Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2581358 A1 2006/04/13

(21) 2 581 358

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2005/09/29
(87) Date publication PCT/PCT Publication Date: 2006/04/13
(85) Entrée phase nationale/National Entry: 2007/03/21
(86) N° demande PCT/PCT Application No.: IB 2005/003103
(87) N° publication PCT/PCT Publication No.: 2006/038114
(30) Priorité/Priority: 2004/10/08 (EPEP04104954.5)

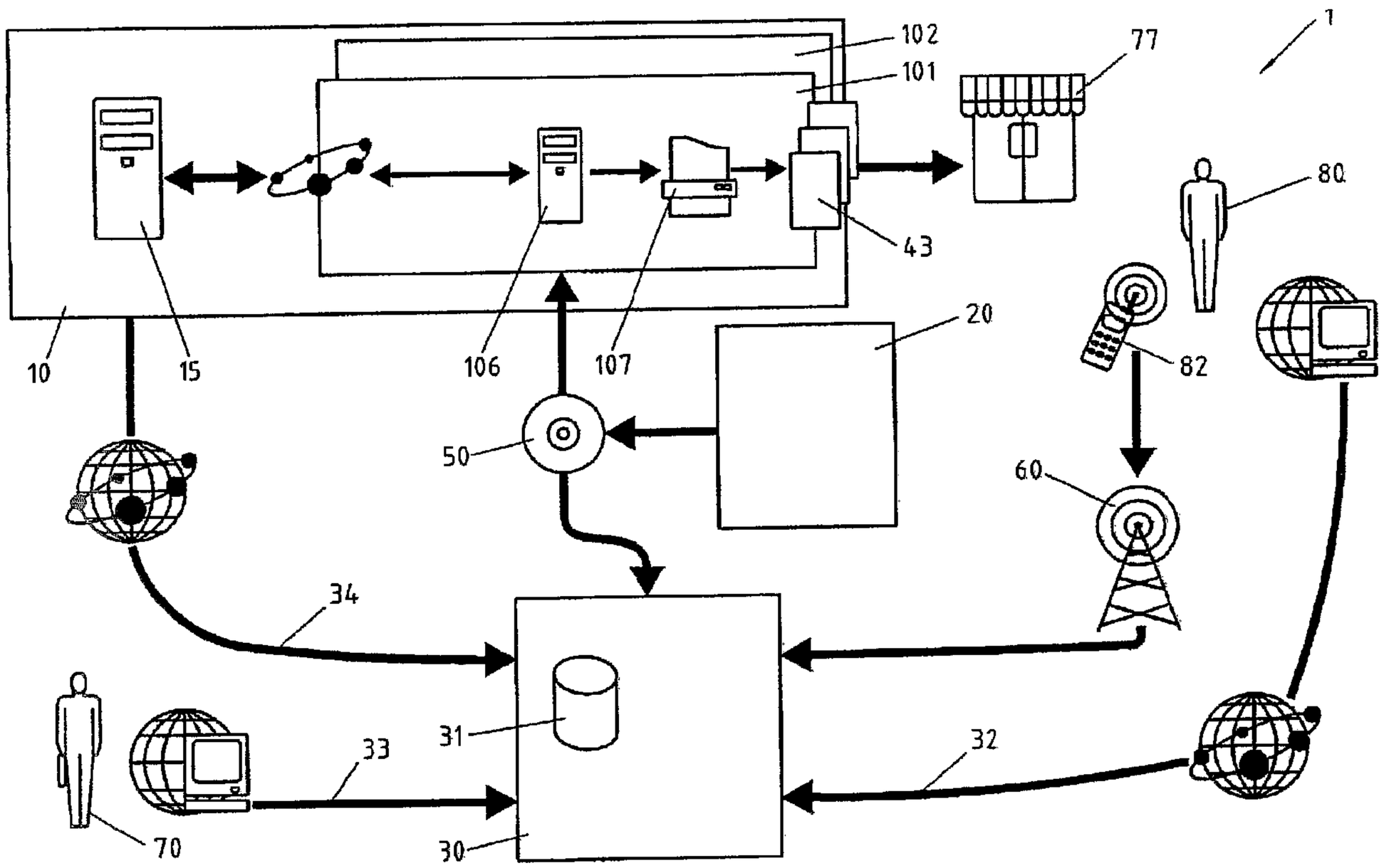
(51) Cl.Int./Int.Cl. *G06K 17/00* (2006.01)

(71) Demandeur/Applicant:
PHILIP MORRIS PRODUCTS S.A., CH

(72) Inventeurs/Inventors:
SAGER, ALAIN, CH;
CHATELAIN, PHILIPPE, CH;
FRADET, ERWAN, CH;
WEISS, JACQUES, CH;
CHEMLA, MARC, CH

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : PROCEDES ET SYSTEMES DE PRODUCTION, DE SUIVI ET D'AUTHENTIFICATION DE PRODUITS
(54) Title: METHODS AND SYSTEMS FOR MAKING, TRACKING AND AUTHENTICATION OF PRODUCTS



(57) Abrégé/Abstract:
Manufactured goods are marked or labeled with a secure unique identifier. A central checking centre allows users to verify the authenticity of a particular good such as a cigarette pack or carton via any convenient interface such as the Internet or a cell phone. A system of secret sharing allows secure authentication of each item and prevents code breaking or misuse.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2006 (13.04.2006)

PCT

(10) International Publication Number
WO 2006/038114 A1

(51) International Patent Classification:
G06K 17/00 (2006.01)

(21) International Application Number:
PCT/IB2005/003103

(22) International Filing Date:
29 September 2005 (29.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
EP04104954.5 8 October 2004 (08.10.2004) EP

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

(72) Inventors: **SAGER, Alain**; Route de Reynet 4, 1615 Bossonnens (CH). **CHATELAIN, Philippe**; Chemin de Chaudremont 12a, 1373 Chavornay (CH). **FRADET, Erwan**; Rue de Maupas 19c, 1004 Lausanne (CH).

(74) Agent: **LLOYD, Patrick, Alexander, Desmond**; Reddie & Grose, 16 Theobalds Road, London WC1X 8PL (GB).

