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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 June 2014 (26.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/095737 A1

(51) International Patent Classification:
G09C 5/00 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/EP2013/076725

(22) International Filing Date:
16 December 2013 (16.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12197525.4 17 December 2012 (17.12.2012) EP

(71) Applicant: **PHILIP MORRIS PRODUCTS S.A.** [CH/CH]; Quai Jeanrenaud 3, CH-2000 Neuchâtel (CH).

(72) Inventors: **CHANEZ, Patrick**; Route d'Yverdon-les-Bains 405, CH-1468 Cheyres (CH). **FRADET, Erwan**; Chemin du Grabe 3A, CH-1091 Grandvaux (CH).

(74) Agent: **PONDER, William Anthony John**; Reddie & Grose LLP, 16 Theobald Road, London Greater London WC1X 8PL (GB).

(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, 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, 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, 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: METHOD AND APPARATUS FOR MARKING MANUFACTURED ITEMS USING PHYSICAL CHARACTERISTIC

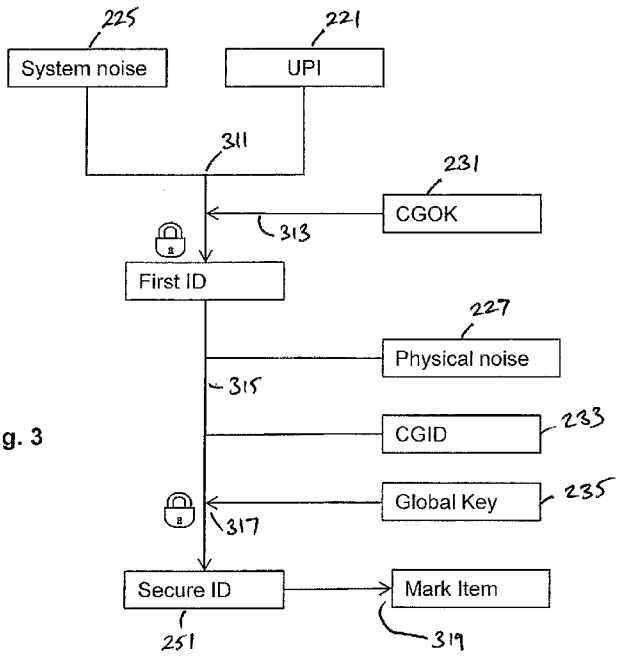


Fig. 3

(57) Abstract: A method of marking a manufactured item is described, comprising: creating a unique product identifier for a manufactured item; creating one or more encryption keys; generating a secret key using the unique product identifier and the one or more encryption keys; generating a system noise value by performing a hash function on the secret key and the unique product identifier; generating a physical key from a measured physical property of the manufactured item; generating a physical noise value by performing a hash function on the physical key and the unique product identifier; generating a secure identifier derived from or incorporating the system noise value and the physical noise value; and placing a mark on the manufactured item, the mark comprising the secure identifier or an identifier derived from the secure identifier. Also described are methods of authenticating items marked in accordance with the described method.

WO 2014/095737 A1

METHOD AND APPARATUS FOR MARKING MANUFACTURED ITEMS USING PHYSICAL CHARACTERISTIC

The present invention relates to methods and apparatus for marking manufactured items. In particular, the present invention relates to marking packaged goods.

Counterfeit and contraband goods are a global problem for customers, manufacturers, and government authorities. Counterfeit goods, which are unauthorized productions of goods usually of inferior quality, are illegally sold all over the world. These goods are detrimental to the customer because they could be of inferior quality which may be hazardous (this is particularly important for products such as pharmaceuticals or other consumed goods). Counterfeit goods are detrimental to manufacturers because they may suffer a loss of reputation, an increase in competition from illegal manufacturers producing their products, and infringement of other legal rights. Contraband goods, which are goods manufactured for the purposes of evading taxes or government regulations, are also a considerable problem for manufacturers and government authorities. These goods are illegally diverted, traded, or imported which results in significant losses of revenue to government authorities due to improper collection of duties or taxes.

It is advantageous to be able to authenticate manufactured items using unique markings on the items without needing to store every unique marking at the location where the items are to be authenticated. It is also desirable to be able to detect counterfeit items, or items for which the unique marking of an authentic product has been copied, without needing to store an authentication record of each unique marking.

In one aspect of the disclosure, there is provided a method of marking a manufactured item, comprising:

creating a unique product identifier for a manufactured item;

creating one or more encryption keys;

generating a secret key using the unique product identifier and the one or more encryption keys;

generating a physical key from a measured physical property of the manufactured item;

generating a secure identifier derived from or incorporating the secret key and the physical key; and

placing a mark on the manufactured item, the mark comprising the secure identifier or an identifier derived from the secure identifier.

The secure identifier may incorporate the unique product identifier.

Preferably, the method further includes the step of generating a system noise value using the secret key and the unique product identifier, wherein the secure identifier is derived from or incorporates the system noise value. Preferably the step of generating the system noise value comprises performing a hash function on the secret key and the unique product identifier.

Preferably, the method further includes generating a physical noise value using the physical key and the unique product identifier, wherein the secure identifier is derived from or incorporates the system noise value. Preferably the step of generating the physical noise value comprises performing a hash function on the physical key and the unique product identifier.

As used herein, "unique product identifier" means an identifier that uniquely identifies a manufactured item. Each manufactured item is given a different unique product identifier. The unique product identifier is typically a numerical or alphanumerical sequence or value.

As used herein, "encryption" means the process of transforming information using an algorithm to make that information unreadable to anyone except those possessing special knowledge in the form of an encryption key. Decryption is the reverse process. An "encryption key" is a piece of information that is used together with an encryption algorithm to encrypt or decrypt information. An encryption key is typically a numerical or alphanumerical sequence or value.

As used herein, the term "secret key" is used to describe a key used in a keyed hash that is generated using a unique product identifier and one or more additional keys or pieces of data. At the time it is generated, the secret key is not known by any other party than the party who created the secret key. The term "secret key" in this context is not limited to mean a private key in the context of an asymmetric encryption scheme.

As used herein, a "hash function" is a function that maps input data to a fixed size output (usually smaller than the input data) called a hash value. A hash function typically substitutes or transposes, or substitutes and transposes, the information to create the hash value or noise value. Preferably, the hash function is a cryptographic hash function. The cryptographic hash function produces a fingerprint or checksum of the input data. Two pieces of data can be assumed to be identical if using the same cryptographic hash function they produce the same hash value. Advantageously, the hash function is a one-way hash function, which means that it is computationally impossible to derive the input data from the hash value. These properties can be used in an authentication process, as will be described. A hash function can be keyed by combining a secret key and an input message in order to create a keyed hash value or noise.

As used herein the term "noise value" means a hash value, or a keyed hash value, or a value or character sequence derived directly from a hash value and a secret key.

The measured physical property of the manufactured item may be any measured physical property and may be based on mass, size, shape, surface texture or patterning, colour, chemical composition or response to a stimulus, such as response to electrical, magnetic or optical stimulus. The measured physical property is preferably chosen and measured to a resolution so that it is likely to be unique for each manufactured item, or at least is more likely to be different than the same for any two manufactured items. The measured physical property preferably provides a physical signature for the manufactured item. In a preferred embodiment the measured physical property is an image of a portion of the packaging of the manufactured item.

The secure identifier may be any type of identifier but is preferably a numerical or alphanumerical sequence or value. The mark may also be a sequence of characters or numbers or may be a graphical representation such as a one or two dimensional barcode.

