

(12) **UK Patent Application** (19) **GB** (11) **2 366 056** (13) **A**

(43) Date of A Publication 27.02.2002

(21) Application No **0020219.2**

(22) Date of Filing **16.08.2000**

(71) Applicant(s)
Link Information Systems Limited
(Incorporated in the United Kingdom)
Bedford Heights, Manton Lane, BEDFORD, MK41 7PA,
United Kingdom

(72) Inventor(s)
Aidan Raphael Cartwright
Martin Geoffrey Scovell
Paul David Mustoe
John Philip Salton

(74) Agent and/or Address for Service
Haseltine Lake & Co
Imperial House, 15-19 Kingsway, LONDON,
WC2B 6UD, United Kingdom

(51) INT CL⁷
G07F 19/00

(52) UK CL (Edition T)
G4H HTG H1A H13D H14A
U1S S1727 S2124

(56) Documents Cited
GB 2331825 A **GB 2264377 A**

(58) Field of Search
UK CL (Edition R) **G4H HTG**
INT CL⁷ **G07F**

(54) Abstract Title
Verifying identities

(57) Apparatus for verifying the identity of an entity comprises a database storing, for each of a plurality of entities, identification information for identifying the entity, and verification information for verifying the identity of the entity. This information can be used for verifying the identities of both parties to a commercial transaction, e.g. an EPOS transaction or electronic commerce over the Internet, by comparison with information (e.g. ID and PIN) sent.