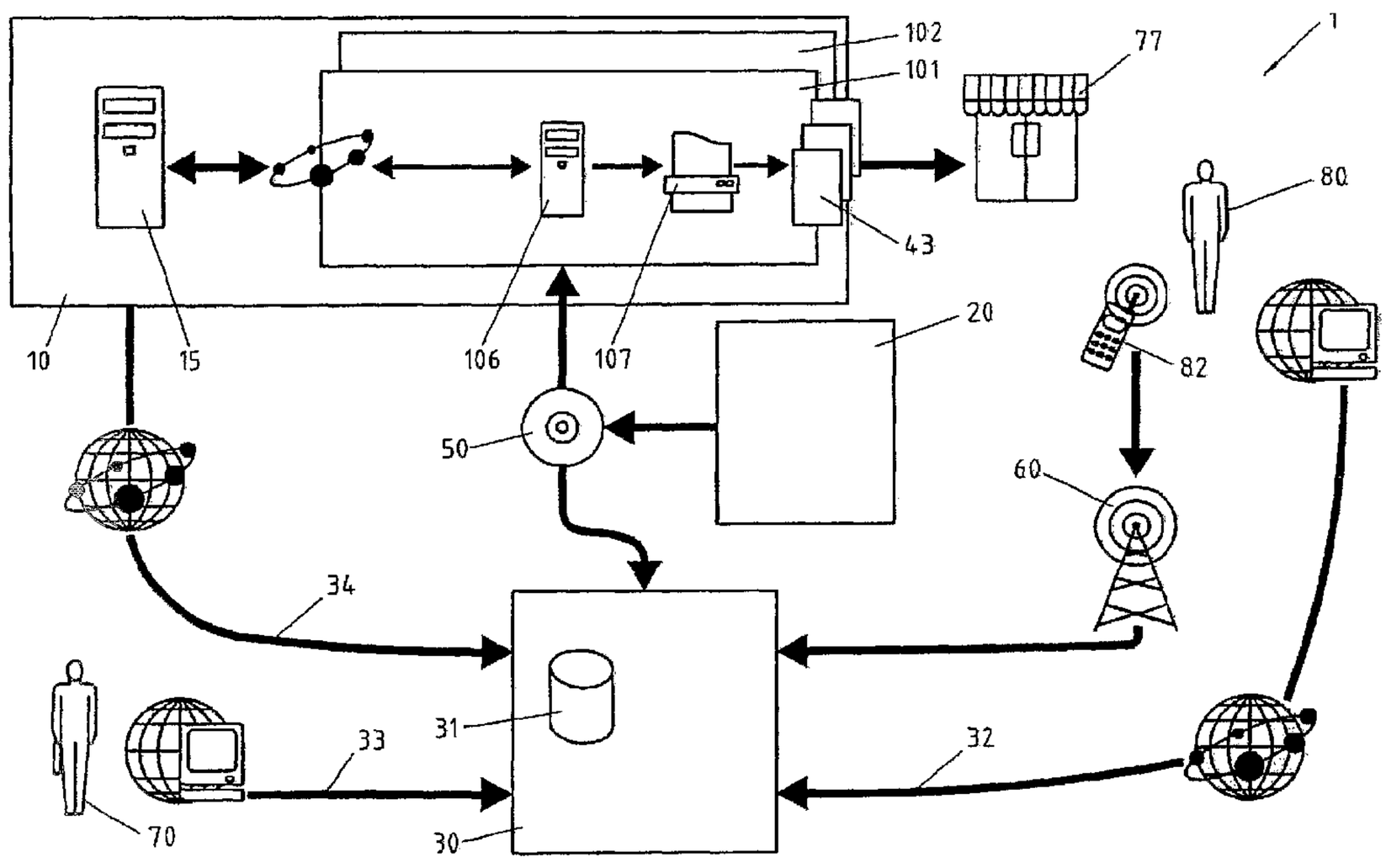
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHODS AND SYSTEMS FOR MAKING, TRACKING AND AUTHENTICATION OF PRODUCTS



(57) Abstract: Manufactured goods are marked or labeled with a secure unique identifier. A central checking centre allows users to verify the authenticity of a particular good such as a cigarette pack or carton via any convenient interface such as the Internet or a cell phone. A system of secret sharing allows secure authentication of each item and prevents code breaking or misuse.

WO 2006/038114 A1

Methods and Systems for Marking, Tracking and Authentication of Products

Field of the invention

This invention relates to the marking, tracking and authentication of goods, in particular, but not exclusively, of packaged goods, for example packs or cartons of cigarettes and other tobacco products. The invention also relates to production control.

Background to the Invention

Contraband and counterfeiting cause significant loss of revenue to producers of traded goods as well as for national authorities. Moreover, the illegal sale of counterfeited goods of inferior quality is detrimental to the customer and to the manufacturer.

Legally produced goods may also be illegally imported or traded, for example in order to evade taxes or national regulations. It is therefore a major concern in several trade areas to detect and avoid unauthorized parallel import channels.

The problems of contraband and counterfeiting are particularly acute for goods subject to special taxation, like tobacco products. They also exist for many other kinds of traded products carrying a strong brand value, in particular for internationally traded products, such as perfumes, alcohols, watches and luxury goods in general.

It is a major concern of the manufacturers of such products to develop methods for reliably marking genuine products such as to enable the unequivocal identification of non-genuine products and the detection of illegal imports.

It is common practice to identify traded goods by a production code, or serial number, impressed or printed on the package, for example a cigarette pack or carton. Such a code, under certain conditions, enables identification of the production site, and the tracking of the trade chain for a particular item. Such knowledge is useful in identifying smuggled items.

A limitation of this practice is that the interpretation and validation of these production codes can be time-consuming and cumbersome. For example, authentication may require every production code impressed on a manufactured item to be recorded in a database and/or the transfer of a large amount of confidential data from the manufacturing site to a central database. These requirements may jeopardize reliability and safety.

Another limitation of this practice is that the production codes can easily be imitated or cloned. To partially obviate this limitation, it is known to add a covert taggant to the ink used to print the production code on the package. Counterfeit items carrying clones of valid codes can be thus detected by the absence of the covert taggant. The security provided by this method depends entirely on the ability to control the sources and the availability of the taggant.

The present invention aims to address the deficiencies in the prior art approaches described above.

According to the invention, there is provided a method of marking manufactured items, comprising: providing a plurality of secret codes to a checking centre and to a production line for the manufactured items; generating an ID code for each manufactured item;

digitally signing each ID code by means of a secret derived from the plurality of secret codes and known to the checking centre; and marking each manufactured item with said signed ID code.

The present invention also provides a method of authenticating an item marked according to the method above comprising transmitting the said signed ID code to said checking centre; and authenticatiing the ID code at the checking centre.

The invention also provides a system for marking manufactured items comprising: a generator, for generating collections of secret codes; a production line for manufacturing the items to be marked, the production line comprising: a code generator for generating an ID code for each manufactured item; a digital signor for signing the ID codes with a secret derived from the secret codes; a data transmitter for transmitting the secret to a checking centre; and a marker for marking each manufactured item with the signed ID code.

The invention also provides a method of authenticating a manufactured item, comprising: generating a code and signing said code with a digital signature within a code generator; marking the item with the signed code; transmitting the signed code to a checking centre over a public network; authenticating the digital signature by the checking centre; retrieving the significance of the code at the checking centre; and transmitting the significance to a user over the public network.

A further aspect of the invention resides in a method of controlling the volume of manufactured items marked the marking method above, comprising: gathering manufacturing volume information at the checking centre; and providing the manufacturing volume information to a user..

The invention also provides a method of tracking an item marked by to the marking method above, comprising: transmitting the signed ID code to the checking centre; authenticating the ID code by the checking centre; and retransmitting the tracking information related to the ID code to a user.

