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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 April 2002 (11.04.2002)

PCT

(10) International Publication Number
WO 02/29732 A2

(51) International Patent Classification⁷: G07C

(21) International Application Number: PCT/EP01/11333

(22) International Filing Date: 1 October 2001 (01.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

00121582.1	2 October 2000 (02.10.2000)	EP
00123516.7	27 October 2000 (27.10.2000)	EP
00126074.4	29 November 2000 (29.11.2000)	EP
00127684.9	18 December 2000 (18.12.2000)	EP
01100361.3	5 January 2001 (05.01.2001)	EP

(71) Applicant *(for all designated States except US)*: **ROTAS REMOTE ONLINE TRANSACTION AUTHORISATION SYSTEMS GMBH** [DE/DE]; Koch 33, 41179 Mönchengladbach (DE).

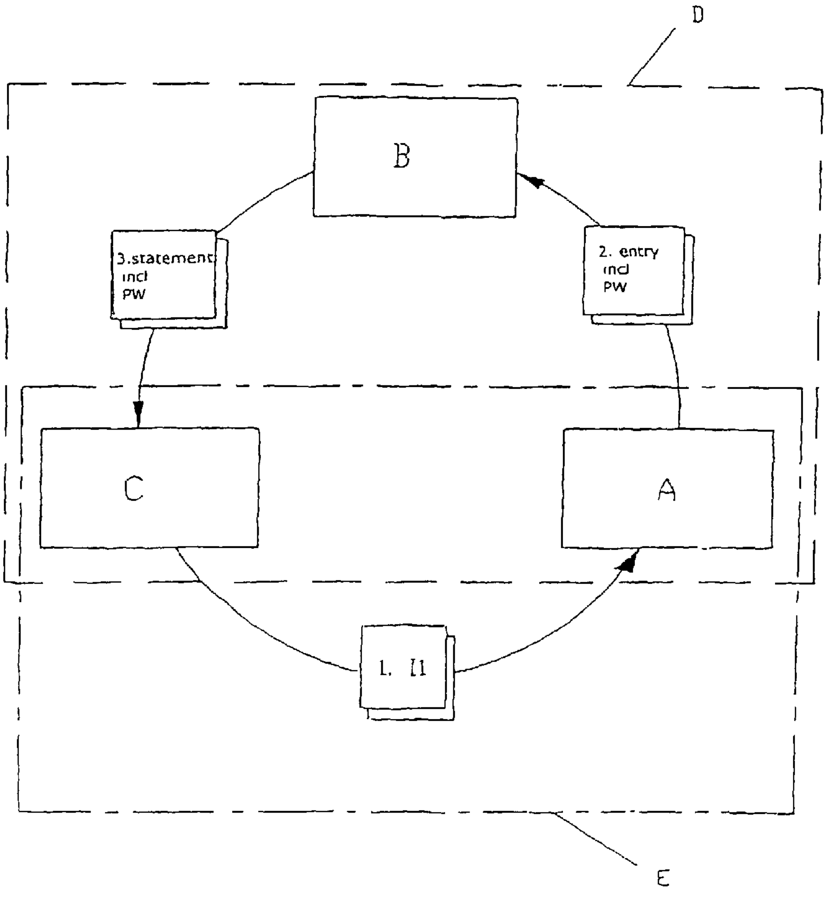
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **STOFFELSMA, Bouke, Christiaan** [NL/DE]; Croonsallee 37, 41061 Mönchengladbach (DE).

(74) Agent: **LIPPERT, STACHOW, SCHMIDT & PARTNER**; Frankenforster Str. 135-137, 51427 Bergisch Gladbach (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,

[Continued on next page]

(54) Title: AUTOMATIC IDENTIFICATION APPARATUS AND IDENTIFICATION METHOD



(57) Abstract: In order to further develop an automatic identification apparatus (A) for the identification of a user (C), wherein the user (C) transmits account details to the automatic identification apparatus (A), and an identification method for the identification of a user (C) for a security-relevant use, in which the user (C) transmits account details to an identification instance, in such a way that identification of a user can be more securely implemented, it is proposed in accordance with the invention that th automatic identification apparatus produces a password and transmits same to the account details of the use (C):

WO 02/29732 A2

MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that 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.

Automatic identification apparatus and identification method

The invention concerns an automatic identification apparatus for the identification of an instance, wherein the instance transmits account details to the automatic identification apparatus.

The instance can be a natural person or a legal entity, for example a user, a closed user group of a corporation or a theatre. It is also possible to envisage a process which for example runs in a computer.

It is known for a user to transmit account details to the automatic identification apparatus on various communication media and for the automatic identification apparatus to check the data of the user in terms of plausibility. Usually, that check is effected on the basis of lists which are stored in the automatic identification apparatus or deposited in a further store, as for example in the case of a bank, wherein the automatic identification apparatus can access the lists, in the context of the plausibility check. Accordingly, the automatic identification apparatus can be installed directly at a bank or a third-party provider.

Transmission of the account details can be effected both orally directly over the telephone or by way of data-processing equipment.

The known automatic apparatuses suffer from the disadvantage that they implement exclusively a plausibility check, that is to say they check the general existence of the specified bank connection, but not whether the user is authorised to access the stated account. Thus for example a user could specify someone else's account details to which he has gained access, as being his own, and those account details are confirmed as being in existence in the context of the plausibility checking procedure. By way of example numerous undertakings list the bank details on their letterheads. Particularly in the e-commerce sector in which personal verification is ruled out, account details are increasingly specified, which are not actually to be associated with the respective user but which by virtue of the positively executed plausibility check are sufficient for identification purposes and which subsequently result in incorrect billing.

Therefore the automatic identification apparatuses known from the state of the art do not afford identification which is sufficiently secure for the e-commerce sector. For that reason, payment by credit card or debit entry procedures is considered to lack security in the e-commerce sector and impedes development of trade over the Internet.

The object of the present invention is to further develop an automatic identification apparatus as set forth in the opening part of this specification, in such a way that user identification can be more securely implemented.