In one embodiment, the step of generating the secure identifier comprises generating a first identifier by encrypting the unique product identifier together with the system noise value and generating the secure identifier by encrypting the first identifier together with the physical noise value.

In this embodiment, the method may further comprise authenticating the manufactured item at a verification centre, the step of authenticating comprising: identifying the mark on the item; decrypting the mark to derive the first identifier and the physical noise value; decrypting the first identifier to derive the unique product identifier and the system noise value; generating a new physical key from a measured physical property of the manufactured item; generating a new copy of the physical noise value by performing a hash function on the new physical key and the derived unique product identifier; comparing the new copy of the physical noise value with the derived physical noise value; and providing at indication of whether the derived physical noise value is identical to or correlates to the new copy of the physical noise value.

The step of comparing may comprise deriving a correlation score and the step of providing an indication comprises providing an indication of whether the correlation score is greater than a threshold value.

In this embodiment, the step of authenticating may further comprise: generating a new copy of the secret key from the unique product identifier and the one or more encryption keys; generating a new copy of the system noise value by performing a hash function on the new copy of the secret key and the unique product identifier; comparing the new copy of the system noise value with the derived system noise value; and providing an indication of whether the new copy of the system noise value and the derived system noise value are identical.

In another embodiment, the step of generating the secure identifier comprises generating a first secure identifier by encrypting the unique product identifier together with the system noise value; generating a second secure identifier by encrypting the unique product identifier together with the physical noise value; and placing a mark on the manufactured item, the mark comprising the first and second secure identifiers or an identifier or identifiers derived from the first and second secure identifiers.

In this embodiment, the method may further comprise authenticating the manufactured item at a verification centre, the step of authenticating comprising: identifying the mark on the item; decrypting the mark to derive the unique product identifier, the system noise value and the physical noise value; generating a new copy of the secret key from the unique product identifier and the one or more encryption keys; generating a new copy of the system noise value by performing a hash function on the new copy of the secret key and the unique product identifier; comparing the new copy of the system noise value with the derived system noise value;

generating a new physical key from a measured physical property of the manufactured item; generating a new copy of the physical noise value by performing a hash function on the new physical key and the derived unique product identifier; comparing the new copy of the physical noise value with the derived physical noise value; and providing an indication of whether both the new copy of the system noise value is identical to the derived system noise value and the new copy of the physical noise value is identical to or correlates to the derived physical noise value.

In either embodiment, the step of generating the first secure identifier may comprise encrypting the unique product identifier and the system noise value using a code generator key, wherein the step of generating the second secure identifier comprises combining the first secure identifier and the physical noise value together with a code generator ID, and wherein the code generator key can be derived or obtained from a look-up table at a verification centre using the code generator ID.

In either embodiment, the method may further comprise the step of storing the one or more encryption keys at a verification centre. The one or more encryption keys may comprise a static key and a dynamic key, and wherein a new dynamic key is created for each batch of manufactured items whereas the same static key is used for plural batches of manufactured items

The unique product identifier may include information identifying a batch of items to which the item belongs.

The invention provides the ability to authenticate both on basis of information from the manufacturer i.e. the various encryption keys, and on the basis of a physical property of the item. This provides two layers of authentication, and allows for the detection of cloning of identifiers on genuine items, but does not require large scale storage of authentication codes.

In another aspect of the invention, there is provided an apparatus for marking a manufactured item, comprising:

a key generator configured to generate encryption keys;

a code generator configured to generate a unique product identifier for each manufactured item;

a physical key generator configured to generate physical keys from a measured physical property of each manufactured item;

processing means configured to:

generate a secret key for each manufactured item using the unique product identifier and one or more encryption keys;

generate a secure identifier derived from or incorporating the secret key and the physical key; and

a marker for marking each manufactured item with the secure identifier or an identifier derived from the secure identifier.

Preferably, the processor is configured to generate a system noise value for each manufactured item using the secret key and a unique product identifier, wherein the secure identifier is derived from or incorporates the system noise value. Preferably, the processor is configured to generate the system noise value for each manufactured item by performing a hash function on the secret key and a unique product identifier.

Preferably, the processor is configured to generate a physical noise value for each manufactured item using the physical key and the unique product identifier, wherein the secure identifier is derived from or incorporates the physical noise value. Preferably, the processor is configured to generate the physical noise value for each manufactured item by performing a hash function on the physical key and the unique product identifier.

In one embodiment the processing means is configured to: generate a first identifier for each manufactured item by encrypting the unique product identifier together with the secret key or the system noise value; and generate the secure identifier for each manufactured item by encrypting the first identifier together with the physical noise value.

In another embodiment, the processing means is configured to: generate a first secure identifier for each manufactured item by encrypting the unique product identifier together with the secret key or the system noise value and generate a second secure identifier for each manufactured item by encrypting the unique product identifier together with the physical key or the physical noise value; and the marker is configured to mark each manufactured item with the first secure identifier and the second secure identifier or an identifier or identifiers derived from the first and second secure identifiers.

The manufactured item may be a container containing a tobacco product. Examples of tobacco products are cigarettes, loose leaf tobacco, cigars, and cartridges or refills for electrically heated smoking systems or other e-cigarette systems.

The invention allows manufactured items to be authenticated without requiring storage of large volumes of information. This is important for any practical system suitable for authenticating items produced in high volumes. Furthermore, the use of a physical key in combination with a unique product identifier (UPI) increases security and makes the production of counterfeit and contraband goods more difficult. The addition of a physical key provides a system that can detect cloning and is difficult to replicate. Even if a counterfeiter had knowledge of the particular tool used to generate the physical key, the combination of the physical key with a UPI to produce an identifier makes cloning almost impossible. The invention also allows for authentication to be carried out online, i.e. connected to a verification centre over a communications network based on the system noise value, as well allowing authentication to be carried out offline based on the physical noise value. The marking required on each item is simply one or more codes and so adds very little expense to each item when compared to some other solutions, which rely on expensive labels that are technically difficult to reproduce.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of a marking system according to one embodiment of the invention;

Figure 2 illustrates how the system noise value and physical noise value are derived;

Figure 3 is a flow chart showing a marking method of one embodiment of the invention, which may be carried out on the system of Figure 1;

Figure 4 is a flow chart showing an authentication method for the embodiment of the invention shown in Figure 3, which may be carried out on the system of Figure 1;

Figure 5 is a flow chart showing a marking method of another embodiment of the invention, which may be carried out on the system of Figure 1; and

Figure 6 is a flow chart showing an authentication method for the embodiment of the invention shown in Figure 5, which may be carried out on the system of Figure 1.

Unique markings on manufactured items can be used for tracking the items. For example, a customer order may be linked to the identifying label or labels of a particular shipping case or cases containing ordered goods. "Goods" in this context means manufactured items or other articles intended for distribution or sale to customers. This allows the customer, the manufacturer and any intermediaries to constantly track the location of the required goods. This may be achieved using scanners for scanning the identifiers and communicating with a verification centre. Alternatively, the identifiers can be read by a human, who can then manually communicate with a verification centre. Identifiers may also be used by customers, national authorities and other parties, to verify that a particular item contains genuine products. For example, a party may use a scanner to read the identifier on a shipping case (or the identifier can be read by a human, as discussed above). The identifier details may be sent to a verification centre. The verification centre can then lookup or otherwise process the identifier details, determine the shipping case production details and send those details to the scanner, thereby allowing the party to verify the shipping case, and the products contained therein, as genuine. In the event that the central database does not recognise the identifier, the party may suppose that the articles in question are counterfeit. The identifiers may also be used for tracing items. For example, if the manufacturer needs to recall the products from a selected number of shipping cases, those shipping cases can be traced using their identifiers.