Embodiments of the various aspects of the invention have the advantage that marking and authentication can be accessed and interrogated remotely by an ordinary network, such as a land or mobile telephone. The marking and authentication has the further advantage that it may not be violated by counterfeiters. Moreover, the genuineness of a manufactured item on sale can be checked easily, for example within a few seconds at the point of sale.

Embodiments of aspects of the invention have the further advantage that cloned codes and unauthorized code duplications may be identified, and that the production volume, for example of a given manufacturer, manufacturing site or manufacturing line, may be controlled.

Embodiments of aspects of the invention have the further advantage that they may be used to replace the system of fiscal stickers that is used in many countries to collect taxes, for example on tobacco products.

Brief Description of the Drawings

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

Figure 1 is a schematic view of a marking and authentication system embodying the invention;

Figure 2 shows schematically a marking code format embodying the invention;

Figure 3 is a flow chart showing a code generation scheme embodying the invention;

Figure 4 is a flow chart showing a code authentication scheme embodying the invention.

Detailed Description of the Invention

Referring to figure 1, the items to be marked are produced on one or more production lines 101, 102. Each production line represents a production facility for one or more manufactured items. For example, a production line may be a cigarette making and packaging line, with the manufactured items being, for example, cigarette packs and cartons of at least one brand. The production may be organized in batches, each batch being dedicated to the production of a certain amount of identical manufactured items, for example cigarette packs and cartons of a particular brand and type.

If there are two or more production lines, these lines may be physically located at one manufacturing site 10, or at different production centres 10 having various geographical locations.

Each production line comprises a code generator 106 arranged to generate and encrypt an identification code for each item manufactured on the production line 101. The production line 101 also comprises a marker 107.

Any suitable marking means may be used such as a continuous inkjet printer, a drop-on-demand inkjet printer, a laser printer, or any other printer or marker that allows the marking of variable information, to impress or print the identification code on each manufactured item. Depending on the nature of the packaging, the identification codes can be impressed on each item, on an external package, on labels or in any other convenient way. In one embodiment, the identification code is printed on adhesive tags, or labels, to be applied to the manufactured items, preferably non-removably.

In one embodiment the identification code is printed by a laser beam on a layer of laser-sensitive material deposited on the item or on the item's package. This method allows the code to be impressed through a transparent wrapping layer.

Other possible supports for the identification code include holographic printing, for example using the HoloSpot® format.

Embodiments of the invention may also include radio, electronic or magnetic recording of the identification code, for example using an RFID transponder, EMID® tags or any other tagging means.

Preferably the system has means to count and report the number of codes generated and printed codes in each production batch or in a given production period, as will now be described in detail. The production lines 101 include a code generation system 106 which generates a unique encrypted identification code SUPI for each item produced. Preferably, the code generation system 106 is a fully autonomous computer or microcontroller dedicated to a particular production line 101. Preferably the code

generation system 106 can communicate with a checking centre 30 via a secure internet connection 34, a local central server 15, or any other suitable data communication means.

The checking centre 30 receives and centralizes production data and processes queries from users 80, 70.

In one embodiment of the invention, several levels of packaging, such as packs and cartons comprising several packs, which are manufactured on the same manufacturing line 101, may be marked using common hardware resources.

In one embodiment the code generation system 106 may comprise different or shared software modules, loaded on a computer common to several production lines, and serve several production lines at the same time. The code generation system 106 may be remotely located, for example in the checking centre, and communicate the generated codes to the production lines, as required, by appropriate network means. The code generation system performs a number of funtions, as described below, including the generation of ID codes for the items and the signing of those ID codes.

In the embodiment of figure 2, the unique identification code SUPI is obtained by processing data in a Production Information Code PIC. The PIC combines various data related to the manufacture of the item, such as a code MC identifying a manufacturing centre 10, a code PL identifying a particular production line 101 within a manufacturing centre 10, and codes YR, DY, HR identifying the year, day and hour, respectively, when a particular item was manufactured. In one alternative embodiment, the PIC may include a code generator ID

instead of the manufacturing centre and production line codes MC, PL.

To obtain the PIC, the individual data elements can be combined by decimal or binary digit juxtaposition, by algebraic composition, by applying a predefined shift value each data element and adding all the shifted values together, or by any other computational means. Preferably the composition function is invertible, to allow decomposition of the PIC into the original elements MC, PL, YR, DY, HR. In the case of a non-reversible composition fuction, an additional element may be introduced into the PIC to ensure uniqueness.

During each production hour, a production line fabricates a large number of items 43. Each item 43 is identified, within a production hour, by an individual number TI, for example a progressive number corresponding to the chronological production sequence. Other manners of generating or assigning individual numbers are possible.

The production information code PIC and the individual number TI are combined to provide an item identifier UPI. In the following description, each UPI is unique to an item, for example to a single cigarette pack or cigarette carton. However the invention is not limited to this case, and includes variants with non-unique UPI numbers, distinguishable from each other by their different digital signatures.

The structure of the UPI code and the significance of the various fields composing the UPI code are exemplary and are not limiting. Any code suitable as item identifier code, having any arbitrary structure and significance, may be employed in the frame of the present invention.

A pseudorandom noise value code is combined with the UPI to authenticate the code generator 106 that produces the code. The noise value acts as a digital signature for the code marked on each manufactured item produced by a particular manufacturing line 101 applied by the code generator 106 which can be verified by the checking centre 30. To ensure verifiability by the checking centre, the pseudorandom noise code may obtained by encrypting a copy of the UPI code with a secret shared by the code generator and the checking centre. 'Secret' designates any data used for generation or authentication of a digital signature. Other ways of adding a digital signature to the UPI code are possible, for example by using asymmetric cryptography, and are included within the scope of the invention. The secret is derived from secret codes, which may be regarded as static secret codes.

In one embodiment of figure 1, a centralized salt generator centre 20 generates alarge collection of secret codes, hereinafter designated as a 'salt matrix' containing a large number of precalculated random or pseudorandom data. Each salt matrix is preferably unique and is transmitted, in duplicate, to the intended manufacturing line 101 and to the checking centre 30. Each manufacturing line 101 receives a unique salt matrix. The salt matrices transmitted to the checking centre are stored in a database 31 accessible to the checking centre 30 and preferably included in the checking centre 30, with identification of the production lines 101, 102 to which they belong.

In the production lines, 101, 102, the salt matrices are used to generate secret keys used to encrypt

the UPI and to generate an electronic signature, as it will be explained later.

To ensure authenticity, confidentiality and integrity of the salt matrix, the matrix is preferably not transferred over a network connection, but rather recorded on non-volatile data carriers 50 such as CD-ROMs (Compact Disc Read-Only Memory), DVD-ROMs (Digital Versatile Disc Read-Only Memory), removable hard disks, magneto-optical devices or any suitable non-volatile memory device. The data carriers are physically transferred to the checking centre 30 and to the production lines 101, 102.