In accordance with the invention that object is attained in that the automatic identification apparatus works out a password and transmits same to the address represented by the account details. The term password means an item of secret information which is recognisable only to a limited user group; the user group can include one or more persons.

Preferably the password comprises a numerical or alphanumeric character chain or string. The length of string is determined in accordance with the required degree of security, in which respect just two alphanumeric characters can represent a level of security which is adequate for the banking sector. The plausibility check which is known from the state of the art is thus enlarged by the production of a password which is transmitted to the account details and which can only be called up by the user who has authorised access for that account so that the password is also only accessible to the user. The access authorisation does not have to be limited to an individual person but can exist for example for a group of users, such as for example in the case of a number of persons in an undertaking or corporation, who are authorised to access a business account. In that respect, for communication of the password from the banking system to the user, recourse is made to an existing, secured transmission path, in respect of which the user access authorisation has already been checked.

Transmission of the password is preferably effected as a purpose of use in a regular bank transaction. The bank transaction can be effected in the form of a debit entry or a credit entry (for example as a remittance). At least the password must be representable on a statement of account or a comparably secure medium.

Transmission of the account details from the user to the automatic identification apparatus is preferably effected by way of data processing, in particular by way of the Internet. Transmission of the bank transaction with the password to the address represented in the account details is effect optionally manually directly, by telephone or preferably also by way of data processing. The known protocols HBCI, DTA or other protocols which are suitable for paperless data carrier exchange are then used for that purpose.

The automatic identification apparatus according to the invention can also be used for mobile commerce (m-commerce). In that situation of use the user transmits his account details to the automatic identification apparatus with a call from his mobile telephone whose call number can be determined by CLI (calling line identification). Instead of a call, the user can also send an SMS with his account details to the automatic identification apparatus. The automatic identification apparatus then transmits the password to the specified account details. In that case the password is a secret telephone number which the user has to call up for enablement purposes (identification). Preferably this involves one or more secret telephone numbers which are associated with the automatic identification apparatus as a reserved circle of numbers. If the user calls such a secret telephone number of the automatic identification apparatus, then the automatic identification apparatus, by virtue of the association of the telephone number of the calling mobile telephone with the secret telephone number, can check identification of the user and the authority for access to the stated account details and, if the result is positive, enable the user or record same in a registration database.

It will be appreciated that this possible use is not limited to mobile telephones but can also be implemented with a fixed line; the crucial consideration is the association of a bank connection with the telephone number of the user making the call.

In order to avoid communication of the account details from the customer to the automatic identification apparatus possibly being tapped, transmission of the account details to the automatic identification apparatus is preferably effected in encrypted form with a public key of the automatic identification apparatus. With that asymmetric encryption process, each user can encrypt his account information, but only the automatic identification apparatus can decrypt the account details. A known asymmetrical encryption process is RSA (Rivest Shamir Adleman). In that configuration, the automatic identification apparatus produces a public key and a private key, of which it makes only the public key available to the users.

Usually, the password can be used for identification purposes for at least one transaction. The term transaction is used to denote any action between two instances, for example implementation of a purchase, calling up items of information, access to proprietary data, making a booking, visiting a cultural event and so forth. The identifications can be implemented by way of the automatic identification apparatus according to the invention or directly with an automatic identification apparatus which is known from the state of the art and which only requires the input of a password, for example a RADIUS system. An Internet Service Provider can thus ensure that only a clearly identified customer can claim the services thereof.

In an alternative development the Internet Service Provider can debit the use charges for the services requested by way of the account details of the requesting user. It can implement that by virtue of operation of an automatic identification apparatus according to the invention, which permits the association of a password with the account details or it can cause it to be carried out as a service by an operator of an automatic identification apparatus according to the invention. For example this may involve various servers in the Internet.

The password can be valid for a limited time or can be used only for a predetermined number of transactions.

The password can be in widely varying formats. In the simplest embodiment the password serves only for unique identification of the user in relation to another instance (automatic identification apparatus, information supplier, Internet Service Provider, theatre, and the like); it thus performs the function of a certificate for proving the identity of an instance or a user. That means that further items of user information (call number of a mobile telephone or telephone specified by the user, his pass number, his social security number, his finger print, further biometric features of a user, a public key and so forth) can be transmitted in certified form with the password. The communication of a further password which for example satisfies a higher security level or which is accessible to a user circle other than the first one is something that can also be envisaged.

The particular attraction is that only the items of information which are transmitted by the user, and no further items, are known to the automatic identification apparatus; at any event however those items of information permit billing with the user by the automatic identification apparatus. If the instance operating the automatic identification apparatus differs from the instance in respect of which a user wishes to afford proof of his identity the user enjoys an anonymity which is equivalent to a cash payment.

Preferably the password is the key for a symmetrical encryption process. Those encryption processes are generally known; a known encryption process of that kind is DES (Data Encryption Standard) which uses a 56 bit-long key. Secure communication is now possible between automatic identification apparatus and user as the password is known to both sides. In the same way, a communication is possible between the user and further information suppliers to whom the password/the key is notified or the computing path for production of the password is known.

A particularly high level of security is offered by a key which can be used for the decryption of a public key used by the user (asymmetrical encryption process). That public key can either be produced by the user himself or it can be transmitted to the user by a further instance, for example on a smart card. As the private key of the user remains with the latter, in this case the automatic identification apparatus can lastingly check the identity of the user with the public key, with conventional challenge-response procedures, by requiring the user to encrypt an item of information with the private key which is known exclusively to the user, which can then be decrypted with the public key associated with the user. Identity of the items of information sent and received by the automatic identification apparatus ensures the identity of the user.

From the point of view of the user, it is possible to achieve a particularly high security stage if the public key is associated with a private key of the user, which is contained in an encryption device in such a way that it cannot be read out. The encryption device for the private key can be for example a money card, a smart card or a dongle. It can also be integrated in a mobile telephone or the like.

The invention also concerns an identification method for the identification of an instance, in which the instance transmits to an identification instance at least one item of information of the instance, which includes account details.

