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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2356314 C 2005/10/11

(11)(21) 2 356 314

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 1999/12/20
(87) Date publication PCT/PCT Publication Date: 2000/07/06
(45) Date de délivrance/Issue Date: 2005/10/11
(85) Entrée phase nationale/National Entry: 2001/06/20
(86) N° demande PCT/PCT Application No.: EP 1999/010141
(87) N° publication PCT/PCT Publication No.: 2000/038932
(30) Priorité/Priority: 1998/12/24 (2557/98) CH

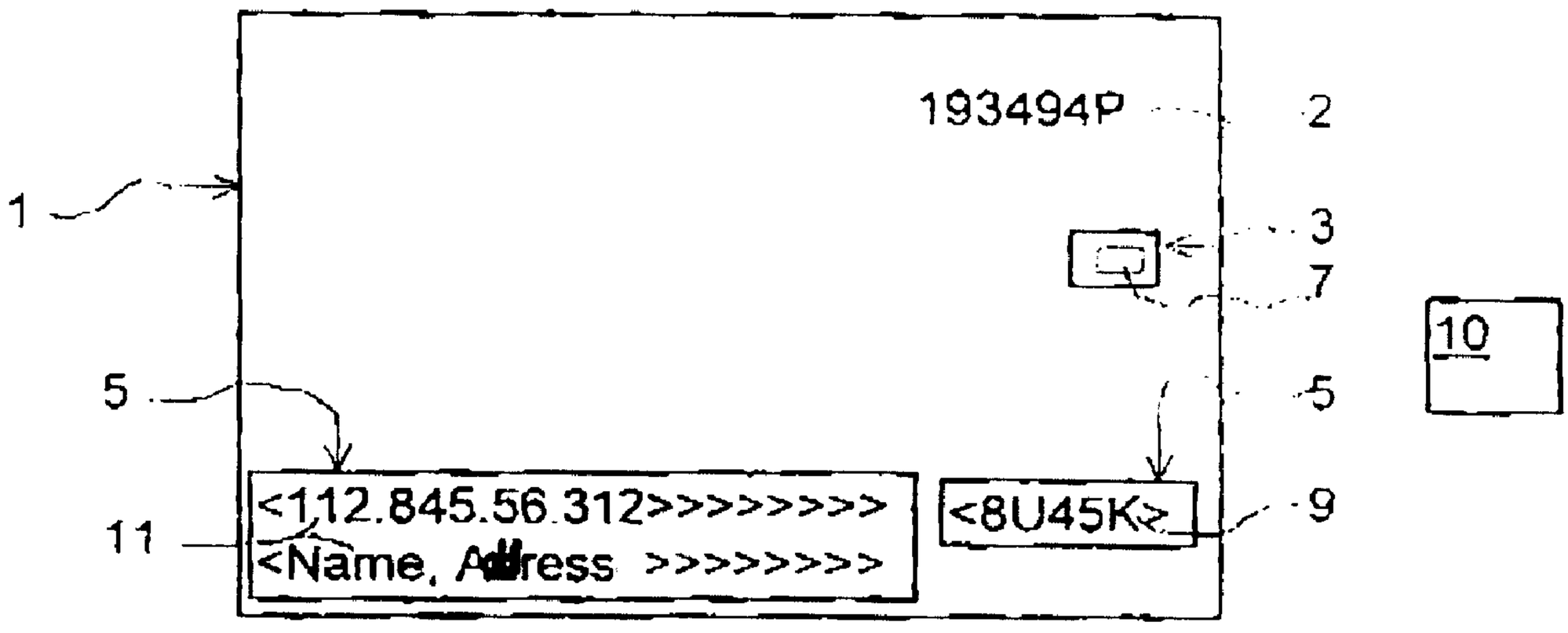
(51) Cl.Int.^{7}/Int.Cl.^{7} G06K 19/10, B42D 15/10, G06K 19/16

(72) Inventeurs/Inventors:
TOMPKIN, WAYNE ROBERT, CH;
STAUB, RENE, CH

(73) Propriétaire/Owner:
OVD KINEGRAM AG, CH

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : DOCUMENT POUVANT ETRE ACTIVE ET SYSTEME POUR DOCUMENTS POUVANT ETRE ACTIVE
(54) Title: ACTIVABLE DOCUMENT AND SYSTEM FOR ACKTIVABLE DOCUMENTS



(57) Abrégé/Abstract:
A document (1) has on the substrate (6) at least one document number (2), an optical marking (3) with a machine-readable identification (7) and a storage field (4) for receiving a check number (9). It is only at the moment of delivery to an authorised person that the check number (9) is produced by means of a cryptographic operation from at least the document number (2), the identification (7) and a first secret key (10) and written into the storage field (4). An authenticity certificate produced in that way can be checked for its authenticity with a verifier using a cryptographic operation and the information stored on the document (1), by means of a second key.

ABSTRACT

A document (1) has on the substrate (6) at least one document number (2), an optical marking (3) with a machine-readable identification (7) and a storage field (4) for receiving a check number (9). It is only at the moment of delivery to an authorised person that the check number (9) is produced by means of a cryptographic operation from at least the document number (2), the identification (7) and a first secret key (10) and written into the storage field (4). An authenticity certificate produced in that way can be checked for its authenticity with a verifier using a cryptographic operation and the information stored on the document (1), by means of a second key.

(Figure 2)

Activatable document and system for activatable documents

The invention relates to an activatable document as set forth in the classifying portion of claim 1 and a system for activatable documents as set forth in the classifying portion of claim 9.

Such activatable documents can be used for personal identifications such as for example bank checks, passes, identity cards, subscriptions, tickets, health cards, credit cards, IC-cards, electronic purses (smart cards), value-bearing documents or stocks and shares and so forth. Such a system which uses activatable documents can be used in particular in relation to authenticity checks and/or owner checks in respect of the documents.

Visually easily recognisable holograms and other diffraction structures are used for safeguarding the stated documents, in which case they are mostly non-detachably connected to the substrate of the document, in the form of labels comprising a plastic laminate for protecting the structures which have the optical-diffraction effect (EP 0 330 738 A1). In themselves such documents have a very high standard of safeguard in relation to forgery or falsification.

EP 0 713 197 A1 discloses a data carrier in card form with an electronic circuit integrated into the card body and an optical marking, wherein the content of the electronic circuit is linked to the information of the optical marking. The optical markings used can be for example characters applied with ink such as a bar code or script characters, or structures which have an optical-diffraction effect, as in CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1, EP 0 883 085 A1 and so forth. The specifications referred to also describe embodiments of reading and writing apparatuses for the optical markings.

Finally US No 3 833 795 describes safeguarding the authenticity of serially numbered documents (banknotes, stocks and shares). Such a document bears two number fields, one being provided for continuous numbering of the documents, being the identity number, while the other is a check number which is selected randomly upon issue and which is

recorded in a centrally held list. An issued document is checked by reference to the external list or by means of a list algorithm, in which case a reading device firstly reads off the identity number and the check number and then compares the check number of the identity number on the document to the check number found by the reading device by means of the external list or the list algorithm. That document however is not protected from copying.

A major problem however arises in connection with the security of documents in the period from manufacture up to transfer of the document to the authorised person, as in that period the documents can be stolen in the course of transport, in order to supply unauthorised persons with those documents.