Preferably, to further increase safety, the salt matrices are encrypted and digitally signed by the salt generator 20, using a suitable encryption and authentication technique, such as DES (Digital Encryption Standard), RSA (Rivest, Shamir, and Adelman algorithm), and the like. The salt matrices are not sent to the checking centre as part of the checking process for items as will be discussed.

Preferably, a salt file contains the following components:

(i) A unique salt file identifier.(ii) The salt matrix encrypted using a strong cipher, such as triple-DES, or AES (Advanced Encryption Standard), according to a key generated in the salt generator 20. A salt matrix may be, for example, a long string of random or pseudorandom digits or characters.

(iii) The encrypted key needed to decode the salt matrix, encrypted with a public-key cipher, for example RSA, using a public key of the checking centre 30. This component is

requested in the salt file sent to the checking centre 30 and may be omitted in the file destined to the production line 101.

(iv) A digital signature of the salt generator, obtained for example by encoding a digest of the full message with a salt generator private key, whose public counterpart is known to the checking centre.

In this embodiment, the code generator of every production line 101 must register with the checking centre 30. This registration occurs only whenever a new salt matrix is used, or at prescribed intervals. The system does not require constant communication between the code generators and the checking centre.

The registration procedure comprises the following steps:

(i) The code generator 106 of the production line 101 connects to the checking centre 30 via a secure internet connection, or via a local central server connected to the internet, and initiates the registration by identifying itself.

(ii) A CD-ROM 50, containing a salt file, is loaded into the code generator, its integrity is verified by its electronic signature, and its unique identifier is transmitted to the checking centre 30.

(iii) The checking centre retrieves its own copy of the salt file, locally or remotely stored, by means of the unique identifier.

(iv) If the salt file has been already used, the checking centre stops the registration and requests another salt file,

or initiates appropriate action, for example issuing a warning to the user or logging it in a security journal.

(v) If the salt file has not yet been used, and the identification of the code generator is satisfactory, the checking centre decrypts the secret key of the salt file with its private key, and transmits it to the code generator over the secure internet connection 34. In the case where the salt file is not unique this step takes place regardless of whether or not the salt file has alerady been used.

(vi) The code generator decrypts the salt matrix.

The registration procedure is arranged such that the salt matrix is never transferred over the internet. Only a one-use decryption key is transmitted from the checking centre 30 to the code generator 106. The salt matrix is made available to the code generator only after a valid registration with the checking centre. This prevents unauthorized use of the code generator as no valid code can be generated.

Preferably the decrypted salt matrix is deleted when the code generator is put out of service to prevent a malicious user from gaining access to the salt matrix without proper registration. Additional means for disabling the code generator and preventing unauthorized use of the code generator and the production line may be provided. The operation of the code generator 106 will now be described with reference to figure 3.

At each production line 101, 102 at the beginning of each production batch, the code generator 106

generates a random salt index alpha, which it transmits to the checking centre 30, with various information related to the item to be manufactured such as, for example, brand, intended market of destination, packaging. A new salt index alpha is generated at every change of production batch. Preferably the checking centre acknowledges successful receipt of the index alpha to the code generator. The index alpha may be regarded as a dynamic secret code.

In an embodiment the UPI code of the first item to be produced in the batch is transmitted with the index alpha to the checking centre 30. The salt index alpha is stored in database 31 related to various information about the item to be manufactured. This enables the checking centre 30, upon receipt of a request to check a particular SUPI code, to retrieve the particular alpha and knowing the salt matrix used by the code generator 106 to sign that SUPI code, validate the signature.

The salt index alpha does not need to be communicated in real time to the checking centre 30, at the beginning of each production batch. Once a value of alpha has been chosen, the code generator can immediately start to generate valid codes and the value of alpha can be communicated after a delay of some hours, or more depending on the availability of the network connection.

Backup procedures such as telephone or fax may be used to communicate the alpha to the checking centre, in case the network connection is unavailable. The random salt index alpha, the salt matrix and the UPI code are used by the code generator for generating a noise code (step 301) which is safe from cryptographic attacks.It does not allow the reconstruction of the original values of alpha, salts matrix and UPI. A variety of known

techniques are available for generating the noise code including, but not limited to, table substitution, indexing, hashing , and variations thereof. The noise code so generated is unequivocally calculated from the UPI, yet the inverse operation is computationally impossible.

The noise code is used as a digital signature, allowing validation of the UPI code. Preferably the alpha code and the salt matrix are combined in a different way for each manufactured item, in order to render the digital signatures robust against decryption attempts.

The salt matrix and the alpha code are known only by the code generator and by the checking centre. Together they constitute a secret allowing the code generator to generate signed codes which the checking centre can subsequently verify.

The UPI number and the calculated noise code are combined at step 302 and, preferably, the resulting code is obfuscated step 303, destroying correlations between successive codes. The obfuscation operation is reversible, allowing the checking centre to retrieve the original UPI and noise value. Several known obfuscation techniques are possible. The particular obfuscation algorithm chosen is preferably not published.

The result of the obfuscation, is the unique SUPI code, which is printed on the manufactured items by the printer 107. Each of the items 43 is marked with a unique digitally signed SUPI code, allowing identification of the production batch in which it has been manufactured.

Preferably, data relating to the production batch, e.g. product type, brand, intended market of destination, packaging is stored in the database 31 with the index alpha at the start of the batch. This data is

accessible to the checking centre. The SUPI code can be printed on the manufactured item by a variety of printing and marking techniques, for example continuous inkjet printing, drop-on-demand printing, laser, etc. The SUPI code may be printed in a human readable format, or a machine-readable formats such as 1-D or 2-D barcodes or characters suitable for OCR (Optical Character Recognition).

Preferably the SUPI code is printed or recorded by a printing or recording means comprising a device such as a code counter or a register, for counting the exact number of marked items, either during a production batch or in a given time interval. The exact number of marked items may be stored in the database 31 accessible to the checking centre and used for production volume control.

In one preferred embodiment, the SUPI code is printed with an ink containing a covert taggant, to allow a quick validity check without querying the checking centre.

The production line 101 may have a sensor to detect the presence of the SUPI (either using a vision system and/or by detecting the covert taggant, if applicable). The sensor can be connected to the controller of the production line, thus enabling the rejection of items not properly marked. The controller can be set to prevent the production line from operating if the sensor unit is disconnected, faulty or on rejection of a defined number of items. A history of rejections may be logged in the Code Generator and communicated to the Checker for monitoring purposes by authorized users. The production information code (PIC code) may be repeated on the manufactured item, in plain format without encryption or obfuscation, allowing the

user to verify the answer provided by the checking centre 30 and useful for management and monitoring of the supply chain.

After leaving the production centre 10, the manufactured items 43 are distributed and commercialized in the usual way. At each stage of the distribution and commercialization process, the authenticity of the item can be verified by sending a query containing the SUPI code of the package to the checking centre. Such verification may be requested for example by generic users, such as retailers, consumers, or customs agents, and by privileged users, for example employees of the manufacturers, or organizations having a privileged agreement with the manufacturer. The SUPI codes may also be employed for tracking the manufacturing items along the distribution and commercialization chain.