In consideration of the disadvantages set out in the opening part of this specification the object of the present invention is to further develop such an identification method, in such a way that identification of the instance can be more securely implemented.

In a first configuration it is proposed that firstly a password is ascertained or produced by the identification instance, and the password is then transmitted to the account details of the instance.

A second configuration provides that the first instance to be identified firstly transmits a password to the identification instance which detects that password for identification of the first instance for still following further identifications.

Finally, the invention concerns an identification method for the identification of an instance to be identified, in which a bank system transmits to an identification instance at least an item of information of the instance, which contains account details. This invention is also based on the above-indicated object.

To attain that object, it is proposed that the identification instance produces or ascertains a password and transmits it to the account details.

What is common to all the above-indicated operating procedures is that an already existing and secure information path of the banking system can be used for transmission of the passwords. It will be appreciated that only the target instance - that is to say either the identification instance or the instance to be identified - has access authorisation to the respectively specified account details so that only the target instance can call up the password. The methods according to the invention additionally ensure that the specified account number exists. As recourse is made to already existing communication paths, communication of the password to the target instance can be quickly implemented.

The identification instance can be a natural person who receives the account details of the instance directly or by telephone, produces a password or ascertains it for example from a table, and transmits it in the form of a bank transaction to the account details specified by the instance or the bank system. Preferably the identification instance is in the form of an automatic apparatus, for example in the form of a server in a data network.

A particular advantage of the identification methods is that closed user groups or LAN/WAN-users can also be easily, quickly and inexpensively identified therewith. Those users cannot be uniquely identified solely by way of the IP address. Thus for example given providers attribute a new IP address to the user for each session. In addition, anonymisers can modify the IP addresses. Finally, IP addresses are repeatedly allocated. The further alternative of transmission of the credit card number is insecure, as stated above, and does not afford a definite and unambiguous identification option. In comparison the method according to the invention is secure and inexpensive as this only involves incurring the costs of a bank transaction for the identification instance. In the optimum case transmission of the password to the first instance can be carried out in real time.

Preferably the first instance is a user.

Entering the password to the specified account details can be in the form of a debit entry or a credit entry (for example a credit transfer or remittance).

Particularly when carrying out the identification method in a data network, for the avoidance of misuse it is desirable for the account details to be transmitted in encrypted form with a public key to the identification instance in order to ensure that only the identification instance having the private key associated with the public key can read the account details. If the message is sent for example to a wrong address, the receiver cannot see the account information.

In use of the identification method in the network, in a further step in the method, the use fee for calling up proprietary data (content) can be debited against the account details. The operation of checking the password can be effected both by the identification instance and also by the server providing the data element, to which the password was previously transmitted.

As described hereinbefore, the identification method does not necessary have to be initiated by the instance. As an alternative for example the bank system or the instance managing customer data can transmit the account details to the identification instance for the production of passwords, which transmits the account details together with the passwords back to the bank connection details. In that manner, banks and institutions managing customer accounts can cause passwords to be generated in the preliminary stage in relation to the specific inquiry of a customer, which passwords the customer can if necessary read off his statement of account and thus call up proprietary information (content) for which the password is required.

In regard to transmission of the password, the password can be accompanied by further items of information which are associated with use of the password, for example the name of the supplier who accepts the password, the location and the time of an event in respect of which tickets were reserved with the password, the financial standing of the user or the number of use options of the password and the like. It can also be provided that, before transmission of the password, firstly the financial standing of the user is checked.

The methods according to the invention are particularly suitable for being employed in uses which are relevant in terms of security. It will be appreciated that, in regard to the methods according to the invention, it is also possible to use the passwords for the areas of use which were described hereinbefore in connection with the automatic identification apparatus.

In the case of the identification method in which the instance to be identified is a user who operates a mobile telephone and who initiates the method by transmitting his account details to the identification instance, the user can specify as his password the number of his mobile telephone so that the identification instance directly receives the account details and the telephone number of the mobile telephone and can for example record those items of information for enablement purposes in a registration database provided at the identification instance.

In a particularly secure development, it can be provided that the password which is transmitted from the identification instance to the specified account details is used only for enablement of the instance to be identified, in particular a user, but cannot be used repeatedly. When first making a connection to the identification instance or the automatic identification apparatus, the instance to be identified specifies that password and is immediately required independently to establish a fresh password which is used in future. Detection of the fresh password can also be effected with the initial detection of the account details and enabled by input of the password transmitted by the identification instance. In that way, both identification of the instance to be identified is completed and also access to the specified account details is guaranteed. It will be appreciated that in that way services requested by the instance to be identified can also be billed by way of the account details. That fresh password can now be used as a symmetrical or asymmetrical key in the above-described manner for the certified communication between the various instances. If the instance to be identified represents a user, the fresh password can include a user name to be determined by the user (for example a username or pseudonym).

The mode of operation of the automatic identification apparatus according to the invention and the identification method is illustrated in the drawings by means of preferred embodiments. In the drawings:

Figure 1 is a diagrammatic view of the mode of operation of a conventional automatic identification apparatus,

Figure 2 is a diagrammatic view of the mode of operation of a automatic identification apparatus according to the invention,

Figure 3 is a diagrammatic view of an automatic identification apparatus according to the invention with passwords which can also be used by other automatic identification apparatuses which do not operate in accordance with the invention,

Figure 4 is a diagrammatic view of an identification method according to the invention which takes place in an alternative fashion, and

Figure 5 is a diagrammatic view of the implementation of a further alternative of the identification method according to the invention.

In the Figures the automatic identification apparatus is identified by A, the user by C and the bank system by B. The automatic identification apparatus A forms the identification instance and the user C an instance to be identified. The bank system can include one or more financial institutions or may comprise institutions managing customer accounts, for example a department store, an airline, a telephone company or an automobile club. The transmitted items of information are represented at the arrows connecting the instances A, B and C, in the boxes therebehind. The arrows identify the direction of the flow of information; the communication paths between the instances A, B and C are identified by broken lines.