Figure 1 is a schematic view of a marking system according to one embodiment of the invention. In this embodiment, system 101 comprises one or more production centres 103, 105, 107 for producing manufactured items 109. Each production centre may comprise a production line or facility which may be a cigarette making and packaging line. Preferably, production is carried out in batches, each batch being dedicated to the production of a certain number of individual manufactured items. If there are two or more production centres, these may be physically located at the same or different manufacturing sites. In this preferred embodiment, the

system includes production centres 103, 105, 107, but the invention may in fact be performed at an importation point, a distribution point, a purchaser, a wholesaler or any other point in the supply chain.

Each production centre includes a code generator 111 for generating codes for the manufactured items 109. Preferably, the code generator 111 is a fully autonomous computer or microcontroller dedicated to a particular production centre. Each production centre also includes a physical key generator 112 that measures or encodes a physical property of each manufactured item and converts that into a physical key 207. The code generator 111 uses the physical keys to generate codes for marking on the items.

In this embodiment, the physical key generator is of the type described in WO2007/071788. A portion of the packaging of each item is illuminated and an image of the illuminated portion captured by a digital image sensor. The portion of the packaging is chosen for its time stable, chaotic microstructure. Materials such as paper and cardboard have a chaotic microstructure which can be used as a "fingerprint" of the item. The image of the microstructure of the portion of the item is converted into a physical key or signature, as described in WO2007/071788, in the form of an alphanumeric value or matrix. A physical key generator of this type is available from Signoptic Technologies, Savoie Technolac, 5 allée Lac d'Aiguebelette BP340 F-73375, LE BOURGET-DU-LAC, France. However, any type of physical key generator may be used and might rely on other physical properties of the item such as mass or shape, or may even rely on chemical or biological properties of the item.

In this embodiment, each production centre also includes a marker 113 for marking the generated codes onto the manufactured items 109. The marker 113 may comprise any suitable marking means, for example but not limited to, a continuous ink jet printer, a drop-on-demand ink jet printer, a holographic printer, a laser printer, or any other printer or marker that allows printing or marking of the generated codes on the individual manufactured items. The printing or marking of the generated codes may be on each item, on an external package, on labels or in any other convenient way. In one embodiment, the generated codes are printed on adhesive tags or labels to be applied to the manufactured items, preferably non-removably. In one embodiment, the generated codes are printed by a laser beam on a layer of laser-sensitive material deposited on the manufactured item or on the item's packaging. This method allows a code to be impressed through a transparent wrapping layer.

The system 101 further comprises a verification centre 114 which includes a key generator 115 for generating keys 209, 211 for use in the marking and authenticating of the manufactured items and a central server 117. In this embodiment, the code generator 111 can communicate with the verification centre 114 via a secure internet connection 119 and a server 121 local to the production centre, or by other data communication means. Alternatively, the code generator 111 might communicate with the verification centre via a manufacturing portal dedicated to one or more production centres.

The key generator 115 generates a cryptographic key, herein referred to as a static key. The key generator 115 generates an unencrypted version of the static key and an encrypted version of the static key. The unencrypted version of the static key, herein referred to as the active static key 209, is shown with a solid border in Figure 1. The encrypted version of the static key, herein referred to as the inactive static key 211, is shown with a dotted border in Figure 1. The active static key 209, that is to say the unencrypted version of the static key, is generated in the key generator 115 and is therefore accessible to the central server 117. The key generator 115 sends the inactive static key 211 to the code generator 111 at the production centre 103, 105, 107.

The inactive static key 211 may be sent from the key generator 115 to the code generator 111 on a non-volatile data support, for example a CD-Rom, a DVD-Rom or a removable hard disk. The data support is physically transferred to the code generator 111 at the production centre 103, 105, 107. Alternatively, the inactive static key 211 may be sent from the key generator 115 to the code generator 111 via a secure network connection, for example one involving encryption. This may be on request from the code generator 111. This ensures authenticity, confidentiality and integrity of the static key.

The key generator 115 also generates the activation code 213, which comprises the key or code for decrypting the inactive static key 211 to form the active static key 209. This activation code 213 is also accessible to the central server 117. Preferably, the active static key 209 and activation code 213 are stored together with identification of the production centre 103, 105, 107 to which they are allocated.

In one embodiment, the static key comprises a number of portions. The primary portion may be a plurality of secret codes, for example a salt matrix. A salt matrix may be, for example, a long string of random or pseudorandom digits of characters. The number of portions may further include a unique identifier for the static key, a serialized code defining how the static key is to be combined with a dynamic key (discussed below), a digital cryptographic certificate associated the static key's unique identifier and a static key policy or licence that contains the digital cryptographic certificate generated above.

Preferably, the inactive static key, that is to say the encrypted version of the static key, and particularly the plurality of secret codes, is encrypted using a strong cipher. An example of a suitable cipher is the Triple DES (Data Encryption Standard) block cipher or the Triple DES/ Rijandel block cipher. Both apply the Data Encryption Standard cipher algorithm three times to each data block and the Triple DES/ Rijandel is a minor variation of the Triple DES which has been developed by IBM. In that case, the Triple DES or Triple Des/Rijandel key comprises the activation code 213. Thus, in a preferred embodiment, the active static key 209 is unencrypted, the inactive key 211 is encrypted using the Triple DES or Triple Des/Rijandel key, and the activation code 213 comprises that Triple DES or Triple Des/Rijandel key.

At next step 203, the inactive static key 211 received by the code generator 111 is registered. This is done by the code generator 111 sending to the verification centre 114 information 215 about the received static key and any relevant machine information (not shown). This is preferably sent via secure internet connection 119, as shown in Figure 1, but may be sent by another suitable route. The verification centre 114 sends back to the code generator 111 the activation code 213. The activation code 213 allows the inactive static key 211 to be activated, and this is shown schematically at 217. The activation code 213 is preferably also sent via secure internet connection 119, as shown in Figure 1. The registration procedure is preferably arranged such that the active static key 209 is never transferred over the internet.

The registration procedure may take the form of a conventional public/private key pair exchange mechanism. This may use an asymmetric key pair associated with the digital cryptographic certificate forming part of the static key, as discussed above. In that case, the public key of the asymmetric key pair may be in the form of a key issued by a third party, for example, a government authority. The information 215 about the received static key which is sent from the code generator 111 to the verification centre 114 may comprise the unique identifier for the static key which forms part of the static key, as discussed above. The relevant machine information (not shown) which is also sent from the code generator 111 to the verification centre 114 may comprise a unique identifier or certificate for the code generator 111 or production centre. That unique identifier may include information about the location and identity of the code generator or production centre, which has been pre-authorized for production. Preferably, the static key unique identifier and the code generator or production centre identifier are encrypted using the public key of the asymmetric key pair associated with the certificate of the static key.

Once the verification centre 114 receives the encrypted static key unique identifier and the code generator or production centre identifier, the verification centre 114 can decrypt using the private key of the asymmetric key pair associated with the certificate of the static key. The verification centre may then check that the static key unique identifier and the code generator or production centre identifier are valid. Then, the verification centre 114 sends back to the code generator 111 the activation code 213. As already mentioned, preferably, the activation code 213 is in the form of a Triple DES or Triple DES/Rijandel cipher. The verification centre encrypts the activation code (for example the Triple DES or Triple DES/Rijandel cipher) with the public key of the asymmetric key pair associated with the certificate of the static key. This allows the activation code (for example the Triple DES or Triple DES/Rijandel cipher) to be decrypted by the code generator using the private key of the asymmetric key pair associated with the certificate of the static key. Then, the inactive static key 211 can be activated using the decrypted activation code 213 in order to form the active static key 209.