Figure 4 shows the processing of a request to validate a SUPI code in the checking centre. The received SUPI code is first de-obfuscated at step 402, by applying the inverse of the obfuscation function described above. At step 402 the original UPI and noise component are extracted. The checking centre performs a first level authentication at step 404 on the manufacturing centre MC and the production line PL. If PL is found to correspond to an existing production line of manufacturing centre MC, the authentication proceeds to the next level, otherwise a response is generated at 420 that the SUPI code is invalid, and the item is counterfeit. In the second level of authentication, the checking centre 30 uses the secret salt matrix received by the salt generator 20 and the alpha code transmitted at the beginning of a production batch. At 410 the checking centre retrieves the information related to the

production batch corresponding to the received UPI code from the database 31. If the retrieval is successful, the retrieved salt matrix and the alpha code are used at 411 to reconstruct the noise code from the received UPI code and to verify the validity of the signature. If the received noise and the reconstructed noise do not match, or if no data corresponding to the PIC is present in the database, the SUPI code is identified as invalid and the checking centre responds at 420 that the item is counterfeit.

In a third level of authentication at step 412, the checking centre verifies whether queries for the same SUPI code have been submitted more than a predefined number of times. In this case, there is then a suspicion that the SUPI code may be a clone of a valid code, identically printed on a large number of counterfeits. The checking centre then issues a reply at step 430 specifying, that the submitted code is valid, but the item is likely to be counterfeit.

The discovery of cloned codes can be refined by making use of other information, for example the origin of the query, which can be determined if the query originated from a phone, or the elapsed time between queries.

Here, 'cloning' means multiple copying of a valid production code, for example for tagging counterfeited articles. If the code has been found valid (step 440), the checking centre retrieves the significance of the code and transmits it to the user, preferably in natural language, for example: "your code corresponds to a pack of brand XYZ, intended market of retail Switzerland", or another appropriate formulation.

The information returned by the checking centre may allow the tracking of the production information for each item, for example information about the production unit, the production line, the date and time of production. Such information can be returned in encoded form, or in natural language.

Optionally the checking centre can formulate the significance of the codes into several languages, and choose the most appropriate language for the reply, according to the origin or language of the query. In a preferred embodiment, the public interface to the checking centre includes a SMS (Short Message Service) or USSD (Unstructured Supplementary Services Data) portal of a public radio communication network, for example a telephone network supporting text or numeric messages like GSM, TDMA, CDMA, PDC, or UMTS standard networks, through which the users 80 can send queries to the checking centre 30 in form of text messages, or SMS, from their own cell phone 82, and receive the reply from the checking centre in the same way or by another channel, for example by a voice call. In this way the user 80 can verify an item 43 directly at the point of sale 77.

The communication may alternatively or additionally be over the internet 32 by a web server at the checking centre 30, by an email server or a WAP (Wireless Application Protocol) server.

Alternatively or additionally, the communication may be to a telephone voice server, able to interpret voice commands or DTMF (Dual-Tone Multi-Frequency) signals generated by a telephone keyboard.

Embodiments of the present invention allow a generic unidentified user to authenticate a manufactured item over a public network, such as the internet 32, a

telephone network or a mobile telephone network. The user need not identify himself, nor has he to have access to any secret code or sensitive information. However, each item can be identified in a cryptographically safe way.

In a preferred embodiment, a privileged user 70, for example an employee of the manufacturer, may have a preferred access to the checking centre 30 and retrieve additional privileged information, unavailable to generic users, for example production volume information, or statistical information on the access to the checking centre. In this case, a privileged user may query information on a particular SUPI without marking it as cloned for successive queries from ordinary customers 80.

The privileged user may communicate with the checking centre 30 by a public network, or an intranet connection 33.

In a further embodiment the checking centre may provide, to generic or privileged users, additional information to which it has access, which are not contained in the UPI code, for example expiry date, warranty information, address of local support, or previous trade steps, importation routes and so forth.

Additionally the checking centre may gather and store information on production volumes, for example the number of items produced in each production batch by each production line, as well as statistical production data per brand and per intended market. Such production volume information may be used for production management, or for official purpose, and may be available to selected users.

Identification steps may be provided to identifying known privileged users, for example by passwords, cookies, voice or biometric data, or by any suitable identification means. The checker may include,

or have access to, a user rights database for storing the profiles of various users, and determining to which information each user has access.

It will be appreciated that embodiments of the present invention do not require a permanent connection between the manufacturing lines and the checking centre, nor that all the SUPIs be individually stored in a database. In fact, no identification code is stored. The digital signature ensures that each item can be verified with a minimal transfer of confidential data, providing a high level of reliability and safety. Moreover production volume can be exactly accounted for. As no identification code is stored at the checking centre, the database required by the cheking centre is relatively small compared to that which would be needed if the codes were stored.

In some situations, particularly if the manufactured goods are subject to special tax regulations, official government bodies may submit requests to the checking centre to obtain the appropriate production data, for example production volumes. In such cases, the checking centre 30 may be maintained by a trusted third party independent from the producer of the manufactured items 43. The embodiments described may be used to replace the system of fiscal stickers that is used in many countries to collect taxes, for example on tobacco products.

Claims

1. A method of marking manufactured items, comprising:

providing a plurality of secret codes to a checking centre and to a production line for the manufactured items;

generating an ID code for each manufactured item;

digitally signing each ID code by means of a secret derived from the plurality of secret codes and known to the checking centre; and

marking each manufactured item with said signed ID code.

2. A method of claim 1, comprising using a covert taggant or a laser device in the marking step.

3. A method according to claim 1 or 2, wherein said plurality of secret codes are precalculated random codes.

4. A method according to of any of claims 1 to 3, providing the plurality of secret codes includes physical transfer of a non-volatile data support, on which the secret codes are recorded.

5. A method according to any of claims 1 to 4, wherein said secret derived from said plurality of secret codes is derived at each of a plurality of production lines.

6. A method according to any preceding claim, wherein part of said secret is transmitted by a code

generator to the checking centre via a secure network connection.

7. A method according to any preceding claim, wherein the plurality of secret codes is a collection of random codes, and comprising:

generating an index relating to the manufacture of one or more items;

transmitting the index to the checking centre;

deriving the secret by a code generator, from the collection of random codes and from the index; and

digitally signing each ID code for each manufactured item with a noise code derived by encrypting a copy of the ID code with the secret.

8. A method according to claim 7, wherein the secret is further derived from the ID code.

9. A method according to any of claims 1 to 8, comprising transmitting additional information concerning the manufactured items to the checking centre.

10. A method according to any preceding claim, wherein said checking centre is managed by a trusted third party, independent from the manufacturer of the manufactured item.

11. A method according to any preceding claim, wherein said marking is performed on packaging of said manufacturing article.

12. A method according to any preceding claim, wherein the ID code comprises at least one of:

a production site identifier;
a production line identifier;
a code generator identifier;
a product identifier; and
time information.