The automatic identification apparatus A shown in Figure 1 in accordance with the state of the art operates as follows: the customer C transmits to the automatic identification apparatus A in step 1 account details I1, generally comprising the following pieces of information: name, account number and bank sort code. In the case of a credit card, the credit card number, name and expiry date are the transmitted items of information. The automatic identification apparatus forwards those items of information to the bank system B in step 2. In the final step 3 the bank B sends to the automatic identification apparatus A the information I2 which states whether the account specified in I1 exists. Under some circumstances the financial standing of the account is also specified. No check is made to ascertain whether the user C is actually authorised to access the specified bank details I1. The entire communication is effected for example over the Internet E.

Figure 2 in contrast shows the basic mode of operation of the automatic identification apparatus and method according to the invention. In step 1 the customer C again sends the information I1 by way of a known communication medium, for example the Internet E, to the automatic identification apparatus A. The automatic identification apparatus thereupon generates a password PW and in step 2 transmits the information I1 with the password PW in the form of a usual account transaction, in particular a remittance, to the bank system B. The transmission from the bank system B to the customer C involves an already established path D of the bank system B, which ensures access authorisation on the part of the customer to the account details. That transaction can be transmitted within the bank system from a bank account associated with the automatic identification apparatus to a bank account corresponding to I1. In the concluding third stage the user C calls up his statement of account including the password PW from the bank system B. Accordingly, the user C obtains the password only when he actually has access authorisation for the account identified by I1.

Figure 3 shows a password PW which is accepted both by the automatic identification apparatus A according to the invention and also by automatic identification apparatuses X,Y and Z which are not designed in accordance with the invention. In that way, the automatic identification apparatus A can generate passwords for other instances, for example for an Internet Service Provider or an information supplier.

The identification method shown in Figure 4 is modified in relation to the above-described methods insofar as, in the first step, the user C transmits the items of information I1 (account number and a name for that account) with a first password PW1 to the automatic identification apparatus A. The automatic identification apparatus A then produces a second PW2 and transmits same to the bank system B. That second password PW2 can now be called up by the user C. Both passwords PW1 and PW2 must be present for identification of the user C in relation to the automatic identification apparatus A. As the first password PW1 is unknown to the bank system B any misuse by the bank system is reliably excluded. The first password PW1 can include for example a pseudonym or username selected by the user.

The password PW1 can be used for secure communication of the user C with the automatic identification apparatus A or third-party instances to which the password PW1 has been previously passed.

Finally Figure 5 diagrammatically shows an identification method according to the invention in which a user C transmits a password PW to account details of the automatic identification apparatus A. For that purpose, in a first step, the user C actuates a bank remittance (electronically or by means of paper) to the account details of the automatic identification apparatus A, which is specified for example on the homepage of the automatic identification apparatus A. In a second step the automatic identification apparatus calls up that password PW from the account details. The password can now be used for the above-described uses for the purposes of the verified communication between the user C, the automatic identification apparatus A and further instances to which the password is notified.

These developments also provide for the use of a conventional information path, for example the Internet E, for communication between the user C and the identification instance A, whereas recourse is had to the existing and secure communication paths D of the bank system B for the transmission of data from the identification instance A to and from the bank system B.

List of references

A	automatic identification apparatus
B	bank system
C	user
PW	password
PW1	first password
PW2	second password
X, Y, Z	automatic identification apparatus
D	communication paths of the bank system
E	Internet

CLAIMS

1. An automatic identification apparatus (A) for the identification of an instance, which transmits account details to the automatic identification apparatus (A), characterised in that the automatic identification apparatus (A) ascertains or produces a password (PW) and transmits same to the address represented in the account details.

2. An automatic identification apparatus (A) according to claim 1 characterised in that transmission of the password is effected in the form of a debit entry.

3. An automatic identification apparatus (A) according to claim 1 characterised in that transmission of the password (PW) is effected in the form of a credit entry.

4. An automatic identification apparatus (A) according to one of claims 1 to 3 characterised in that transmission of the account details and/or transmission to the address represented in the account details is effected by a data processing procedure.

5. An automatic identification apparatus (A) according to one of claims 1 to 4 characterised in that transmission of the account details to the automatic identification apparatus (A) is effected encrypted with a public key of the automatic identification apparatus.

6. An automatic identification apparatus (A) according to one of claims 1 to 5 characterised in that the password (PW) can be used for identification for at least one transaction.

7. An automatic identification apparatus (A) according to one of claims 1 to 5 characterised in that the password (PW) can be used for identification for at least one transaction which is checked by the automatic identification apparatus (A).

8. An automatic identification apparatus (A) according to claim 6 or claim 7 characterised in that the password (PW) is invalid after a time which is predetermined by the automatic identification apparatus (A) and/or a predetermined number of transactions.

9. An automatic identification apparatus (A) according to one of claims 1 to 8 characterised in that the password (PW) is the key for a symmetrical encryption process.

10. An automatic identification apparatus (A) according to claim 9 characterised in that the password (PW) is the key for a symmetrical encryption process between the instance and the automatic identification apparatus (A).

11. An automatic identification apparatus (A) according to claim 9 or claim 10 characterised in that the key can be used for transmitting or decrypting a public key used by the instance.

12. An automatic identification apparatus (A) according to claim 11 characterised in that the public key can be used for the communication between the instance and the automatic identification apparatus (A).

13. An automatic identification apparatus (A) according to claim 11 or claim 12 characterised in that the public key is associated with a private key of the instance, which is contained in an encryption device in such a way that it cannot be read out.

14. An automatic identification apparatus (A) according to one of claims 1 to 13 characterised in that it has a data store for the passwords which are worked out and the associated bank details.

15. An automatic identification apparatus (A) according to one of claims 1 to 14 characterised in that it has means for encryption and decryption of items of information in accordance with symmetrical key methods.

16. An automatic identification apparatus (A) according to one of claims 1 to 14 characterised in that it has means for encryption and decryption of items of information in accordance with asymmetrical encryption methods.