Once the inactive static key 211 at the code generator 111 has been activated, the production centre is able to manufacture items and produce codes for the manufactured items at the code generator 111.

The code generator 111 generates a new key, herein referred to as dynamic key 219,for each batch of manufactured items. The dynamic key 219 is preferably a random secret code, such as a random number. The code generator uses the dynamic key 219 for a batch, together with the active static key 209, to generate a secret key 223. The secret key 223 is the n used in combination with the physical keys and a unique product identifier (UPI) for each item to generate codes 221 (for example alpha-numeric codes) to be marked onto the manufactured items in that batch. In this embodiment, the UPI for each item comprises production details identifying the time of production together with an incremental counter value to distinguish items produced within a single time period by the same production centre.

The code generator uses a cryptographic hash function on a combination of the UPI with the secret key and a combination of the UPI with the physical key. This creates digital fingerprints, referred to herein as "noise values", for the item, and these noise values are used to generate the codes 221 that are marked on the items by marker 113. In addition to commonly used cryptographic hash functions, a variety of techniques are available for generating the hash values or noise values, including, but not limited to: transposition, substitution, table substitution and indexing.

Figure 2 illustrates the method of generating the noise values carried out by the code generator 111. To generate the system noise value 225, the secret key is first derived from the active static key 209, the dynamic key 219 and the UPI 221. The dynamic key 219 and the active static key 209 are known only to the verification centre 114 and the code generator 111. In step 301 the dynamic key and the UPI are used to extract the secret key from the salt matrix contained in the static key, in accordance with the serialized code within the static key. The secret key 223 and UPI 221 are then hashed in step 303 to produce the system noise for the item. To generate the physical noise value 227, the physical key 207 is hashed with the UPI 221 in step 305. The hash function used to generate the system noise value may be the same or different to the hash function used to generate the physical noise value.

Figure 3 illustrates a method of using the system noise value and physical noise value to generate a secure identifier for each item in accordance with a first embodiment of the invention. In step 311 the system noise value 225 and the UPI 221 are combined. In step 313 the combined system noise value and UPI is encrypted by the code generator obfuscation key (CGOK) 231 to produce a first identifier 241. The CGOK is particular to the code generator and is pre-loaded onto the code generator. The first identifier 241 is then combined with the physical noise value 227 and a code generator identifier 233. The code generator identifier (CGID) 233 will allow the CGOK to be obtained during authentication. The combination of the first identifier, the physical noise value and the CGID is then encrypted using a global key 235 in step 317 to produce the secure identifier 251. The global key 235 is common to all production centres, and may be part of a symmetric or asymmetric key pair known by the verification centre. The secure identifier 251 is then marked on the item in step 319 by marker 113.

The code generator 111 or production centre 103, 105, 107 keeps a count of the codes which are marked onto the manufactured items. In addition, the code generator 111 sends the dynamic key 219 for each batch, together with information about the batch (not shown), to the verification centre 114. This may be performed via secure internet connection 119. The information about the batch may include various pieces of information, for example but not limited to brand, intended market or intended destination. The dynamic keys 219 do not need to be sent to the verification centre 114 in real-time and can be communicated to the verification centre at any appropriate time, for example monthly. The dynamic keys 219 sent to the verification centre 114 are stored in a database (for example at central server 117) at or accessible from the verification centre 114. The dynamic key 219 for each batch is preferably stored together with the batch information sent to the verification centre 114 at the same time.

Preferably, the active static key 209 is deleted when the code generator 111 at a particular production centre 103, 105, 107 is put out of service. This prevents a malicious user from gaining access to the active static key 209 without proper registration. Additional means for disabling the code generator 111 and preventing unauthorized use of the code generator 111 and production centre may be provided.

Figure 4 illustrates the steps carried out by the verification centre 114 and by the user 601 when a user 601 wishes to authenticate an individual manufactured item marked in accordance with the process of Figure 3. The user 601 reads the code 221 on the item and sends it to the verification centre 114. This is shown in Figure 1. The user 601 may send the code to the verification centre 114 by any suitable means such as a secure or non-secure internet connection.

The verification centre receives the secure identifier in step 321. The secure identifier is decrypted using the global key 235 (or the corresponding key in the key pair if asymmetric keys are used) in step 323 to reveal the physical noise value 227 and the first identifier 241. The CGID is also revealed. Using a look-up table, the CGOK 231 is then obtained from the CGID. The first ID is then decrypted in step 325 using the CGOK 231 to reveal the system noise 225 and the UPI 221. With this information, together with the active static key 209 and dynamic key 219 and a new physical key, both the physical noise value and the system noise value can be recreated to authenticate the item.

To recreate the physical noise value a new physical key must be obtained by the user 601 in step 327 by recording an image of the portion of the item in the same manner and under the same conditions as used to generate the original physical key 207. The UPI and new physical key are then hashed to generate a new physical noise value in step 329. In step 331, the new physical noise is compared with the extracted physical noise value revealed in step 323. If the new physical noise value is sufficiently similar to the extracted physical noise value then one part of the authentication process is completed. If the new physical noise value is not sufficiently

similar to the extracted physical noise value then the item is determined to be not authentic in step 339.

The new physical noise value may be required to be identical to the extracted physical noise value in order for the item to be considered authentic. However, it is possible to allow for some differences between the new physical noise value and the extracted physical noise value by using a correlation score and requiring a threshold correlation score in order to consider the item authentic. US2005/0257064 describes a suitable statistical method to calculate a degree of correlation or similarity between two digital signatures derived from measured physical properties of a fibrous medium.

It is possible for either the user 601 or the verification centre 114 to carry out step 329 and 331. If the user 601 is provided with the UPI by the verification centre, the end user can authenticate the item based on the physical noise value. Similarly, if the new physical key is provided to the verification centre 114, the verification centre can authenticate the item based on the physical noise value.

To recreate the system noise value, the secret key must be regenerated, In step 333, using the UPI and the CGID, the verification centre 114 is able to retrieve the dynamic key 219 and the active static key 209 from records held at the verification centre. The secret key can then be regenerated using the UPI 221, the dynamic key 219 and the active static key 209. In step 335 a new system noise value is recreated by hashing the UPI and the secret key. In step 337 the new system noise value is compared to the system noise value extracted in step 325. If the new system noise value and the extracted system nose value are identical the item can be determined to be authentic in step 339.

In one embodiment, both the physical noise value and the system noise value comparisons are required in order for an item to be considered authentic. However, it is possible to allow authentication on the basis of only one of these checks if desired.

From the derived active static key 209, the production centre 103, 105, 107 at which the item was manufactured can be determined, since the active static keys are preferably stored in the verification centre together with details of their associated production centres. From the derived dynamic key 219, the batch information for the item can be determined since the dynamic keys are preferably stored in the verification centre together with the associated batch information. Thus, the verification centre 114 can derive, from the code 221 sent from user 601, various pieces of information 603 about the individual item as well as checking the authenticity of the item. Then all, or selected portions of, the information 603 including an indication of whether or not the item is authentic can be sent to the user 601. This is shown in Figure 1. The information 603 is preferably sent to the user 601 via the same means as the original code was sent.