13. A method according to any preceding claim, comprising encrypting the ID code.

14. A method of any of the preceding claims, wherein said item is a cigarette pack or a cigarette carton.

15. A manufactured item marked by the method according to any preceding claim.

16. A method of authenticating an item marked according to the method of any of claims 1 to 14 comprising:
transmitting the signed ID code to the checking centre; and
authenticating the signed ID code at the checking centre.

17. A method according to claim 16, comprising:
marking on each manufactured item part of the information contained in the ID codefor that item; and
verifying the consistency of information with processed information retransmitted by the checking centre.

18. A method according to claim 16, comprising retransmitting additional information related to the transmitted ID code by the checking centre.

19. A method according to any of claims 16-18 comprising detecting cloned 10 codes at the checking centre.

20. A checking centre for authenticating an item by the method of claims 16, 17 or 18.

21. A system for marking manufactured items comprising :

a generator for generating collections of secret codes;

a production line for manufacturing the items to be marked, the production line comprising:

a code generator for generating an ID code for each manufactured item;

a digital signor, for signing the ID codes with a secret derived from the secret codes;

a data transmitter, for transmitting the secret to a checking centre; and

a marker for marking each manufactured item with the signed ID code.

22. A system according to claim 21, wherein said marker comprises a printer or a laser device.

23. A system according to claim 21 or 22, wherein the production line is arranged for the production of tobacco products.

24. A system according to claim 21, 22 or 23, wherein the generator comprises a data recorder, for recording the collection of secret codes on a non-volatile data support.

25. A system according to any of claims 21-24, wherein the checking centre comprises an interface for accepting text or numeric queries from a network and for transmitting answers via the network.

26. A system according to any of claims 21 to 25, wherein the generator for generating collections of secret codes is a salt generator.

27. A system according to any of claims 21 to 26, wherein the production line 101 comprises a sensor to detect the marked signed ID code.

28. A method of authenticating a manufactured item, comprising:

generating a code and signing said code with a digital signature within a code generator;

marking the item with the signed code;

transmitting the signed code to a checking centre over a public network for authentication;

authenticating the digital signature by the checking centre;

retrieving the significance of the code at the checking centre; and

transmitting the significance to a user over the public network.

29. A method according to claim 28, wherein codes generated by the code generator are not stored.

30. A method according to claim 28 or 29, wherein the code is signed with a secret shared by the code generator and the checking centre.

31. A method according to claims 30, wherein the secret is extracted from a collection of secret codes shared by the code generator and the checking centre and is modified during operation of the code generator.

32. A method according to claim 30 or 31, wherein said secret is different for each manufactured item.

33. A method of controlling the volume of manufactured items marked according to the method of any of claims 1-14, comprising:

gathering manufacturing volume information at the checking centre; and

providing the manufacturing volume information to a user.

34. A method according to claim 33, wherein the manufacturing volume information is obtained from ID codes transmitted to the checking centre.

35. A method of tracking an item marked according to the method of any of claims 1-14 comprising:

transmitting the signed ID code to the checking centre;

authenticating the signed ID code by the checking centre; and

retransmitting the tracking information related to the ID code to a user.

36. A method according to claim 34, wherein the tracking information is obtained from the ID codes of manufactured items transmitted to the checking centre.

37. A method according to any of claims 32-35, comprising identifying the user.

38. A method according to any of claims 33 to 37, comprising a step of denying information to users not belonging to a predefined group of privileged users.

39. A method of authenticating manufactured items, comprising marking the items by:

providing a plurality of secret codes to a checking centre and to a production line for the manufactured items;

generating an ID code for each manufactured item;

digitally signing each ID code by means of a secret derived from the plurality of secret codes and known to the checking centre; and

marking each manufactured item with said signed ID code; and authenticating a manufactured item on request by validating the secret at the checking centre.

40. A system for authenticating manufactured items, comprising: a system for marking manufactured items comprising:

a generator for generating collections of secret codes;

a production line for manufacturing the items to be marked, the production line comprising:

a code generator for generating an ID code for each manufactured item;

a digital signor, for signing the ID codes with a secret derived from the secret codes;

a data transmitter, for transmitting the secret to a checking centre; and

a marker for marking each manufactured item with the signed ID code; the authentication system further comprising a checking centre for authenticating a manufactured item on request by validating the secret.

41.