17. An automatic identification apparatus (A) according to one of claims 9 and 10 characterised in that the instance is a user (C) and that the key can be used

for decryption of a biometric identification feature produced by the user (C) and/or transmission.

18. An automatic identification apparatus (A) according to one of claims 1 to 17 characterised in that the instance is a user (C) who transmits to the automatic identification apparatus (A) the account details together with a telephone number of a telephone he uses, in particular a mobile telephone.

19. An identification method for the identification of an instance to be identified, in which the instance transmits to an identification instance at least one item of information of the instance, which includes account details, characterised in that the identification instance produces or ascertains a password (PW) and transmits it to the account details.

20. An identification method for the identification of an instance to be identified, in which the a bank system transmits to an identification instance at least one item of information of the instance, which includes account details, characterised in that the identification instance produces or ascertains a password (PW) and transmits it to the account details.

21. An identification method for the identification of an instance to be identified, in which the instance transmits to an identification instance at least one item of information of the instance, which includes account details, characterised in that the instance

transmits a password (PW) to the identification instance which detects said password (PW) for the identification of the first instance for still following identifications.

22. An identification method according to claim 19 or claim 20 characterised in that the transmission is entered as a debit entry.

23. An identification method according to claim 19 or claim 20 characterised in that the transmission is entered as a credit entry.

24. An identification method according to one of claims 19 to 22 characterised in that the account details are transmitted encrypted with a public key to the identification instance.

25. An identification method according to one of claims 19 to 24 characterised in that the password (PW) is used for identification purposes for at least one transaction.

26. An identification method according to claim 25 characterised in that the password (PW) is used for identification purposes for at least one transaction which is checked by the identification instance.

27. An identification method according to one of claims 19 to 26 characterised in that the password (PW) becomes invalid after a number of transactions and/or a time which is predetermined by the identification instance.

28. An identification method according to one of claims 19 to 27 characterised in that the password (PW) is the key for a symmetrical encryption process.

29. An identification method according to claim 28 characterised in that the password (PW) is the key for a symmetrical encryption process between the instance and the identification instance.

30. An identification method according to claim 28 or claim 29 characterised in that the key decrypts and/or certifies a public key produced by the instance.

31. An identification method according to claim 30 characterised in that the public key is used for the communication between the instance and the identification instance.

32. An identification method according to claim 30 or claim 31 characterised in that the public key is associated with a private key of the instance, which is contained in an encryption device in such a way that it cannot be read out.

33. An identification method according to one of claims 19 to 32 characterised in that the identification instance encrypts and/or decrypts items of information with a symmetrical encryption method.

34. An identification method according to one of claims 19 to 32 characterised in that the identification

instance encrypts and/or decrypts items of information with an asymmetrical encryption method.

35. An identification method according to one of claims 19 to 34 characterised in that the password (PW) is transmitted to at least one further instance.

36. An identification method according to one of claims 19 to 35 characterised in that the information containing the account details is transmitted with a first password (PW1) and the identification instance produces a second password (PW2) and transmits it to the account details.

37. An identification method according to one of claims 19 to 36 characterised in that the plausibility of the information containing the account details is checked.

38. An identification method according to one of claims 19 to 37 characterised in that the instance is a user (C).

39 An identification method according to claim 38 characterised in that the financial standing of the user (C) is checked prior to transmission of the first password (PW1) and/or the second password (PW2).

40. An identification method according to claim 38 or claim 39 characterised in that the key can be used for decryption and/or transmission of a biometric identification feature produced by the user (C).

41. An identification method according to one of claims 38 to 40 characterised in that the first password (PW1) and/or the second password (PW2) can be called up by the user (C).

42. An identification method according to one of claims 38 to 41 characterised in that the user (C) transmits his account details together with a telephone number of a telephone he uses, in particular a mobile telephone, to the identification instance, and that the password (PW) transmitted to the user represents a secret call number which the user (C) must call for enablement purposes.

43. An identification method according to one of claims 38 to 41 characterised in that the user (C) transmits his account details together with a telephone number of a telephone and a password (PW) to the identification instance, wherein the password (PW) transmitted to the identification instance is the telephone number of the telephone.

44. An identification method according to one of claims 19 to 43 characterised in that the instance to be identified determines a fresh password after call-up of the password (PW1) and/or the second password (PW2).

45. An identification method according to claim 44 characterised in that the fresh password replaces the password or the second password.