The object of the present invention is to safeguard documents which are inexpensively produced in large numbers and which are protected from copying, in such a way that the authenticity features thereof are completed only upon being brought into circulation and the authenticity features can be easily and inexpensively checked by machine.

In accordance with the invention that object is attained by the features recited in the characterising portions of claims 1 and 9. Advantageous configurations of the invention are set forth in the appendant claims.

Embodiments of the invention are described in greater detail hereinafter and illustrated in the drawing in which:

Figure 1 shows a document,

Figure 2 shows an activated document,

Figure 3 shows an IC-card as a document,

Figure 4 shows an information strip,

Figure 5 shows a system,

Figure 6 shows a validation device, and

Figure 7 shows a verifier.

In Figure 1 reference 1 denotes a document, reference 2 denotes a document number, reference 3 denotes an optical marking, reference 4 denotes a storage field, reference 5 denotes a check field and reference 6

denotes a substrate. The document 1 has a substrate 6 of paper, plastic non-woven fabric, plastic foil, a laminate structure of plastic, lacquers and/or paper and so forth. The two surfaces of the substrate 6 can be printed upon, as is usual in the case of bank checks, passes, identity cards, subscriptions, tickets, health cards, credit cards, IC-cards, electronic purses (smart cards), value-bearing documents or stocks and shares, banknotes and so forth, and have at least on one side the at least machine-readable document number 2. The document number 2 can be applied to the substrate 6 in clear text and/or in the form of a bar code in known manner using normal, fluorescing or magnetic ink. Characters such as a bar code, script characters or the like, or structures having an optical-diffraction effect, can be used for the optical marking 3, being applied for example with normal, fluorescing or magnetic ink or produced by perforation of the substrate 6. The optical marking 3 includes digital information, an identification 7. Use of the optical marking 3 with structures having an optical-diffraction effect is of particular advantage, because of its high level of safeguard in relation to forgery and copying. They are known from above-mentioned specifications CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1 and so forth and are suitable in particular for machine reading of an identification 7 contained in the optical-diffraction marking 3. The identification 7 contains items of information about the nature of the document, the document series and so forth, but not about the document number 2 which identifies the document 1 within a series, that is to say the documents 1 of a series can be inexpensively produced and differ only by virtue of the document numbers 2 which are applied for example by printing. The size of the optical marking 3 is determined by the identification 7 contained therein and the area required typically embraces approximately 1 mm^2. Extreme values in respect of that area may achieve a lower limit at 0.1 mm^2 and an upper limit at 1 cm^2. The optical marking 3 can also be provided in a visually invisible fashion in a transparent foil in accordance with CH 653 161 A5 or may also be inconspicuously concealed within a hologram or an optical-diffraction pattern, a security feature 8, for example in accordance with CH 659 433 A5. The security feature 8 serves

to identify the document 1 for the man in the street and has a highly conspicuous action on the document 1.

The storage field 4 and the check field 5 remain empty for the purposes of delivery to the persons bringing the document into circulation (points of sale, points of issue, bank clerks etc). The document 1 is useless without a check number 9 in the storage field 4, as shown in Figure 2. When the documents are brought into circulation, the documents must attain validity by virtue of activation thereof. For example the document number 2 and the identification 7 are read off the document 1 by machine. At least those items of information are linked together in a cryptographic operation with a first secret key 10 which is present outside the document, and the check number 9 associated with the document 1 is produced from the result, and written into the storage field 4. The document 1 is only now complete and its validity can be checked on the basis of the document number 2, the identification 7 and the check number 9. With certain kinds of document, provision is also made for writing to the check field 5 during activation. The content of the check field 5 includes at least visually readable, individual information related to a person, institution, company and so forth, such as name, address, social or other insurance number, nationality, time information, amount of money and so forth. Those items of information, referred to hereinafter as the code 11, can also be processed together with the document number 2 and the identification 7 with the cryptographic operation in relation to the check number 9.

In an embodiment of the document 1, in accordance with one of the known methods the storage field 4 and/or the check field 5 is written with the check number 9 and the code 11 in machine-readable printing. This clear text, for example OCR-text, is both visually readable and also machine-readable. Instead of or together with the printing, the check number 9 can also be represented in the form of a bar code which is widespread in the retail trade.

Figure 3 shows a further embodiment of the document 1 in the form of a card (health card, credit card, IC-card, smart card, and so forth). Let into the substrate 6 is a per se known module 12 with a microchip 13, the

storage field 4 being established in the memory 14 thereof. The storage field 4 can be written only once with the check number 9 upon activation of the document 1 by means of an electronic signal sequence which is transmitted by way of a contact field 15, and there is no longer any possibility of a later change. As in the above-mentioned EP 0 713 197 A1 the signal sequence can also be transmitted by means of inductive or optical means (not shown here) to a module 12, of suitable configuration, of the document 1.

Another embodiment of the document 1 in card form has a magnetic strip 16 on the substrate 7. The check number 9 (Figure 2) and the code 11 (Figure 2), upon activation of the document 1, are recorded in magnetically encoded form in the storage field 4 or in the encoding field 5 on the magnetic strip 16. The storage field 4 has at least the magnetically readable check number 9 after activation in the storage field 4.

A further embodiment of the document 1 has in the storage field 4 an optical-diffraction information carrier 17 which is shown in Figure 4 and which is applied to the substrate 6 during the process for manufacture of the document 1, as described in above-mentioned EP 0 718 795 A1. In the unwritten condition 17', the information carrier 17 has a row of diffraction fields 18 which are arranged in pairs 19, wherein the two microscopic diffraction structures of a pair 19 differ in respect of at least one grating parameter. During the activation procedure the check number is reproduced in the form of a digital sequence on the information carrier 17, in which case in the writing operation corresponding to the bit value in each pair of one of the two diffraction fields 18 the diffraction structure is destroyed by the application of heat energy or the diffraction structure is rendered inoperative by being covered over, for example with a non-transparent cover lacquer. After activation, in each pair, one of the two diffraction structures no longer has an optical-diffraction effect, in the information carrier 17". The storage field 4 now has the check number 9 in optically easily machine-readable characters. The advantage of this information carrier 17 is that it can be written only once. Any further change in the information carrier 17 can be easily detected by machine.

In an embodiment of the document 1 the optical marking 3 and the check number 9 is produced with diffraction structures and disposed on the same information carrier 17. The advantage of this embodiment is that the operation of reading off the identification 7 and the check number 9 and the operation of writing to the information carrier 17 are effected with a single optical reader 26 in accordance with EP 0 718 795 A1. The expensive security feature 8 (Figure 1) can be omitted.

The entries 2, 9, 11, the module 12 and the magnetic strip 16 can in themselves be distributed in any desired fashion on the two sides of the document 1, in which respect it is usually only the magnetic strip 16 which is arranged on the rear side of the substrate 6.

Figure 5 shows a system 20 which is suitable for use of the above-described documents 1. The system 20 includes at least one document 1, a validation device 21 for activation of the document 1 and a verifier 22 with which an authenticity check in respect of the document 1 is to be carried out. While the validation devices 21 are set up at the small number of people bringing the documents into circulation, a multiplicity of verifiers 22 which are simple to operate and which are as far as possible autonomous must be in operation wherever such documents 1 are subjected to an authenticity check.