Figure 5 illustrates a marking process in accordance with a second embodiment of the invention. In the method of Figure 5 two secure identifiers are produced, one based on the

system noise value 225 and another based on the physical noise value 227. The system noise value 225 is combined with the UPI 221 in step 341. The combination of the system noise value and the physical noise value is then encrypted with the CGOK 231 in step 343 to produce the first ID 241 as in the first embodiment of Figure 3. The first ID 241 is then combined with the CGID in step 345 and encrypted with the global key 235 in step 347 to produce a first secure ID 271. The Physical noise value 227 is combined with the UPI in step 221 to produce a second ID 261. The second ID is encrypted with the global key 235 in step 353 to produce a second secure ID. The item can then be marked in step 355 with the first secure ID 271 and the second secure ID 281, or with a mark or marks derived from a combination of the first secure ID 271 and the second secure ID 281.

Figure 6 illustrates the steps carried out to authenticate an item marked using the process illustrated in Figure 5. In step 401 the mark or marks are read by the user and the user derives the first secure identifier 271 and second secure identifier 281. In step 403, the global key 235 is used to derive the physical noise value 227, a first copy of the UPI 221, the first ID 241 and CGID 233. If the user has the global key 235, the user can authenticate the item based on the second secure identifier offline, i.e. without requiring connection to the verification centre. The user generates a new physical key in step 407 and this is hashed with the UPI to generate a new physical noise value in step 409. The user can compare the new physical noise value with the physical noise value extracted in step 403 in step 411. As described with reference to Figure 3, the item can be considered authentic in step 419 if the new physical noise value is the same as, or sufficiently similar to, the extracted physical noise value.

In step 405 the CGID is used by the verification centre to retrieve the CGOK 231, and the CGOK is used to decrypt the first ID 241 to reveal the system noise and a second copy of the UPI. In step 408, the second copy of the UPI can optionally be compared to the second copy of the UPI as a check. In step 423, the verification centre 114 retrieves the dynamic key 219 and active static key 209 using the CGID and UPI. In step 415 a new system noise value is generated by first regenerating a secret key from the UPI, dynamic key and static key, and then by hashing the secret key with the UPI. In step 417 the new system noise value is compared to the system noise value extracted in step 405. If they are identical the item can be authenticated in step 419. As with the embodiment of Figure 3, authentication based both on the system noise value and the physical noise value may be required for an item to be considered authentic.

Although the invention has been described with reference to cigarette manufacture, it should be clear that the invention is applicable to any products that require authentication, such as pharmaceutical, alcoholic beverages and luxury goods.

CLAIMS

1. A method of marking a manufactured item, comprising:

creating a unique product identifier for a manufactured item;

creating one or more encryption keys;

generating a secret key using the unique product identifier and the one or more encryption keys;

generating a physical key from a measured physical property of the manufactured item;

generating a secure identifier derived from or incorporating the secret key and the physical key; and

placing a mark on the manufactured item, the mark comprising the secure identifier or an identifier derived from the secure identifier.

2. A method according to claim 1, further comprising generating a system noise value using the secret key and the unique product identifier, wherein the secure identifier is derived from or incorporates the system noise value.

3. A method according to claim 1 or 2, further comprising generating a physical noise value using the physical key and the unique product identifier, wherein the secure identifier is derived from or incorporates the system noise value.

4. A method according to any preceding claim, wherein the secure identifier incorporates the unique product identifier.

5. A method according to claim 4 when dependent on claims 2 and 3, wherein the step of generating the secure identifier comprises generating a first identifier by encrypting the unique product identifier together with the system noise value and generating the secure identifier by encrypting the first identifier together with the physical noise value.

6. A method according to claim 5, further comprising authenticating the manufactured item at a verification centre, the step of authenticating comprising:

identifying the mark on the item;

decrypting the mark to derive the first identifier and the physical noise value;

decrypting the first identifier to derive the unique product identifier and the system noise value;

generating a new physical key from a measured physical property of the manufactured item;

generating a new copy of the physical noise value by performing a hash function on the new physical key and the derived unique product identifier;

comparing the new copy of the physical noise value with the derived physical noise value; and

providing at indication of whether the derived physical noise value is identical to or correlates to the new copy of the physical noise value.

7. A method according to claim 6, the step of authenticating further comprising:

generating a new copy of the secret key from the unique product identifier and the one or more encryption keys;

generating a new copy of the system noise value by performing a hash function on the new copy of the secret key and the unique product identifier;

comparing the new copy of the system noise value with the derived system noise value; and

providing an indication of whether the new copy of the system noise value and the derived system noise value are identical.

8. A method according to claim 4 when dependent on claim 2 and 3, wherein the step of generating the secure identifier comprises generating a first secure identifier by encrypting the unique product identifier together with the system noise value;

generating a second secure identifier by encrypting the unique product identifier together with the physical noise value; and

placing a mark on the manufactured item, the mark comprising the first and second secure identifiers or an identifier or identifiers derived from the first and second secure identifiers.

9. A method according to claim 8, further comprising authenticating the manufactured item at a verification centre, the step of authenticating comprising:

identifying the mark on the item;

decrypting the mark to derive the unique product identifier, the system noise and the physical noise;

generating a new copy of the secret key from the unique product identifier and the one or more encryption keys;

generating a new copy of the system noise value by performing a hash function on the new copy of the secret key and the unique product identifier;

comparing the new copy of the system noise value with the derived system noise value;

generating a new physical key from a measured physical property of the manufactured item;

generating a new copy of the physical noise value by performing a hash function on the new physical key and the derived unique product identifier;

comparing the new copy of the physical noise value with the derived physical noise value; and

providing an indication of whether both the new copy of the system noise value is identical to the derived system noise value and the new copy of the physical noise value is identical to or correlates to the derived physical noise value.

10. A method according to any preceding claim, wherein the one or more encryption keys comprise a static key and a dynamic key, and wherein a new dynamic key is created for each batch of manufactured items.

11. A method according to any preceding claim wherein the unique product identifier includes information identifying a batch of items to which the item belongs.

12. An apparatus for marking a manufactured item, comprising:

a key generator configured to generate encryption keys;

a code generator configured to generate a unique product identifier for each manufactured item;

a physical key generator configured to generate physical keys from a measured physical property of each manufactured item;

processing means configured to:

generate a secret key for each manufactured item using the unique product identifier and one or more encryption keys;

generate a secure identifier derived from or incorporating the secret key and the physical key; and

a marker for marking each manufactured item with the secure identifier or an identifier derived from the secure identifier.

13. An apparatus according to claim 12, wherein the processor is configured to generate a system noise value for each manufactured item by performing a hash function on the secret key and a unique product identifier, wherein the secure identifier is derived from or incorporates the system noise value.

14. An apparatus according to claim 12 or 13, wherein the processor is configured to generate a physical noise value for each manufactured item by performing a hash function on the physical key and the unique product identifier, wherein the secure identifier is derived from or incorporates the physical noise value.

15. An apparatus according to any one of claims 12 to 14, wherein the manufactured item is a container containing a tobacco product.