Fig. 1

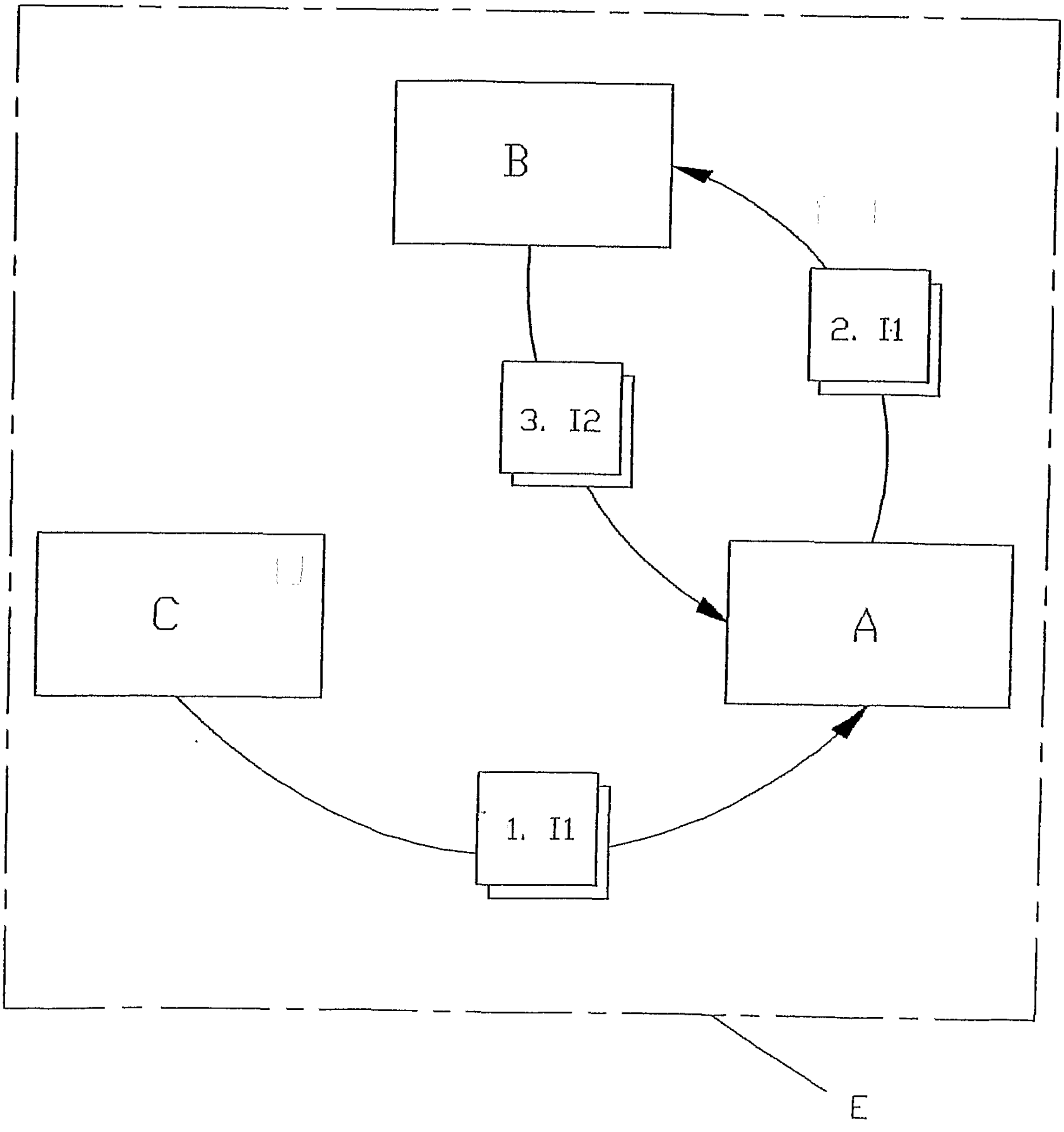


Fig. 2

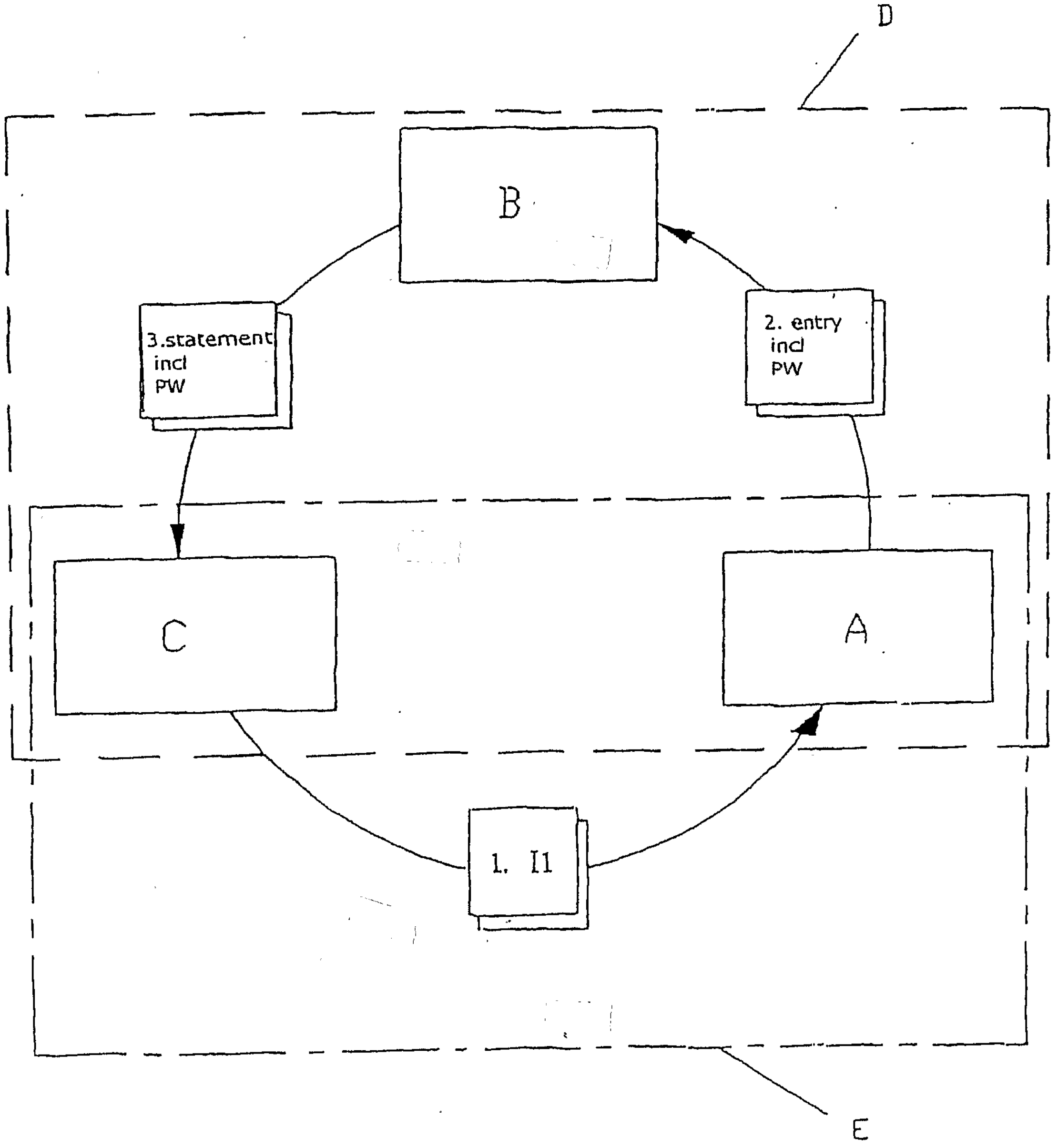