The documents 1 supplied by the manufacturer, with the document number 2, are stored by the persons bringing the documents into circulation, until one of the documents 1 is allocated to an authorised person, in which case the document 1 allocated to that person is completed by means of the validation device 21 by writing the check number 9 into the storage field 4, to constitute an authenticity certificate 23.

An embodiment of the validation device 21 as shown in Figure 6 includes a computing unit 24, a transport device 25 for the document, an optical reader 26 for machine reading of the identification 7 (Figure 1) on the optical marking 3 of the non-activated document 1 and a recording means 27. Further optional reading units 29 which are shown in broken line in Figure 6 permit reading-off of the document number 2 (Figure 1), the check number 9 (Figure 2) and the code 11 (Figure 2). The reading units

29 differ according to the recording technologies once selected for the system 20, which are predetermined for the document number 2, for the check number 9 and for the code 11. The transport device 25, the optical reader 26, the one or more recording means 27 and the reading units 29 are connected to the computing unit 24.

The computing unit 24 is connected by way of lines to the transport device 25, the optical reader 26 and the recording means 27, it controls those units 25, 26 and 27 and receives the items of information emitted by those units 25, 26 and 27 so that the document 1 can be read off and labelled, by machine. The computing unit 4 has at least one security module 30 which in an integrated circuit includes a microprocessor with associated memory locations. The microprocessor executes cryptographic operations and uses the first secret key 10 contained in the memory locations.

In an embodiment, the transport device 25 produces a relative movement between the document 1 on the one hand and the reading means 26, 29 and the recording means 27 on the other hand. In Figure 6 the document 1 is moved with respect to the stationary reading means 26, 29 and the recording means 27. Different per se known embodiments for sheets or for cards are known and can be used for the transport device 25. It is possible to forego an expensive transport device 25 if the optical marking 3 or the security element 8 (Figure 1) is designed in accordance with the teaching in EP 0 883 085 A1 and writing of the storage field 4 is effected manually.

The recording means 7 is adapted to write the check number 9 and the code 11 into the storage field 4 and the encoding field 5 respectively, and uses the recording procedure provided for the document 1, for example a printing, ink jet, xerographic, perforation and the like method, a writing method described in EP 0 718 795 A1 for the information carrier 17, a magnetic recording procedure or electronic storage in the memory 14 (Figure 3). The check number 9 can also be written manually into the storage field 4, with waterproof ink. The perforation method for documents 1 is described for example in German utility model No G 93 15 294.9.

The keyboard 28 is quite generally an input device for items of information consisting of digits or alphanumeric characters. The input device can also be connected to the validation device 21 by way of a connection 28' to a telephone or computer network 37 (Figure 5) and in particular the items of information forming the code 11 can be called up from a central exchange.

The reading unit 29 is adapted to the recording technology used for the document 1. The reading unit 29 is for example a clear text reader, a bar code reader and the like for visually readable characters, from which the document number 2, the check number 9 and the code 11 are composed. Those reading units 29 use a light beam to scan parts of or the entire document 1 and measure the level of intensity of the light which is scattered back from the document 1. The reading unit 29 which is suitable for the magnetically recorded information or for electronically reading out of the memory 14 is generally known.

The structure and mode of operation of the optical reader 26 and for a reading unit 29 which is capable of reading the check number 9 out of the optical information carrier 17 (Figure 4) are known for example from above-mentioned specifications CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1 and EP 0 883 085 A1.

In an inexpensive embodiment for the activation procedure, an operator of a non-activated document 1 visually reads off the document number 2 thereof and manually inputs the document number 2 (Figure 2) into the computing unit 24 by way of a keyboard 28. Then, the document 1 is fitted or placed into the transport device 25 which is reduced to a passage or a platform, under the optical reader 26, so that the optical reader 26 can read off the identification 7 and communicate it to the computing unit 24. The computing unit 24 encrypts the identification 7 and the document number 2 with the first secret key 10 and reproduces a digital signature, the check number 9, on a display 31. The operator now manually transfers the check number 9 into the storage field 4 on the document which now activated in that way has become the authenticity certificate 23 (Figure 5). The storage field 4 can be divided into fields for

respective characters of the check number 9 in order to facilitate machine reading of the manually entered check numbers 9.

A second embodiment has a reading unit 29 which is shown in dotted line in Figure 6 and which reads off the document number 2 by machine directly from the document 1 and passes it to the computing unit 24. The computing unit 24 encrypts at least the identification 7 and the document number 2 with the first secret key 10 to form the check number 9. The recording means 27 then transmits the check number 9 into the storage field 4 using the technology which is predetermined by the system 20.

In a third embodiment the validation device 22 is additionally provided with the keyboard 28 and the display 31 in order by way of the keyboard 28 to input the code 11, with the display 31 serving to check the code 11. The code is also transferred with the recording means 27 on to the document 1. For particularly important documents 1 the validation device 21 is designed to demand the input of a personal identification number (PIN) from the user. In one case that PIN as a permission PIN identifies the operator who is operating the validation unit 21 and in a second case as an owner PIN it identifies the document owner, in which respect, upon activation of the document 1, the owner types in his PIN by way of the keyboard 28 and in the computing unit 24 the owner PIN serves together with the code 11 or on its own as a parameter for production of the check number 9.

In a fourth embodiment of the validation device 21, instead of the optical reader 26 and the reading unit 29, a single reader 26 is so designed that it can detect both the optical marking 3 and the document number 9.

In a fifth embodiment the validation device 21 is also adapted to detect the check number 9. Thus the validation device 21 is capable of distinguishing between activated and non-activated documents 1 and in addition checking the check number 9 for the correctness thereof.

The check number 9 is the result of the cryptographic operation in the computing unit 24, a mathematical function f:

check number 9 = f(document number 2, identification 7, first secret key 10), and

check number 9 = f(document number 2, identification 7, code 11, first secret key 10).

As the systems 20 differ not only in terms of the recording technology but also in respect of the number and nature of the parameters of the cryptographic operation, for the purposes of greater ease of description hereinafter the values which are present for production of the check number 9 on the document 1 such as document number 2, identification 7, code 11 and the owner PIN which is stored separately from the document 1, are referred to as parameters of the cryptographic operation, in which respect that means at least the document number 2 and the identification 7, if need be supplemented by the code 11 and/or the owner PIN. A system 20 is thus defined by the technologies used, the nature of the document 1, the parameters of the cryptographic operation and the first secret key 10.

Neither the first secret key 10 nor the algorithm are known to the public and are issued by a certification authority in a security module 30 for insertion into the computing unit 24. After the parameters of the function f in the security module 30 are inputted into the computing unit 24 the easily replaceable security module 30 directly produces the check number 9 or an intermediate result which serves for calculation of the check number 9 in the computing unit 24.

The first secret key 10 serves both for the cryptographic operation for producing the check number 9 and also for checking the correctness of the check number 9 with knowledge of the items of information present on the document 1.