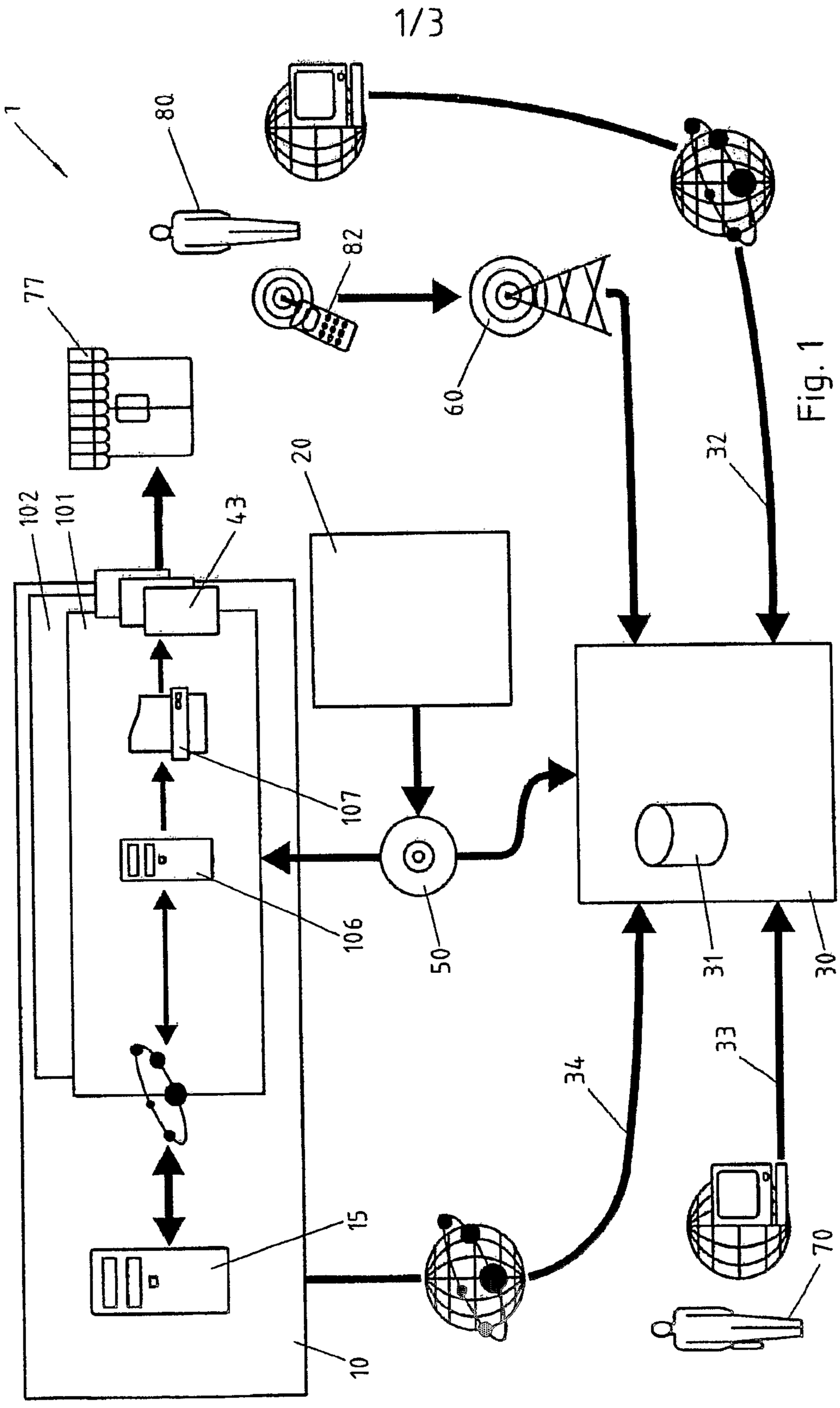


Fig. 1

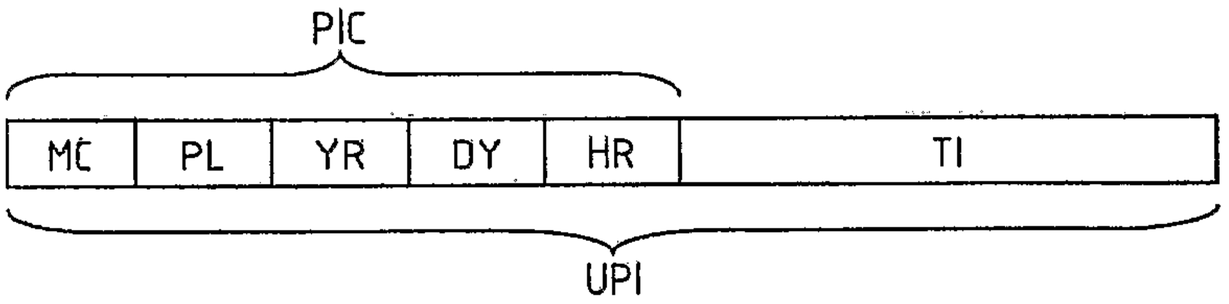

PIC
MC
PL
YR
DY
HR
TI
UPI

Fig. 2

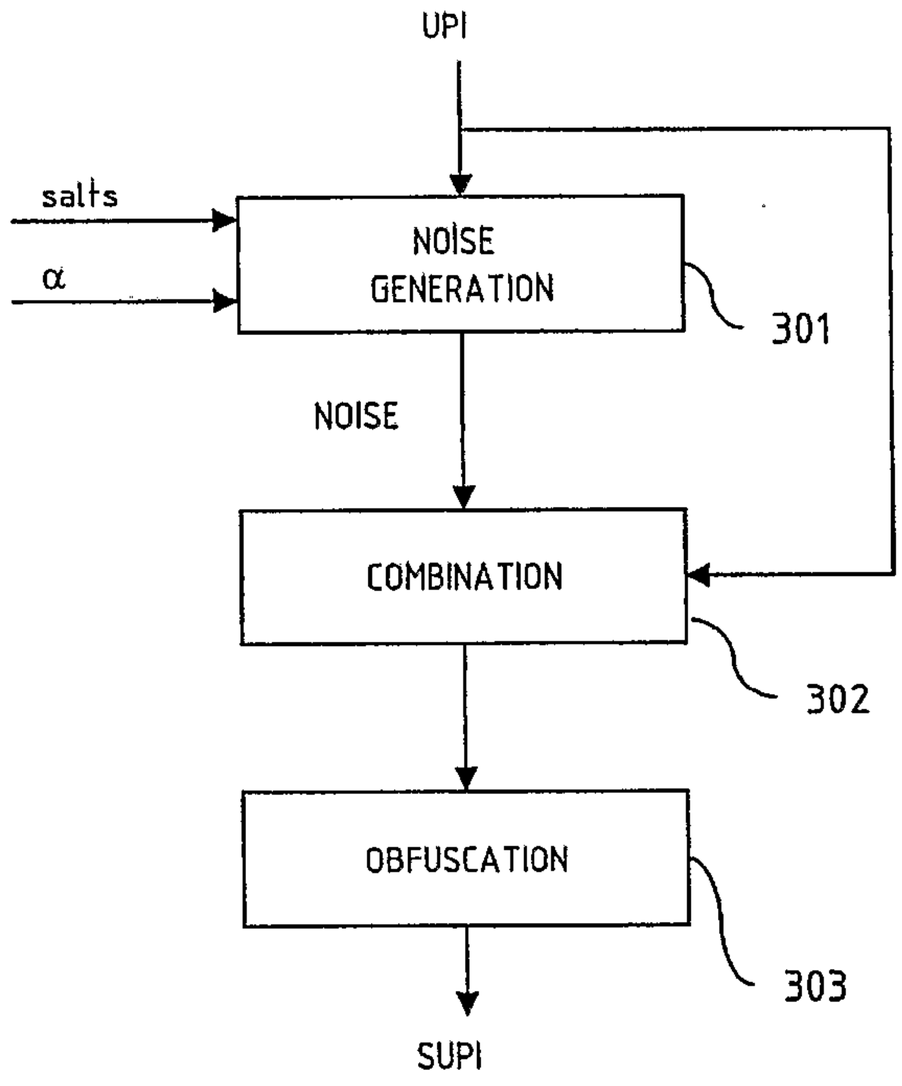

UPI
salts
α
NOISE GENERATION
301
NOISE
COMBINATION
302
OBFUSCATION
303
SUPI

Fig. 3

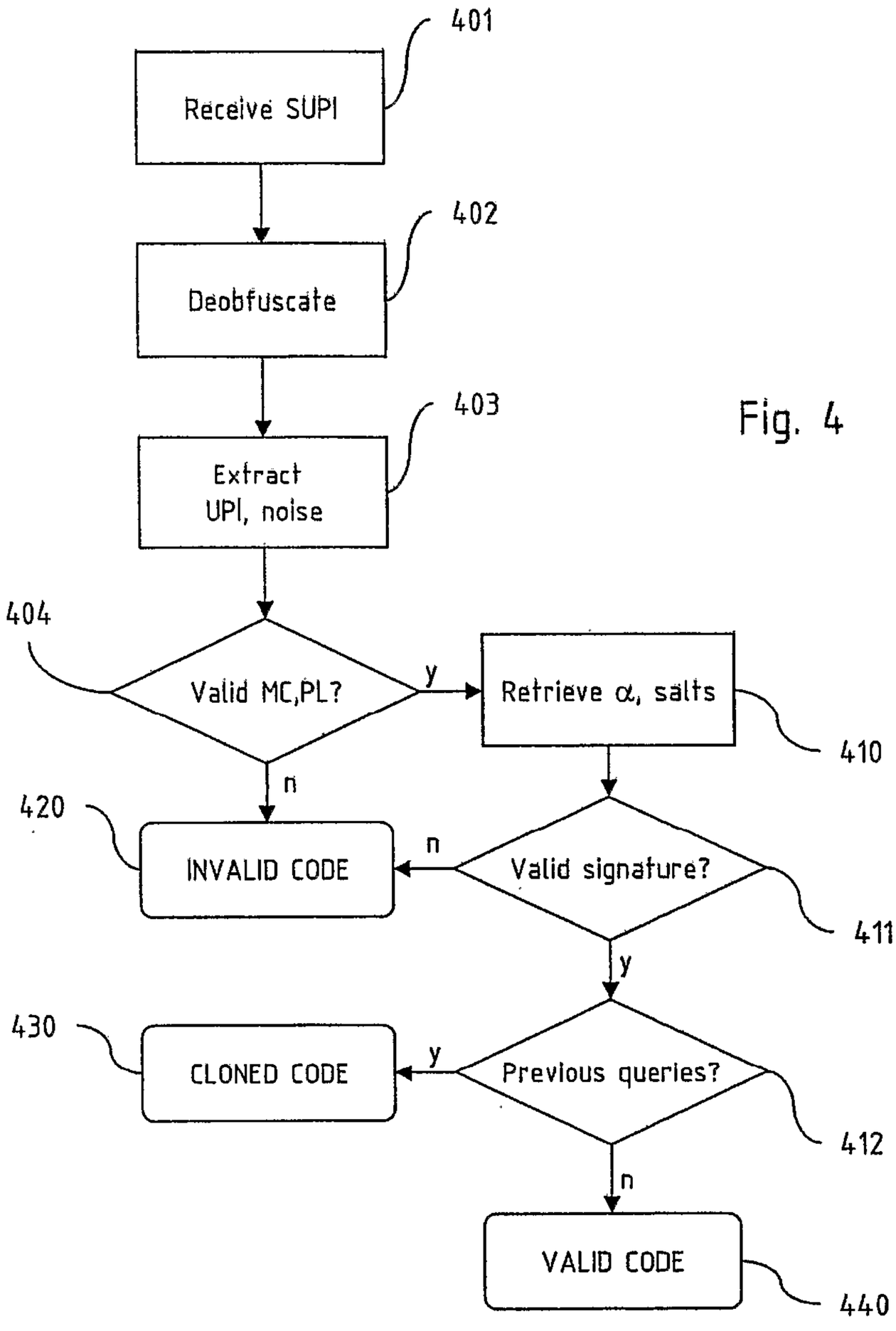