Fig. 3

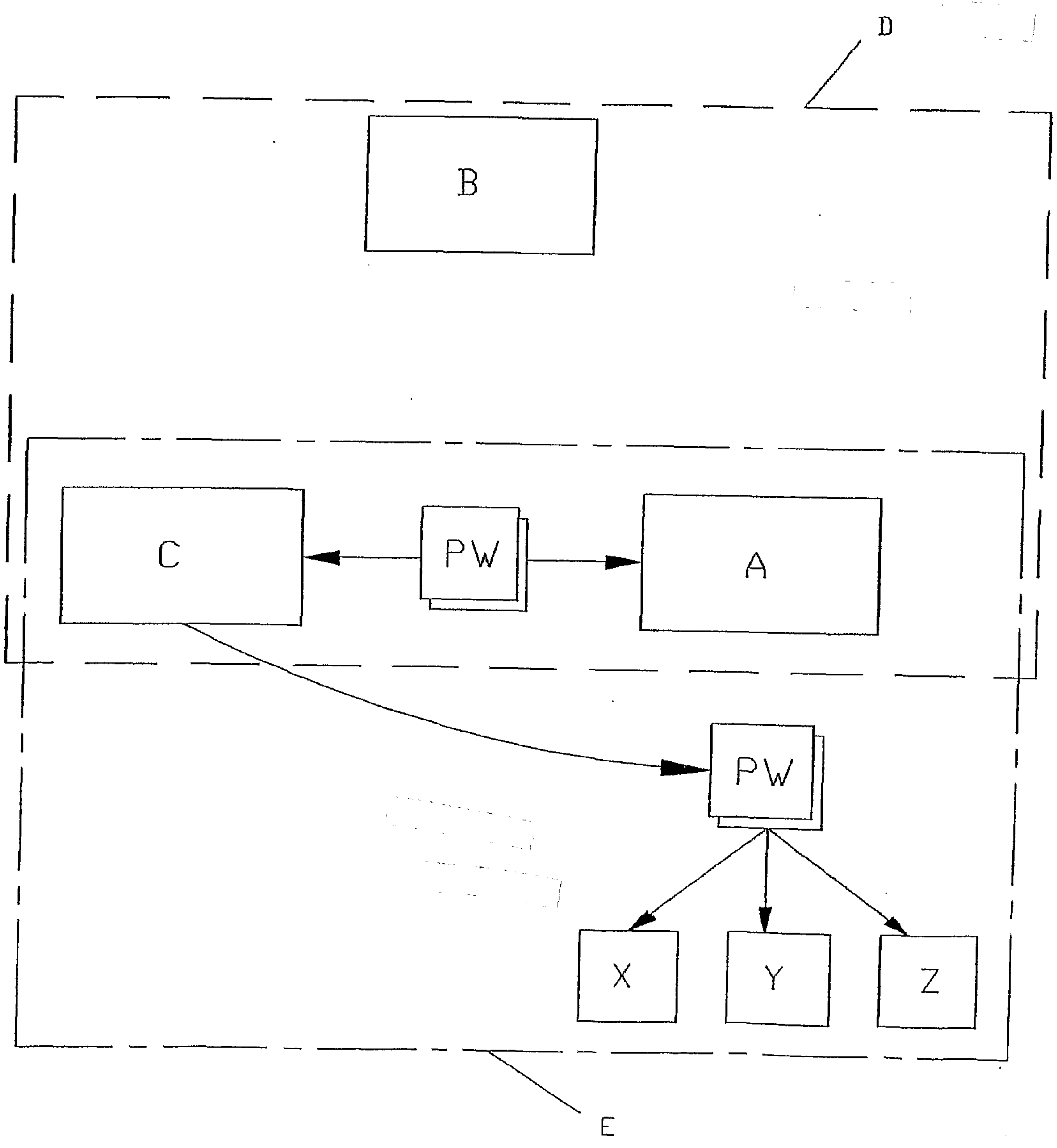


Fig. 4

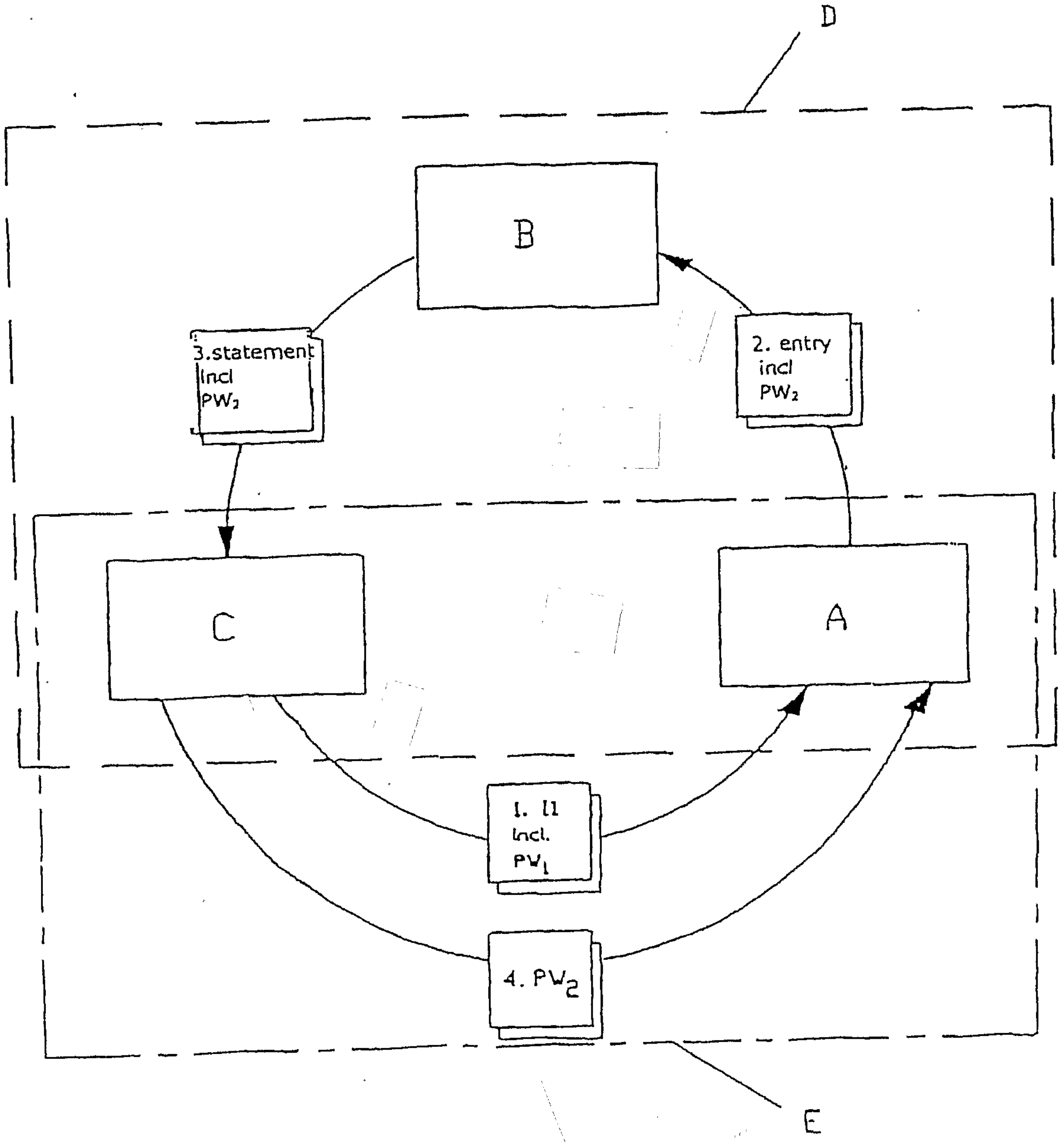