Fig. 1

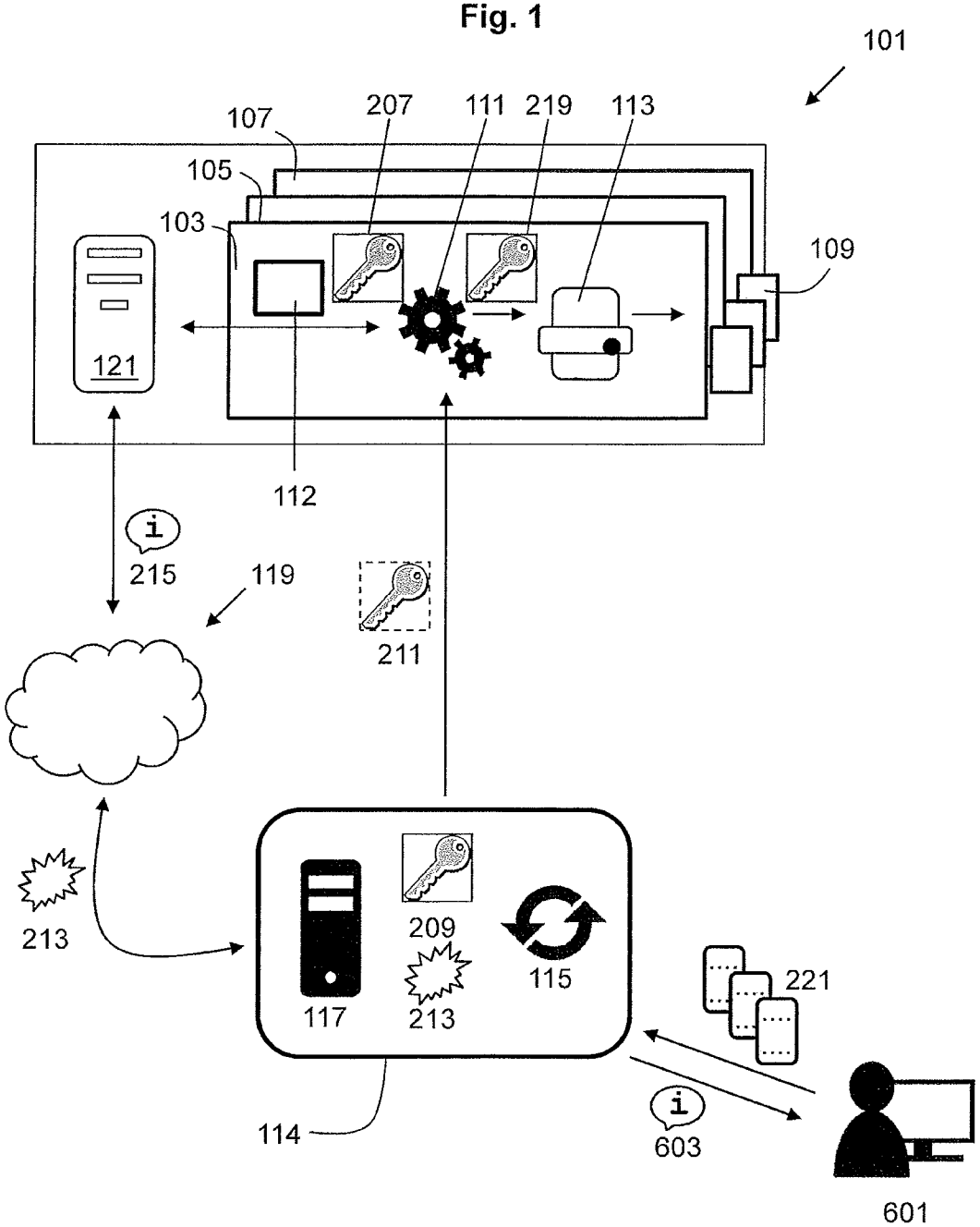
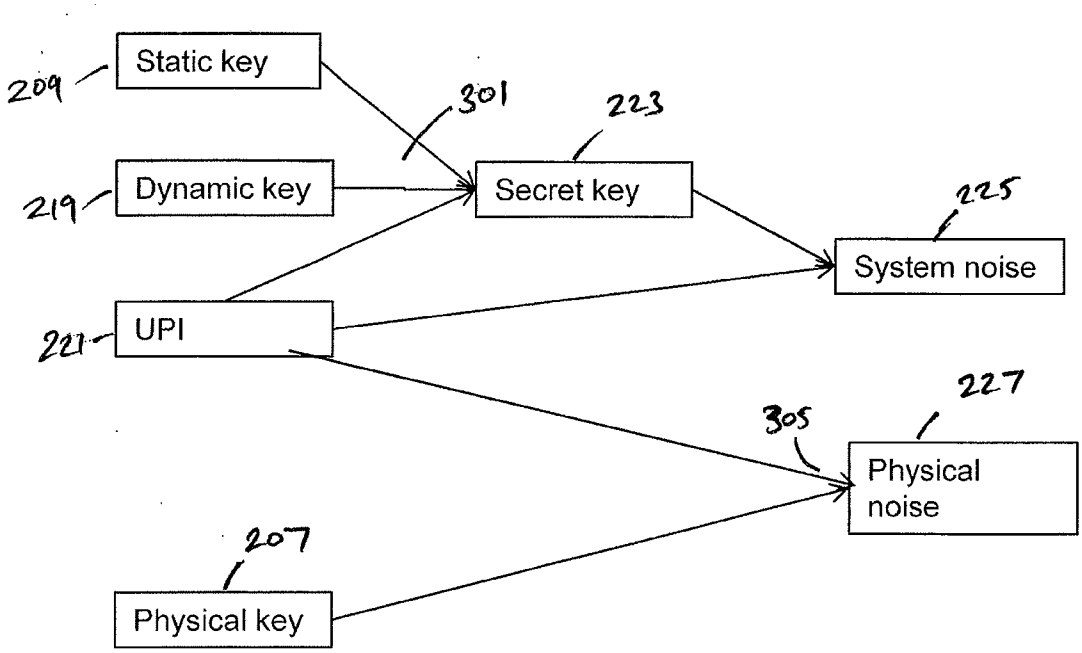

101
107
207
111
219
113
105
103
109
121
112
215
119
211
213
209
213
115
117
221
114
603
601