The verifier 22 in Figure 7 has the same components as the validation device 21 (Figure 6), except for the recording means 27 (Figure 6). The design configurations of the verifier 22 differ in respect of the reading units 29 which differ according to the recording technology adopted for the system 20 (Figure 5). In the inexpensive embodiment the verifier 22 includes at least one receiving means 32 for an authenticity certificate 23 to be checked (Figure 5), a computing unit 33 with the security module 30, the optical reader 26 for the identification 7, the keyboard 28 and the display 31. The computing unit 33 is connected to the optical reader 26, the keyboard 28 and the display 31. With another cryptographic operation, the

computing unit 33 checks whether the check number 9 (Figure 2) matches the parameters of the cryptographic operation, which include at least the document number 2 and the identification 7. For that purpose the computing unit 33 uses a second key 34 which is contained in the security module 30 with the corresponding algorithm. The computing unit 30 cannot implement with the other cryptographic operation any encryption procedures like the computing unit 24 (Figure 6) in the validation device 21. The use of the second key 34 which is completely different from the first key 10 affords the advantage that the difficulty of keeping the second key 34 secret, which arises out of the wide-spread use of the verifiers 22, is irrelevant in regard to the security of the system 20. The computing unit 32 represents the result of the authenticity check on the display 31.

For an authenticity check, a checker visually reads off the parameters of the cryptographic operation, at least the document number 2 and the identification 7, on the authenticity certificate 23 and the check number 9 in the storage field 4, and supplies the computing unit 33 with the read-off sequence of characters, by way of the keyboard 28. The receiving means 32 can also be a simple platform under the optical reader 26, on which the checker lays the document 1 in such a way that the optical marking 3 is in the region of the optical reader 26. The identification 7 which is machine-read passes directly into the computing unit 33. The result of the authenticity check appears on the display 31. In the simplest case, the display comprises two signal lamps in order to represent the yes/no result of the authenticity check. It is advantageous however if the display 31 displays both the check number 9 and the parameters inputted by way of the keyboard 28, and the yes/no result.

In another embodiment, the verifier outputs a permission signal by way of a signal line 35 to a services apparatus 36. Receipt of the permission signal enables the service of the apparatus 36, for example door opening, issue of money, purchase of goods, registration and so forth.

Another embodiment of the verifier 22 has a receiving means 32 in the form of a transport system for documents 1 which are in sheet or card form. Connected to the computing unit 33 is the receiving means 32 which

is controlled by the computing unit 33 and, in addition to the optical reader 26, at least one reading unit 29 for communicating items of information. The reading unit 29 reads off by machine one or more parameters of the cryptographic operation. There is no need of a keyboard 28 for this embodiment. One reading unit 29 is sufficient if the parameters of the cryptographic operation and the check number 9 on the authenticity certificate 23 are recorded using the same recording technology.

For a system 20 in which the owner PIN is used, the keyboard 28 is provided for the owner who identifies himself to the verifier 22, with the owner PIN. The owner PIN which is inputted by way of the keyboard is used in the cryptographic operation as a parameter for checking the check number 9.

As in the case of the validation device 21, identification of the checking person by means of his user PIN is also advantageous in order to set the hurdle for possible hackers into the system 20 as high as possible. Input of the correct user PIN by way of the keyboard 28 permits the computing unit 33 to identify the user and to enable the validator 22 for operation.

In regard to Figure 5 it is also to be noted that the system 20 is advantageously embedded into a bidirectional telephone or computer network 37 for data exchange between the validation devices 21 and the verifiers 22 on the one hand and a computer 39 on the other hand. The validation device 21 is connected by way of the connection 28' to the network 37 and the network 37 by way of a line 38 to the central computer 39. Besides the above-mentioned call-up of data from the central computer 39 for the code 11 (Figure 2), the network 37 also makes it possible to set up in the central computer 39 a negative list of document numbers 2 of revoked authenticity certificates 23. The verifiers 22 which are connected to the central computer 39 by way of the network 37 receive by way of a data line 40 the regularly updated negative list, being transmitted into the computing unit 33 (Figure 7). The negative list is stored in a data memory 41 (Figure 7) of the computing unit 33 so that revoked authenticity

certificates 23 are detected by the verifiers 22 even in the event of failure of the network 37.

NEW CLAIMS

1. A method of using an activatable document (1) with an at least machine-readable document number (2), an optical marking (3) with a machine-readable identification (7) and a storage field (4) disposed on the substrate for receiving an at least machine-readable check number (9), characterised

in that the steps to complete the document (1) to provide an authenticity certificate (23), when the document is put into circulation, comprise

reading out the document number (2) and the identification (7),

producing the check number (9) as the result of a cryptographic operation with at least two parameters, the document number (2) and the identification (7), and a first secret key (10),

and

writing the check number (9) into the storage field (4),

and

in that after the document is put into circulation the authenticity of the authenticity certificate (23) is checked by the steps

reading the check number (9) out of the storage field (4) and at least the parameters, the document number (2) and the identification (7), on the authenticity certificate (23),

checking the relatedness of the check number (9) and the parameters by means of another cryptographic operation using a second key (34) different from the first key.

2. A method as set forth in claim 1 characterised in that the machine-readable identification (7) is optically read out of optical-diffraction structures of the optical marking (3).

3. A method as set forth in claim 1 or claim 2 characterised in that an at least visually readable, individual code (11) related to a person is

written into a check field (5) on the substrate (6).

4. A method as set forth in one of claims 1 through 3 characterised in that for activation of the document (1) the check number (9) is written in at least machine-readable characters into the storage field (4) arranged on the substrate (6).

5. A method as set forth in one of claims 1 through 4 characterised in that the check number (9) is written into the storage field (4) of a memory (14) of a microchip (13) let into the substrate (6) and that after the activation procedure the storage field (4) is so blocked that the content of the storage field (1), once written in, can no longer be altered electronically.

6. A method as set forth in claim 1 or claim 2 characterised in that the magnetically readable check number (9) is written in a magnetic strip (16) arranged on the substrate (6) with the storage field (4).

7. A method as set forth in claim 1 or claim 2 characterised in that the check number (9) is written at least into a part of the storage field (4) of an optical information carrier (17, 17') arranged on the substrate (6) and that after the activation procedure the check number (9) is optically read out of the optical information carrier (17, 17") which can no longer be altered in the storage field (4).

8. A method as set forth in claim 7 characterised in that the identification (7) is written into another part of the optical information carrier (17, 17').

9. A system (20) comprising at least

a document (1), wherein arranged on a substrate (6) of the document (1) is an at least machine-readable document number (2), an optical marking (3) with a machine-readable identification (7) and a

storage field (4) for receiving an at least machine-readable check number (9),

a validation device (21) which includes at least a transport device (25) for receiving the document (1) without a check number (9), a computing unit (24) with an input keyboard (28), a recording means (27) and an optical reader (26) for mechanically reading off the identification (7), wherein the recording means (27), the input keyboard (28) and the optical reader (26) are connected to the computing unit (24), the computing unit (24) is programmed for cryptographic operations with a first secret key (10) for producing the check number (9) by encryption of at least two parameters, the document number (2) and the identification (7) which is read off by the optical reader (26), and the recording means (27) is adapted to write the produced check number (9) into the storage field (4) so that upon being put into circulation the document (1) is completed with the check number (9) to provide an authenticity certificate (23), and

a verifier (22) which includes at least a computing unit (33) adapted for another cryptographic operation with a second key (34), the optical reader (26) for machine reading of the identification (7) and a receiving means (32) for aligning the authenticity certificate (23) to be checked in the machine reading operation, wherein the computing unit (33) is connected at least to the input keyboard (28), to a display (31) and to reading-off means (26; 28; 29) and is adapted for the authenticity checking operation by means of the cryptographic operation with the second key (34) to check the relatedness at least of the numbers recorded on the authenticity certificate (23), the check number (9) and the parameters used for producing the check number (9), and which has the display (31) for representing the result of the authenticity check and/or a signal line (35) for the delivery of a permission signal.