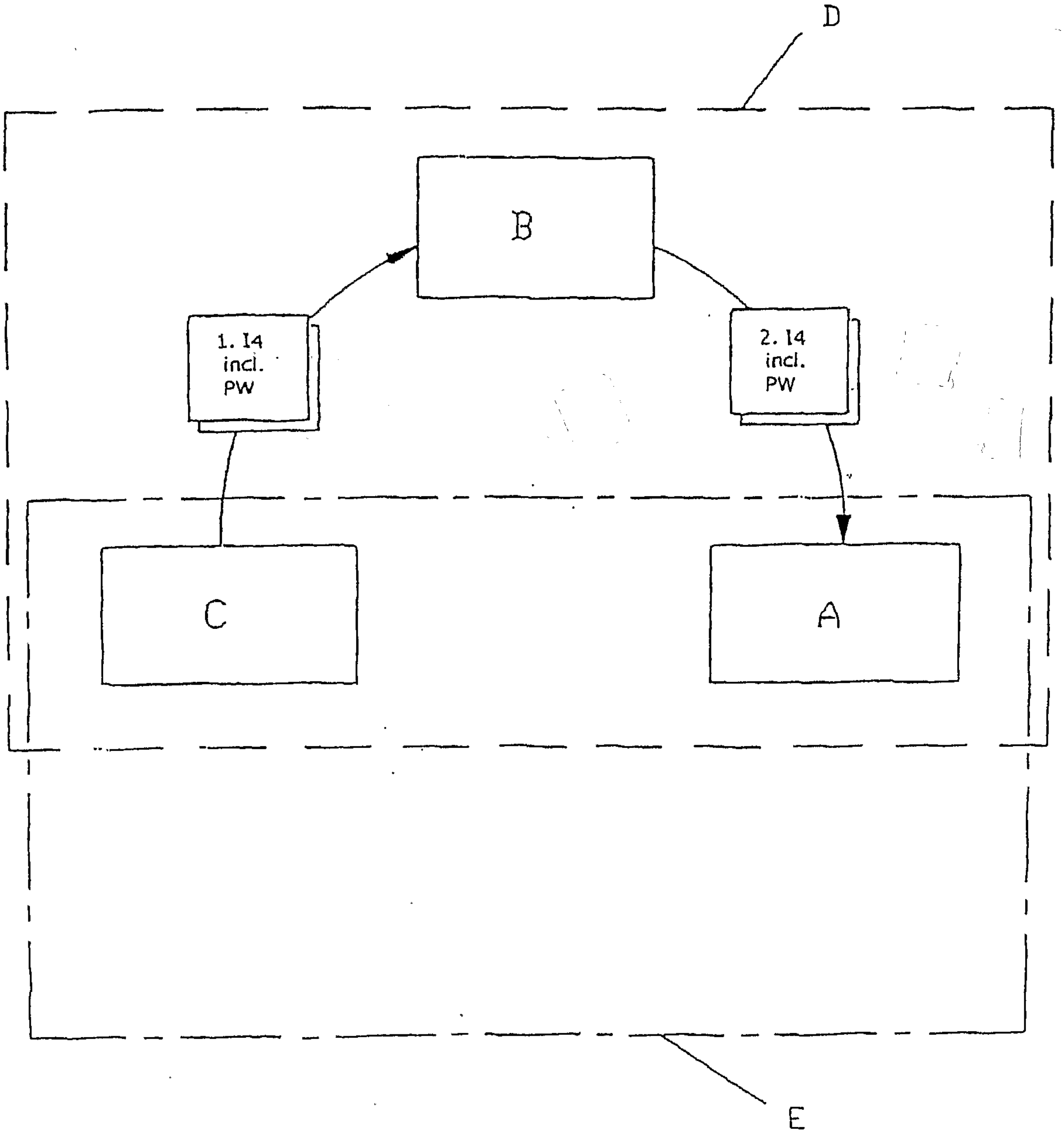


Fig. 5


D
B
1. I4
incl.
PW
2. I4
incl.
PW
C
A
E