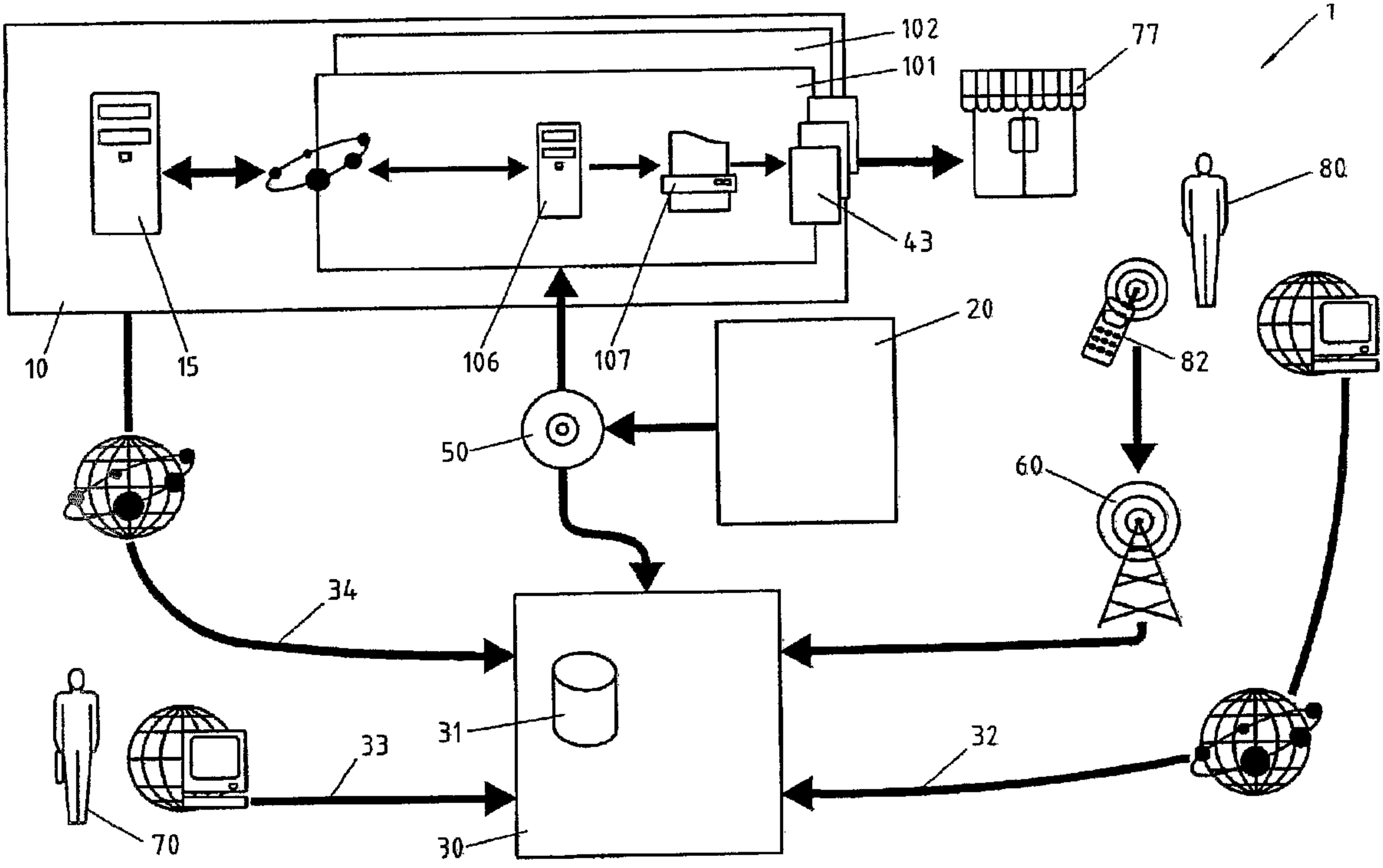

401
Receive SUPI
402
Deobfuscate
403
Extract
UPI, noise
404
Valid MC,PL?
y
Retrieve α, salts
410
n
420
INVALID CODE
n
Valid signature?
411
y
430
CLONED CODE
y
Previous queries?
412
n
VALID CODE
440

Fig. 4


1
102
101
77
80
43
10
15
106
107
20
82
50
60
34
31
33
32
70
30