Fig. 2


209
Static key
301
223
219
Dynamic key
Secret key
225
System noise
221
UPI
227
305
Physical noise
207
Physical key

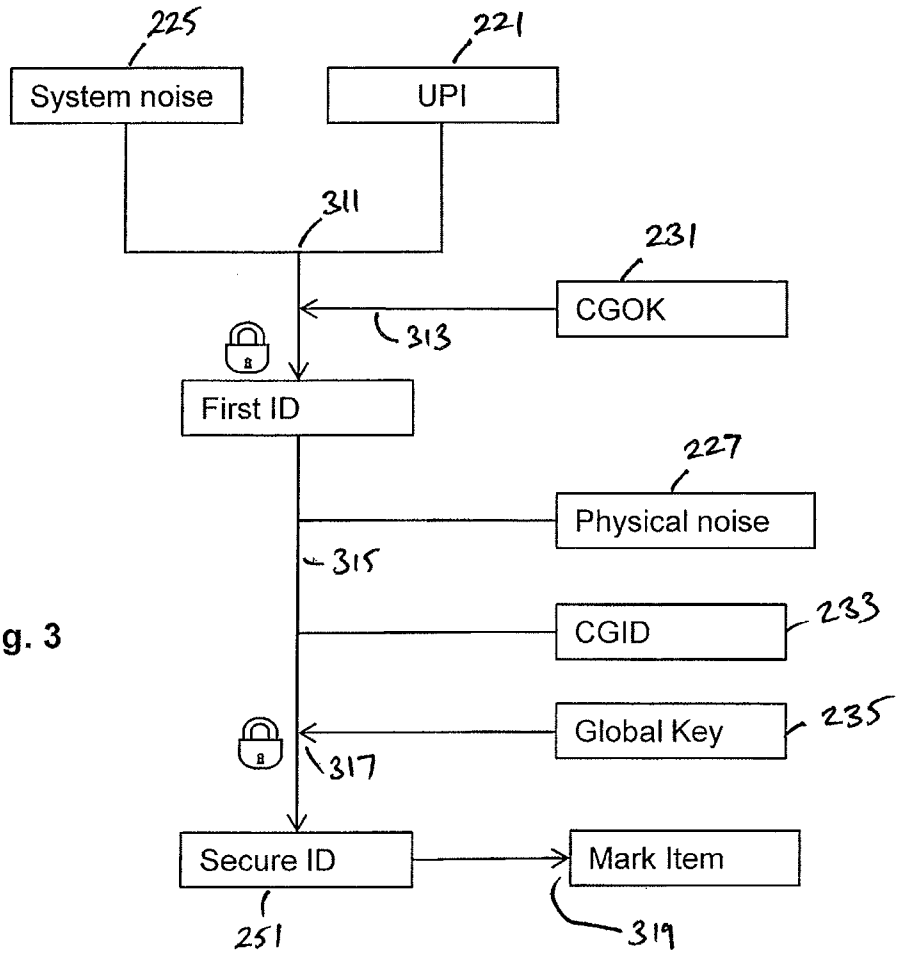

225
System noise
221
UPI
311
231
CGOK
313
First ID
227
Physical noise
315
CGID
233
Global Key
235
317
Secure ID
Mark Item
251
319

Fig. 3

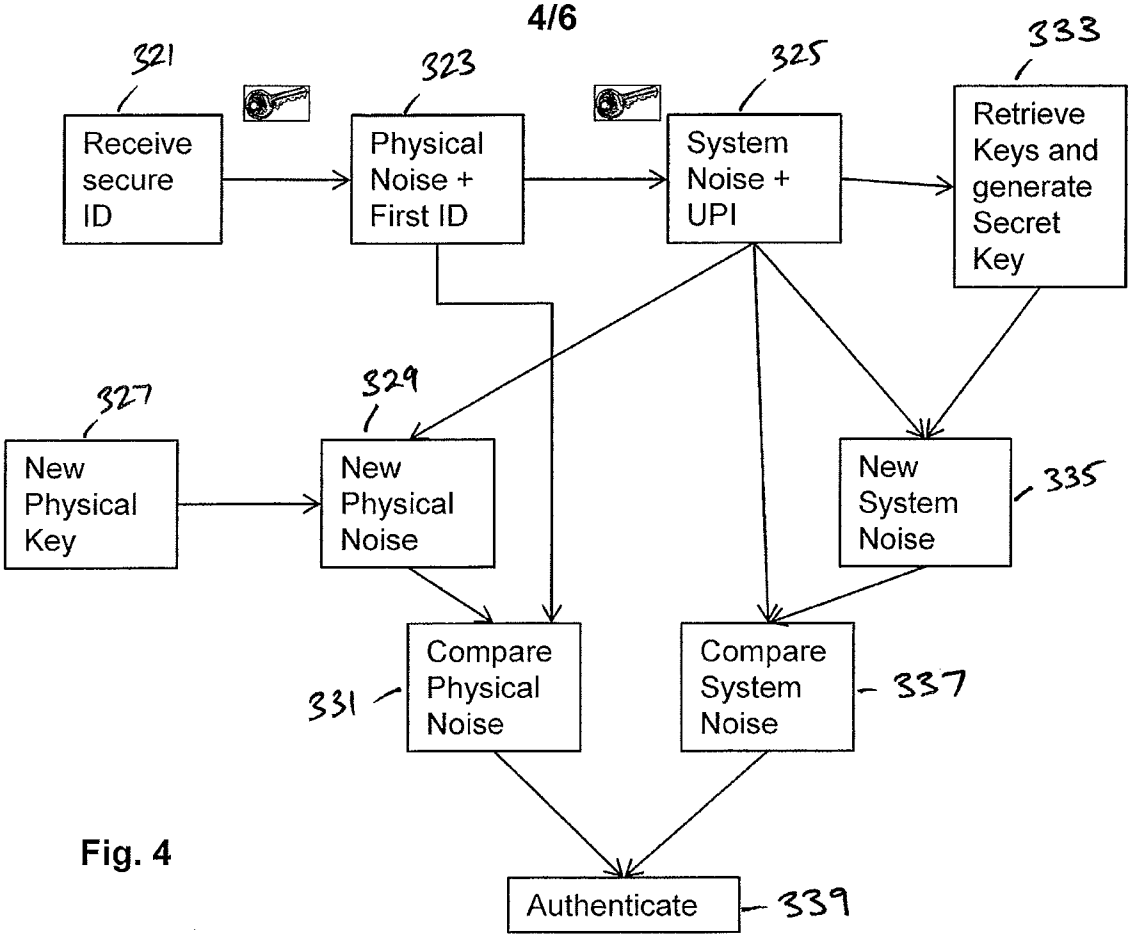

321
Receive secure ID
323
Physical Noise + First ID
325
System Noise + UPI
333
Retrieve Keys and generate Secret Key
327
New Physical Key
329
New Physical Noise
New System Noise
335
331
Compare Physical Noise
Compare System Noise
337
Authenticate
339