10. A system (20) as set forth in claim 9 characterised in that the verifier (22) has the input keyboard (28) for manual input of a personal identification number (PIN) for enablement of the verifier (22) and that

the verifier (22) is adapted to check the personal identification number of the user.

11. A system (20) as set forth in claim 9 or claim 10 characterised in that the verifier (22) has the input keyboard (28) connected to the computing unit (33) for manual input of the parameters for the cryptographic operation with the second key to the computing unit (33), wherein the parameters include at least the document number (2) and the check number (9).

12. A system (20) as set forth in one of claims 9 or 10 characterised in that the verifier (22) has at least one reading unit (29) connected to the computing unit (33) for manual input of the parameters for the cryptographic operation with the second key to the computing unit (33), wherein the parameters include at least the document number (2) and the check number (9).

13. A system (20) as set forth in one of claims 9 through 12 characterised in that the validation device (21) has the input keyboard (28) connected to the computing unit (24) for manual input at least of the document number (2) to the computing unit (24).

14. A system (20) as set forth in one of claims 9 through 12 characterised in that the validation device (21) has the reading unit (29) connected to the computing unit (24) for machine input of the document number (2) to the computing unit (24).

15. A system (20) as set forth in one of claims 9 through 14 characterised in that the validation device (21) is adapted for the input of an individual code (11) related to a person, by means of the input keyboard (28), that the validation device (21) includes a recording means (27) in the validation device (21) for writing the code (11) into the check field (5), and that the code (11) is one of the parameters for producing the check number (9) in the validation device (21) or for the authenticity check in the verifier (22).

16. A system (20) as set forth in one of claims 9 through 15 characterised in that the computing unit (24) in the validation device (21) is such that upon encryption of the check number (9) a personal identification number of the authorised person which is inputted by way of the input keyboard (28) is incorporated as a parameter for production of the check number (9) and that the verifier (22) produces the permission signal in the computing unit (33) only if, during the authenticity checking procedure, the personal identification number is incorporated by way of the input keyboard (28) of the verifier (22) in the computing unit (33) as a parameter of the cryptographic operation with the second key.

17. A system (20) as set forth in one of claims 9 through 16 characterised in that at least one validation device (21) and at least one verifier (22) are connected by way of a network (28', 38, 40; 37) to a central computer (39) for bidirectional data exchange.

18. A system (20) as set forth in one of claims 9 through 17 characterised in that the at least one verifier (22) is connected by way of a signal line (35) to a service apparatus (36) and that the service apparatus (36) is adapted to enable a service by means of the permission signal sent to the service apparatus (36) by way of the signal line (35).

Fig. 1:

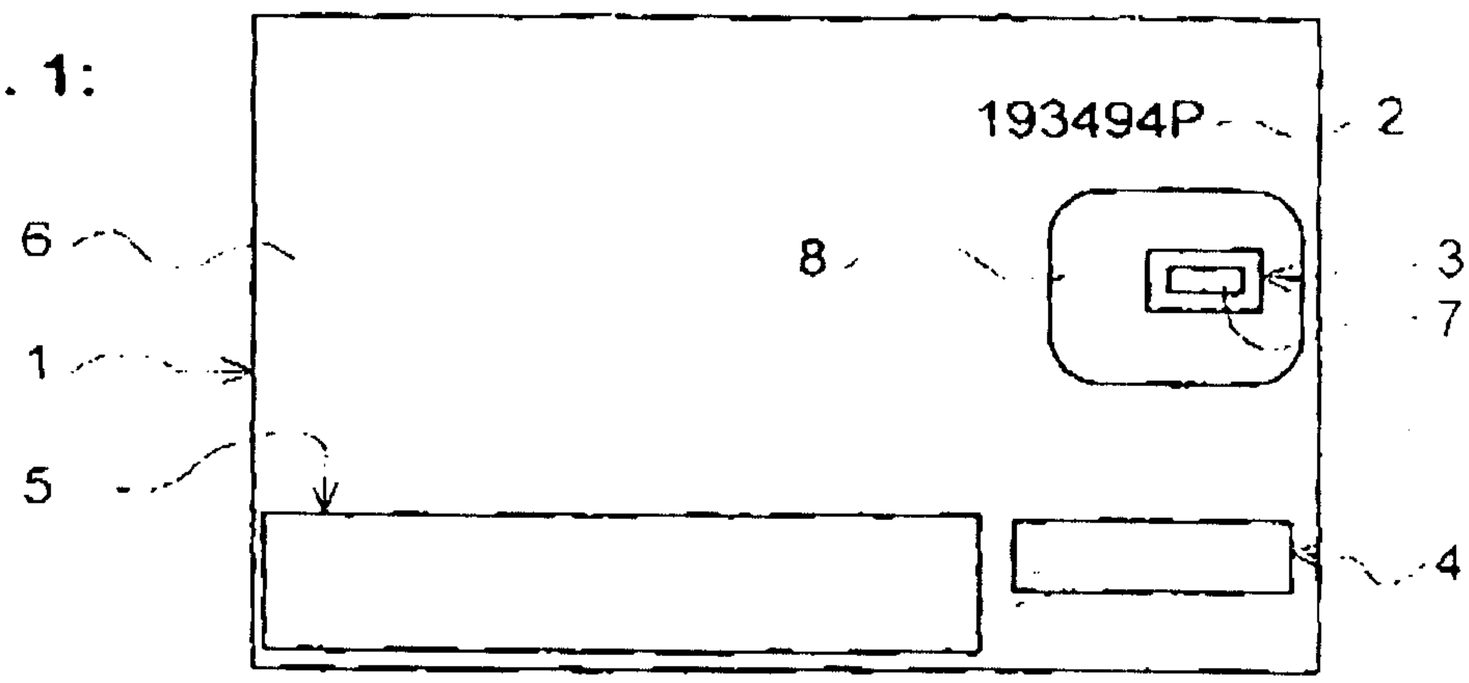


Fig. 2:

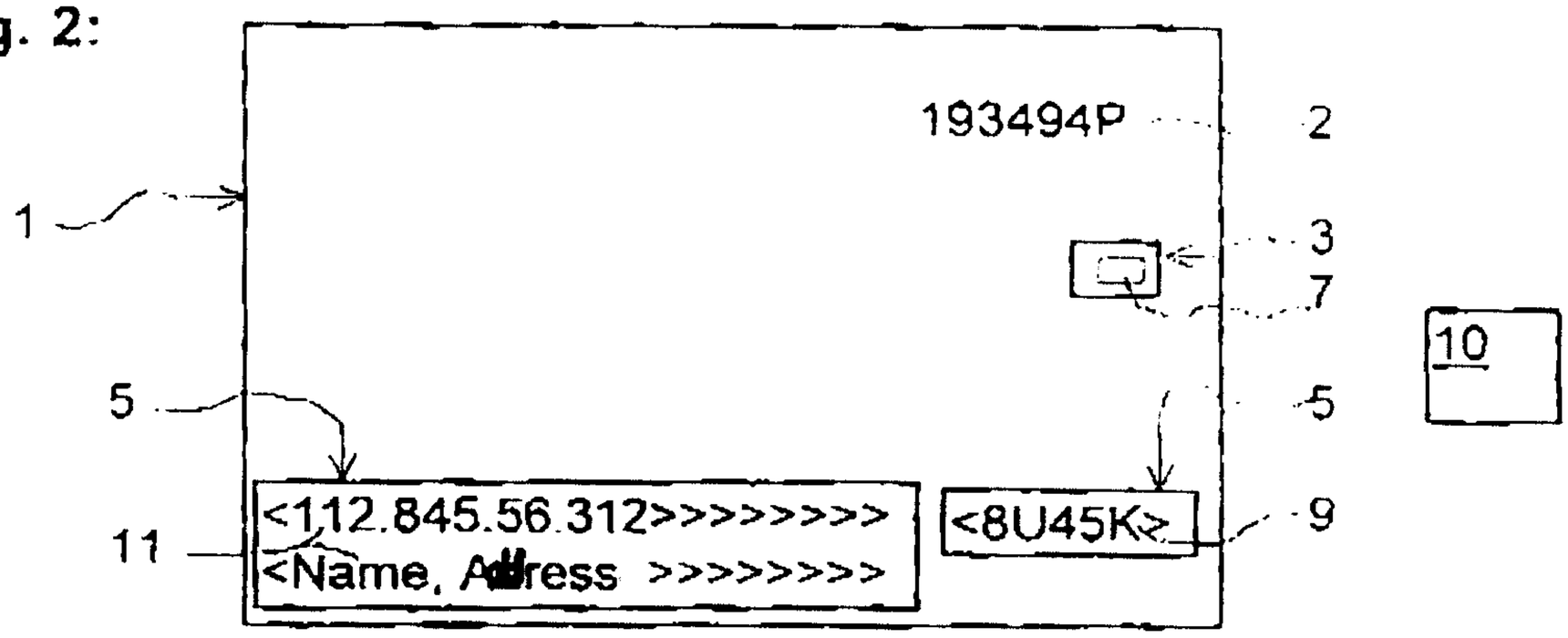


Fig. 3:

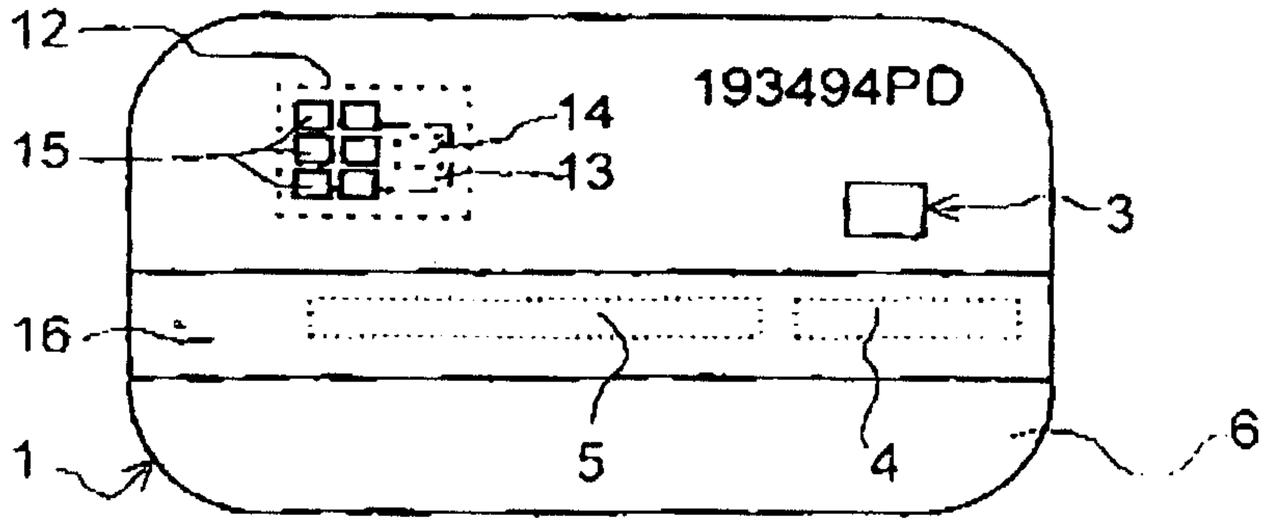
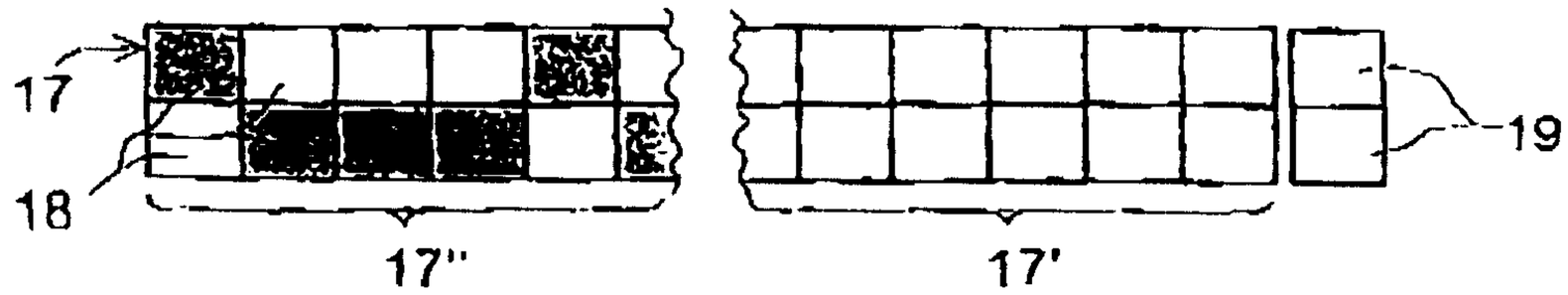


Fig. 4:



P2900

Fig. 5:

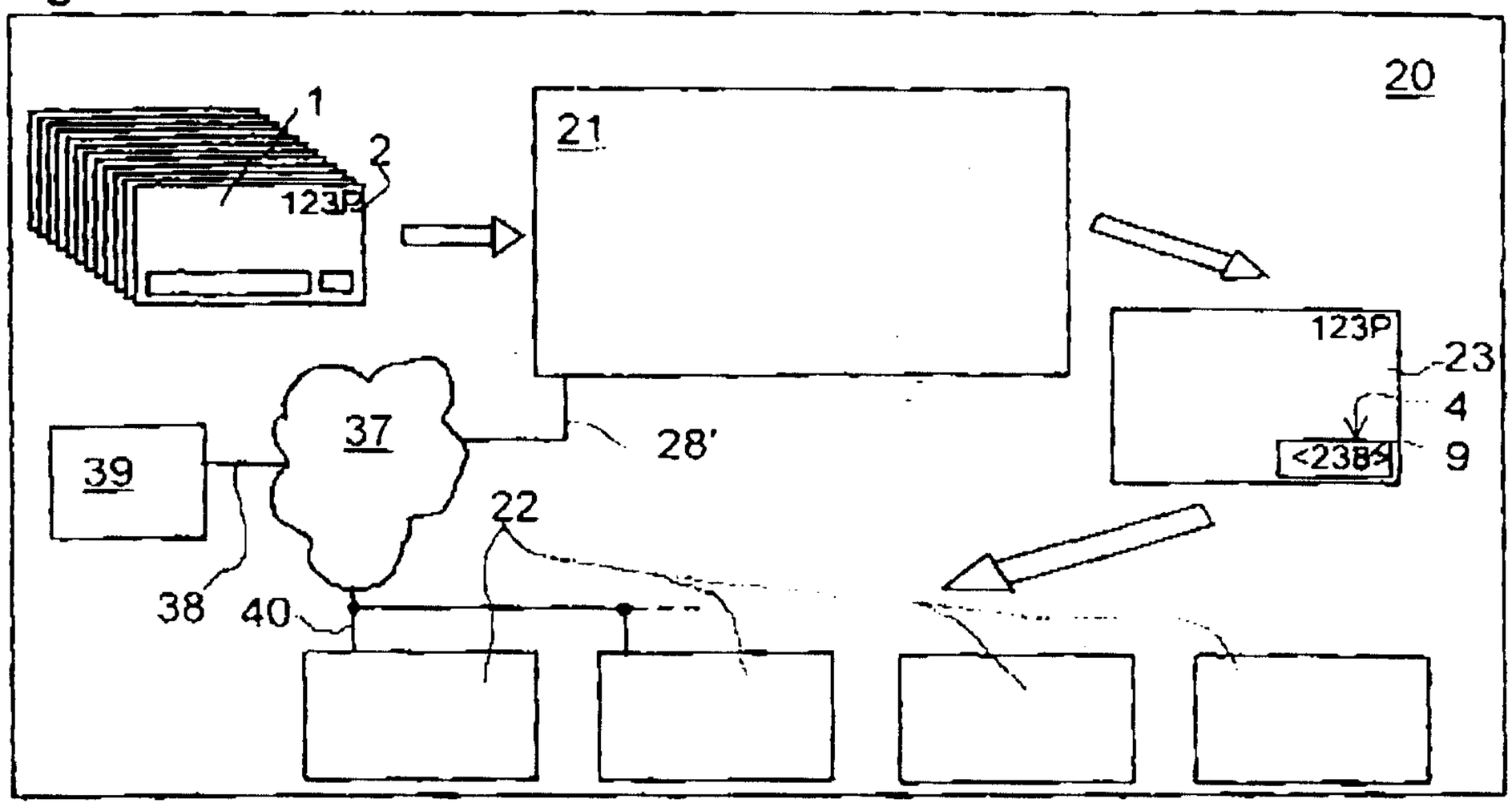

20
1
2
123P
21
123P
23
4
9
<23B4
37
39
28'
22
38
40

Fig. 6:

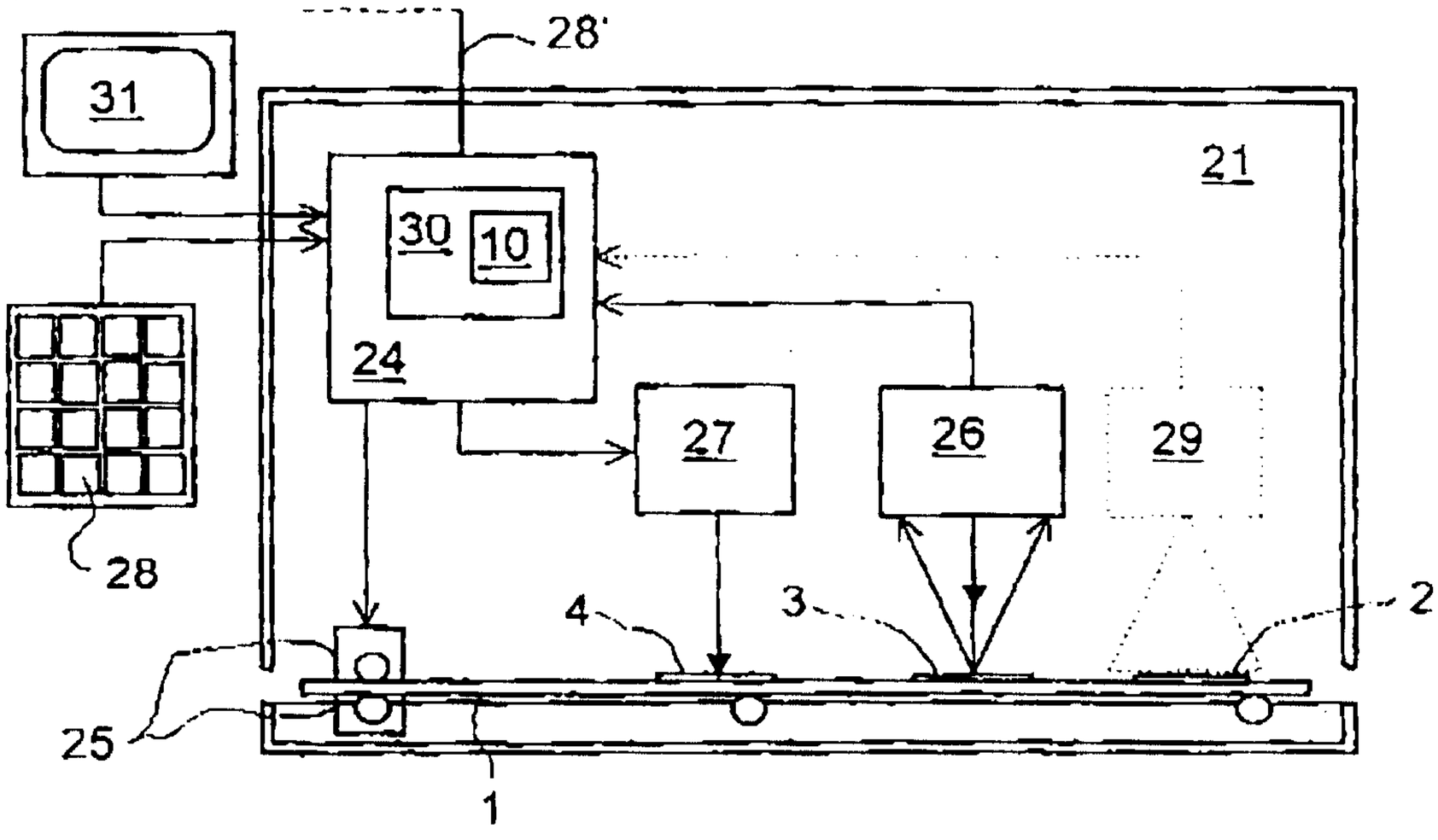
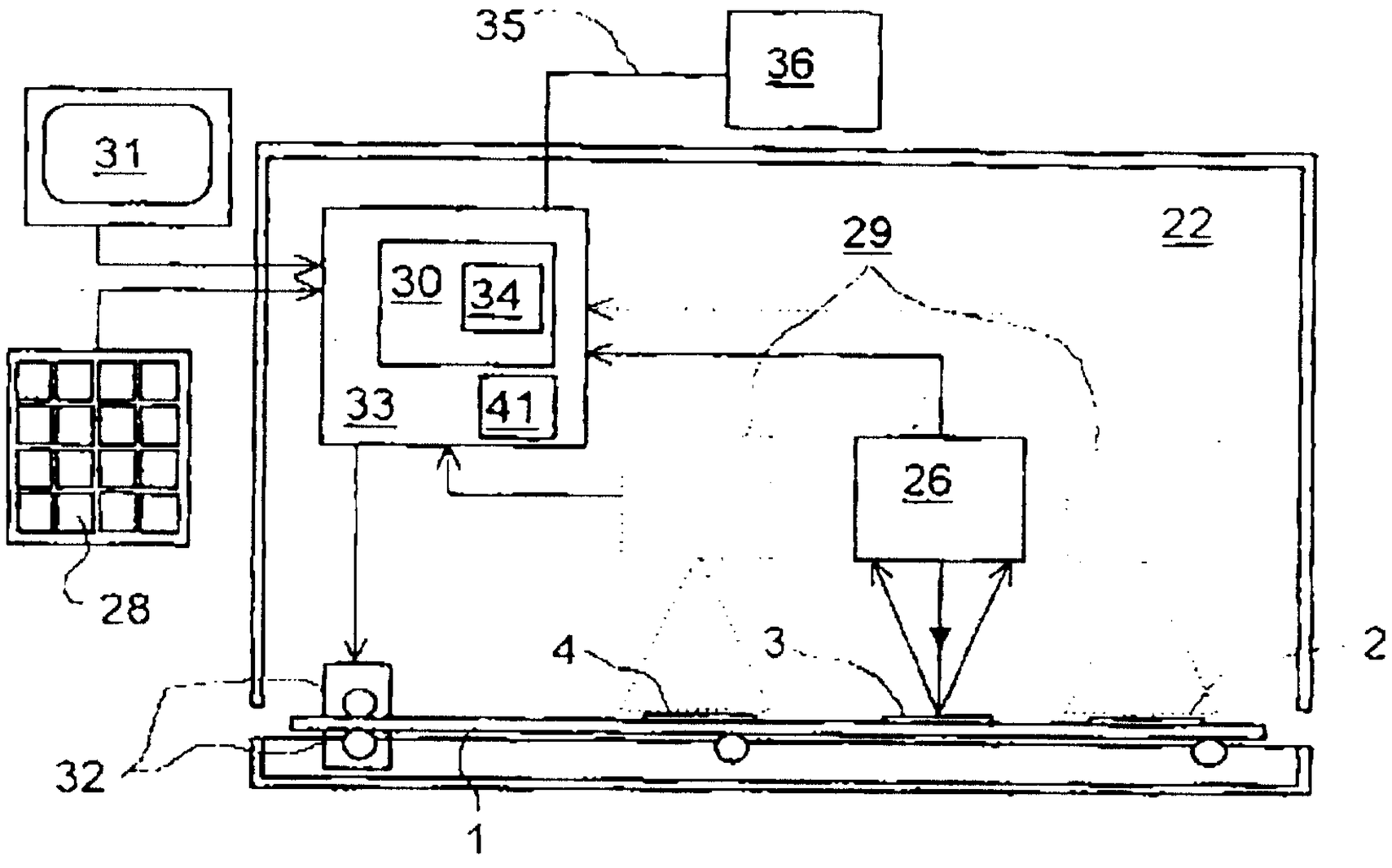
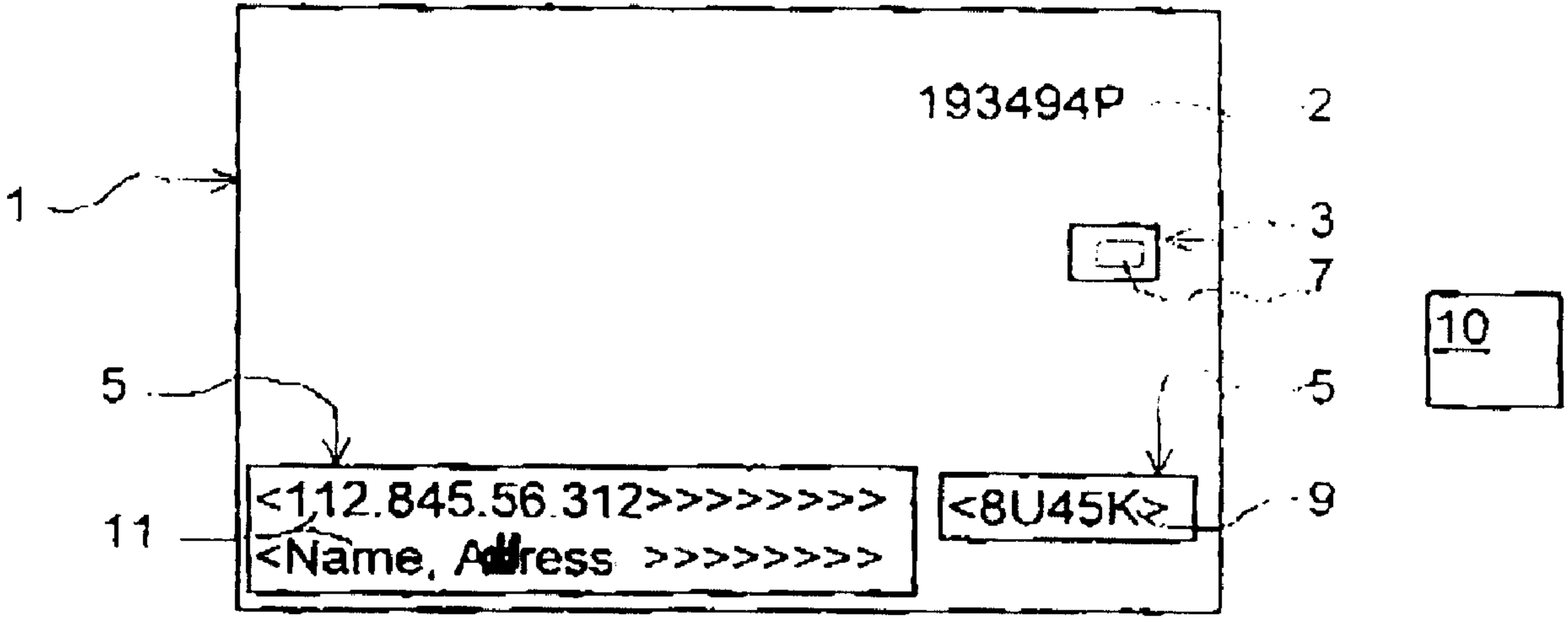

28'
31
21
30
10
24
27
26
29
28
4
3
2
25
1

Fig. 7:




193494P
2
1
3
7
10
5
5
<112.845.56.312>>>>>>>>>
<Name, Address >>>>>>>>>
11
<8U45K>
9