or activated at a later time. For "active code" is meant in the present description a code for which can verify the validity. The code is not valid if there is no correspondence between the field signature and the relative fields in clear and/or the code is not current and/or the code is passed toggles between active (i.e. is in the state used)and/or the code and multiple, as better explained below.

[0039] The activation of the code can occur both by means of the supplier F both by the producer P or even by personnel assigned to product distribution or batch. In particular, the producer can decide whether authentication codes receive from the service state material already active if selectively activate the codes at the time of production, or if they activate at a subsequent

stage along the network of storage and distribution of the product or batch, according to the mode of distribution and sale of goods corresponding. In such cases this activation can be carried out directly at retail points of sale.

[0040] Once activated, the code will remain active as long as the product or batch to which is associated does not will be sold or not more than smerciabile. In particular, in the case of sale of the product or batch, the state of the code will be modified between Active used.

[0041] According to the method described above, furthermore the authentication codes material are characterized by a duration of validity and from a given expiration date product (optional), passed one of which the code is no longer valid. The duration of the code and the possible expiration date product are affixed concretely in appropriate fields in the clear of the code. They can be immediately checked both manually and by means of the app verification by someone who has interest to make it as, for example, a user. In particular, the code will be valid until expiry date of the product has not been exceeded, or that its duration of validity is not expired. In the contrary case, the code is not valid.

[0042] More in detail, the code PAC in accordance with the present invention will be

. If the field "authentic " signature coincides with a suitable cryptographic signature obtained from certain fields of code thanks to the public key of the service and the verification key represented by fields and codeEx prodld.

. If the field "current" expiration date product is not instantiated, and if the data reported in the field expiration date code is not exceeded, or if the data reported in the field expiration date product is not exceeded.

. In a state "Active" if it has been made as to a manager and has not been subsequently inactivated from the same or another operator or optionally by a user;

. "Single" if on the basis of the input provided by users and operators, one and the same code is not associated with two products or distinct batches.

[0043] A code which satisfies all the above properties described valid, and

otherwise invalid. Correspondingly, the product associated with the code must be considered as original and sold/smerciabile in the case in which the code is valid, and counterfeit or not sold/smerciabile in the contrary case.

[0044] As can be deduced from the above description , the process which results in its entirety to establish whether a given code is valid or not can be composed of distinct steps in terms of interaction and effects on the system. A step is constituted by the actions of verification of the authenticity and current state of the code, which can be carried out in local, without direct intervention of an operator and without any modification to the state of the system.

[0045] A further step is the one that involves a modification of a code by active to inactive and signalling turn corroborate or to invalidate the properties of uniqueness. This second step that - unlike the first - is of the active type, i.e. presumes a communication with the system and has the outcome to change its status. As already indicated, modifications of the state from which can be activated to Active and that can be exerted only by providers, while the modification from the Active state to that used could be exerted in addition to the providers also by users.

[0046] merely by way of example , the points of sale can be equipped with cash registers provided with readers of authentication codes to be able to accomplish the task of deactivating the codes relative to products sold, or arrange suitable reading unit and management of the codes immediately before the box points. Alternatively, it would be possible to arrange for the output of readers of the points box bar to be remote service management unit or to a local dedicated exclusively to the deactivation of the codes. This solution presupposes that the users have the possibility to check the validity of the codes autonomously by for example smart telephones provided with app of verification. A further scenario is that in which the users is allowed to deactivate the codes through the app of checks, in which case the point of sale could avoid to implement the whole code readers/inspectors PAC. For example verification functionality with deactivation of the codes could be allowed only to those users that are

connected to service through WiFi officially offered by the connection point of sale for this purpose, if necessary in the presence of appropriate adjustment by the same, as a deterrent deactivations erroneous or illicit actions on the part of users.

[0047] The generated code univocally for a given product or batch as indicated above is therefore applied on the specific product or batch before the introduction on the market and in such a manner that the code can be read by control means. By way of example the authentication code material can be applied to the package of the product externally to the materials of packaging. By way of example and not limiting control means can be devices, preferably mobile, designed to be connected to the Internet and comprising at least one camera and/or a camera. In an embodiment, such devices are smart phone, computers, portable computer, tablet. It is obvious that these devices, for the purposes of the present invention must be provided with a computer application (app)capable of to read the codes described herein is to provide, on the other, the required information (authenticity or less of the product)by means of the connection to the system managed by the supplier F. Furthermore, the system must be able to discriminate different roles, for example, the manager and the user. This discrimination can be effected on the basis of both the type of app or web interface.

[0048] Moreover, the control means can be also able to geo-location of the product or batch is affixed on which said code. In this embodiment therefore, in addition to the verification of the authenticity of the product or batch, it is possible also a location of the same on territories of production, distributing and/or selling.

[0049] In the case the control means also allow the geo-location, it is also possible to provide a invalidation of the code when the latter is located in more than one point on the territory. When the code is located at several points of the territory, the code and said multiple.

[0050] According to the process described herein, the originality of the product or batch and therefore verified by first of all the reading of the codes by the control means. Substantially the reading can also provide for a control of

the fields of expiration date (product and code)and a comparison between the data present in the fields and in the field signature. In the case in which the data on a field in the clear and field not already correspond naturally signature, the product or batch would be not original i.e. counterfeited. The inventive step can also be also checked by means of the control of the state attributed to the code. In particular, a product or batch will not be sold/smerciabile applied thereto when the code is not active, i.e. is activated when the code is in the state or in the used.

[0051] The process described herein can also be comprised in a control system of the type anti-adulteration of a product or batch. In fact in this context assumes particular importance not only the monitoring the composition of the original product through suitable techniques such as chemical methods, etc. but also the traceability of biotechnological products. In view of the above, the method described herein can represent a considerable added value for the reliability and the overall security of a system for the control of adulteration.

[0052] The present invention has hereto been described with reference to preferred embodiments thereof. It is to be understood that may be other embodiments afferent to the same inventive kernel, all of which are within the scope of protection of the claims set out below.