Fig. 4

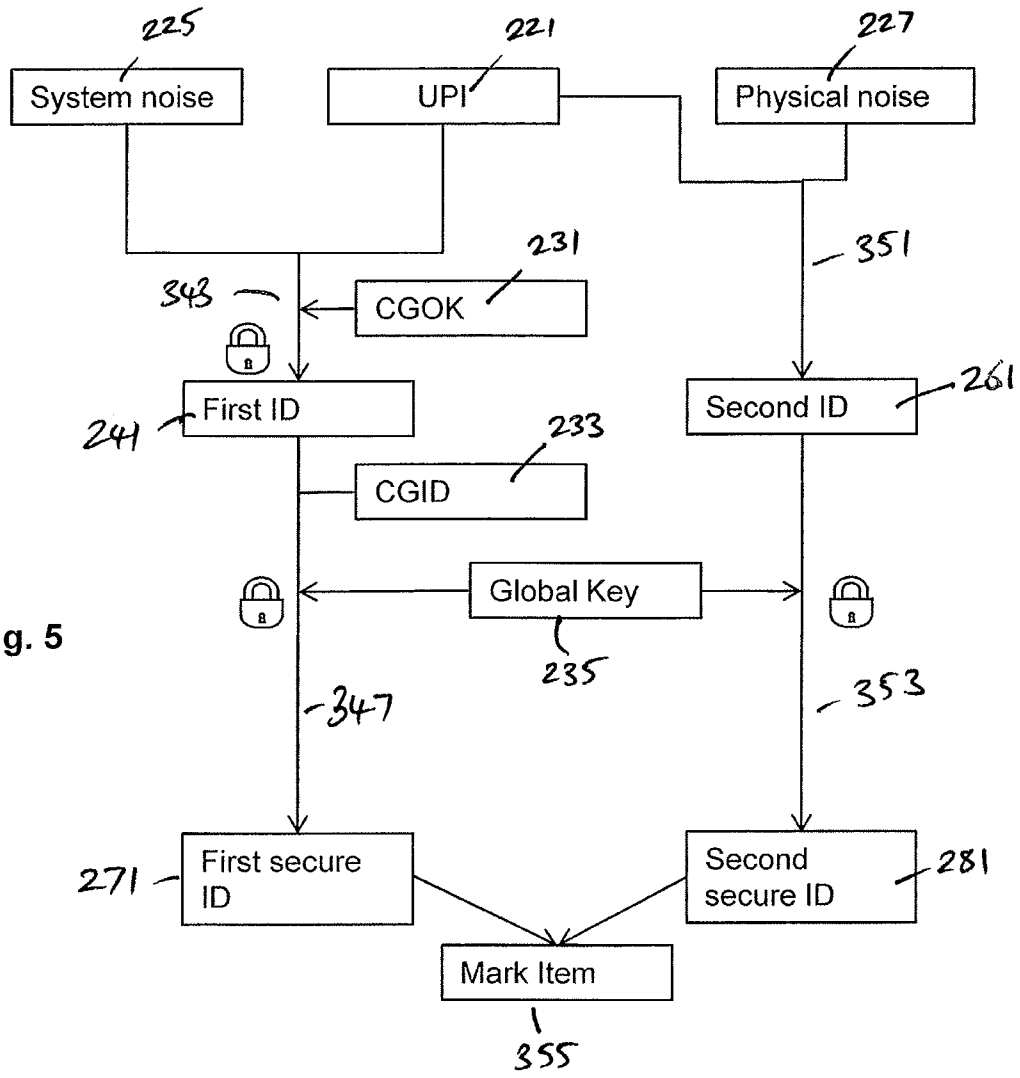

225
System noise
221
UPI
227
Physical noise
231
CGOK
343
351
First ID
241
Second ID
261
233
CGID
Global Key
235
347
353
First secure ID
271
Second secure ID
281
Mark Item
355

Fig. 5

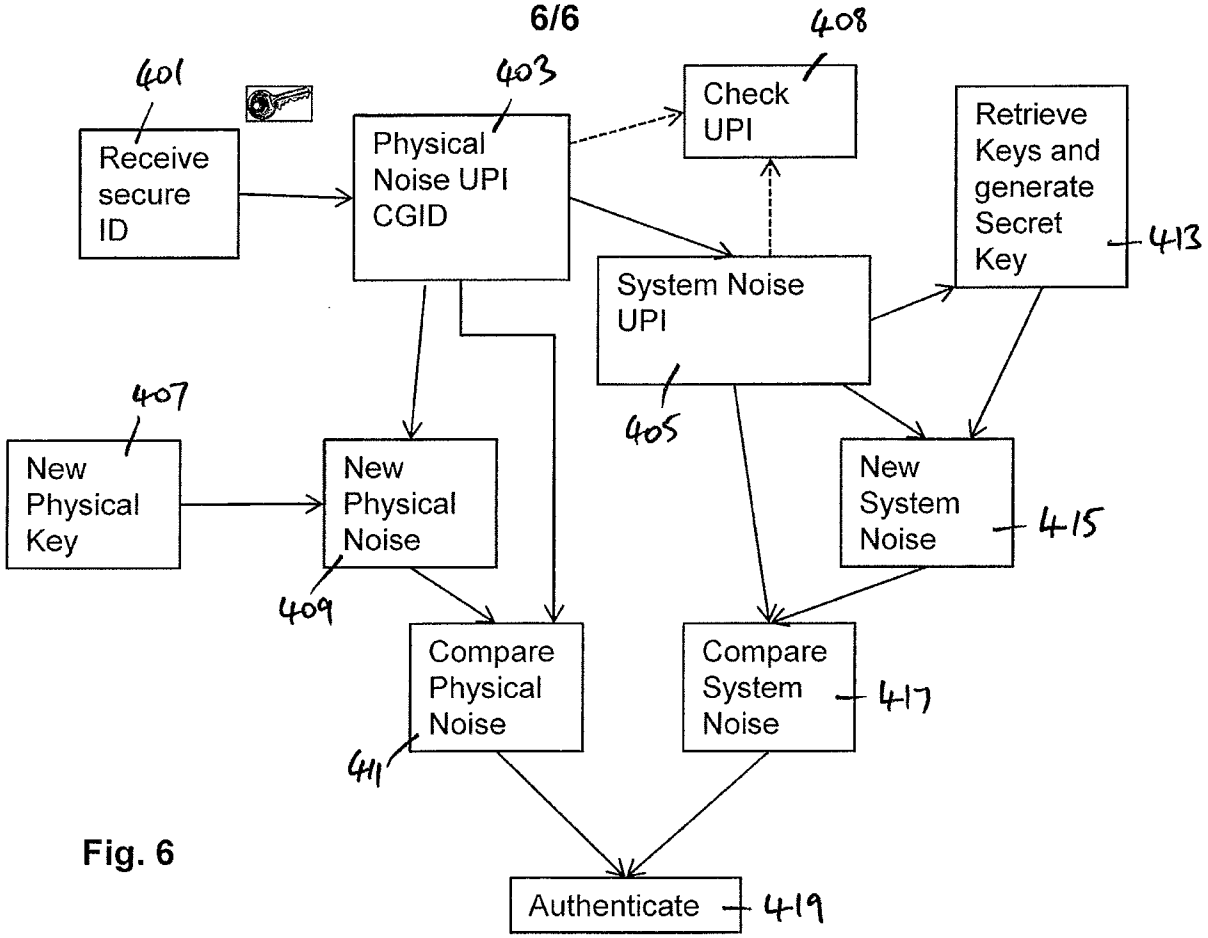

401
Receive secure ID
403
Physical Noise UPI CGID
408
Check UPI
Retrieve Keys and generate Secret Key
413
System Noise UPI
405
407
New Physical Key
New Physical Noise
409
New System Noise
415
Compare Physical Noise
411
Compare System Noise
417
Authenticate
419

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/076725

A. CLASSIFICATION OF SUBJECT MATTER
INV. G09C5/00 H04L9/00
ADD.

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)
G09C H04L

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/43086 A1 (MISCHENKO VALENTIN ALEXANDROVI [BY]; HRISHANOVICH IGOR A [BY]; MISCHEN) 14 June 2001 (2001-06-14) abstract page 4, line 1 - page 5, line 12 page 7, line 5 - page 8, line 8 -----	1-15
A	WO 97/24699 A1 (S E AXIS LIMITED [GB]; KARIAKIN YOURY D [BY]) 10 July 1997 (1997-07-10) abstract page 2, line 34 - page 6, line 12 -----	1-15
A	US 6 212 638 B1 (LEE GEORGE C [US] ET AL) 3 April 2001 (2001-04-03) abstract column 1, line 39 - column 3, line 11 ----- -/--	1-15

[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
12 February 2014	20/02/2014

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	Di Felice, M

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/076725

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LEHTONEN MIKKO ET AL: "Features, Identity, Tracing and Cryptography in Product Authentication", THE 13TH INTERNATIONAL CONFERENCE ON CONCURRENT ENTERPRISING: CONCURRENT INNOVATION: AN EMERGING PARADIGM FOR COLLABORATION & COMPETITIVENESS IN THE EXTENDED ENTERPRISE, CENTRE FOR CONCURRENT ENTERPRI , 4 June 2007 (2007-06-04), pages 1-8, XP002560506, Retrieved from the Internet: URL:http://www.stop-project.eu/Portals/1/publications/ICE07_SToP_ProdAuth.pdf [retrieved on 2009-12-15] the whole document -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/076725

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0143086 A1	14-06-2001	AT 241834 T	15-06-2003
		AU 2087200 A	18-06-2001
		DE 69908425 D1	03-07-2003
		DE 69908425 T2	06-05-2004
		EP 1153373 A1	14-11-2001
		US 6928552 B1	09-08-2005
		WO 0143086 A1	14-06-2001
WO 9724699 A1	10-07-1997	AU 4311896 A	28-07-1997
		WO 9724699 A1	10-07-1997
US 6212638 B1	03-04-2001	NONE	