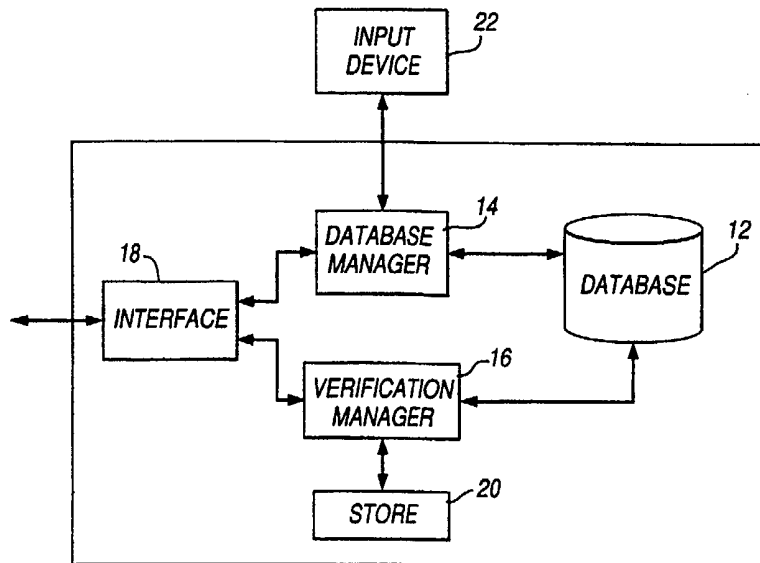


Fig.1

GB 2 366 056 A

1/6

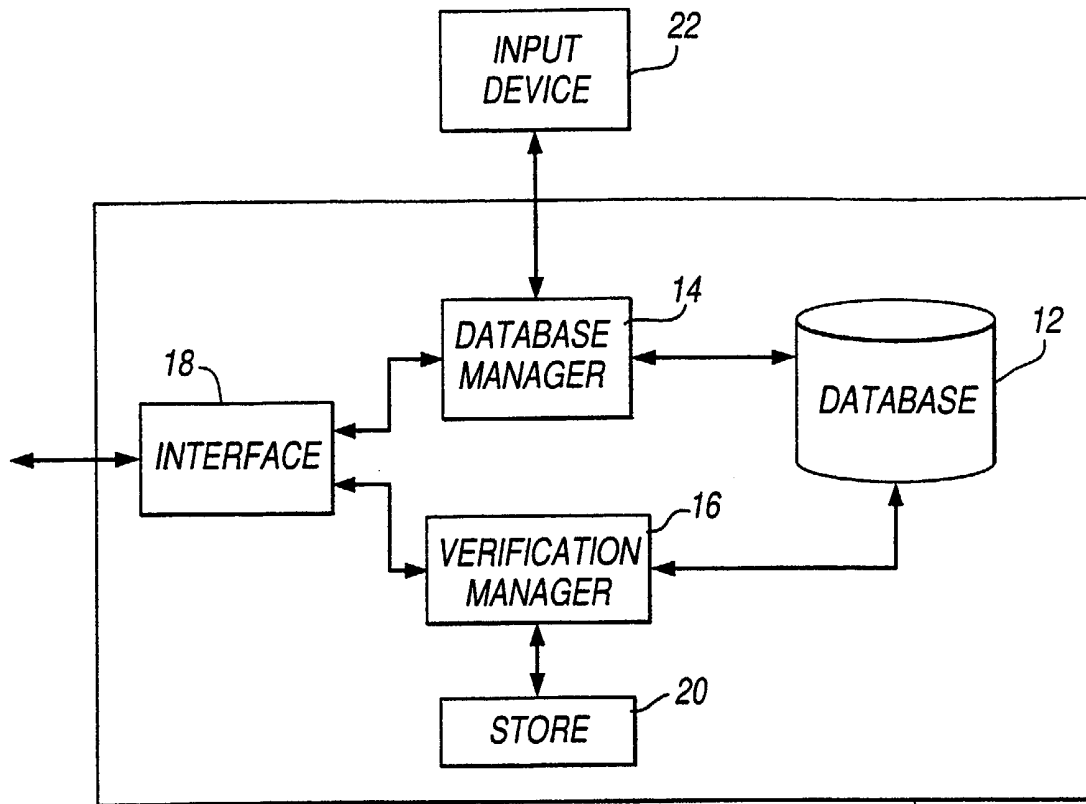


Fig. 1

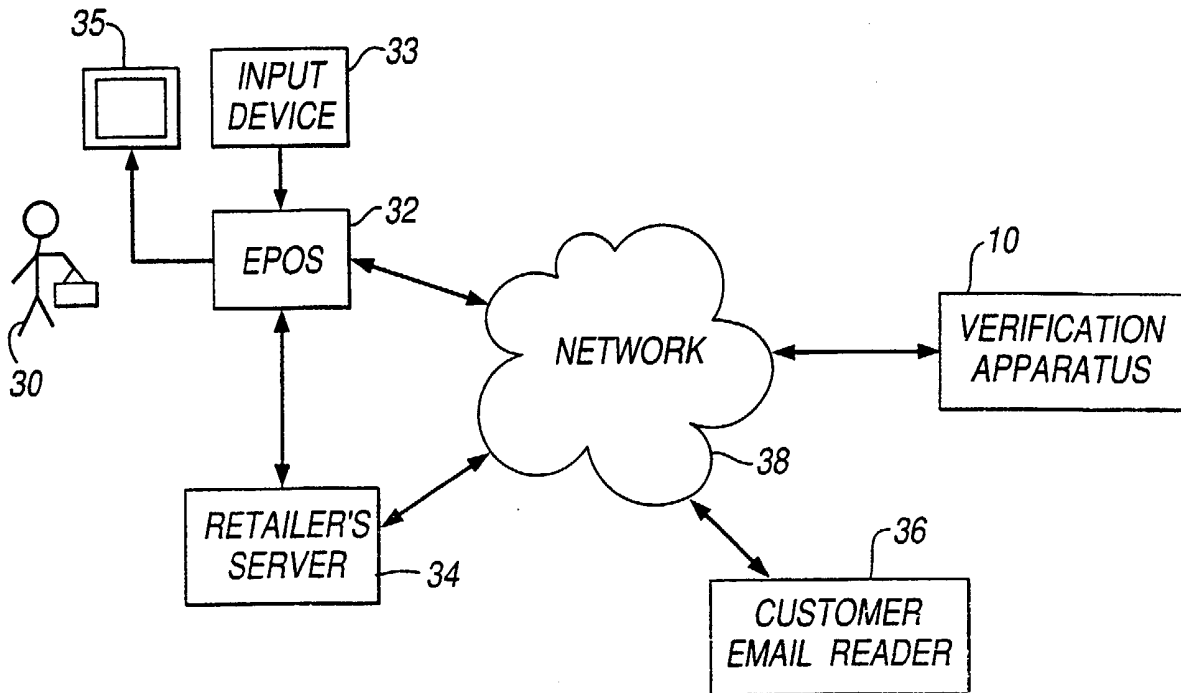


Fig. 2

FIG. 2

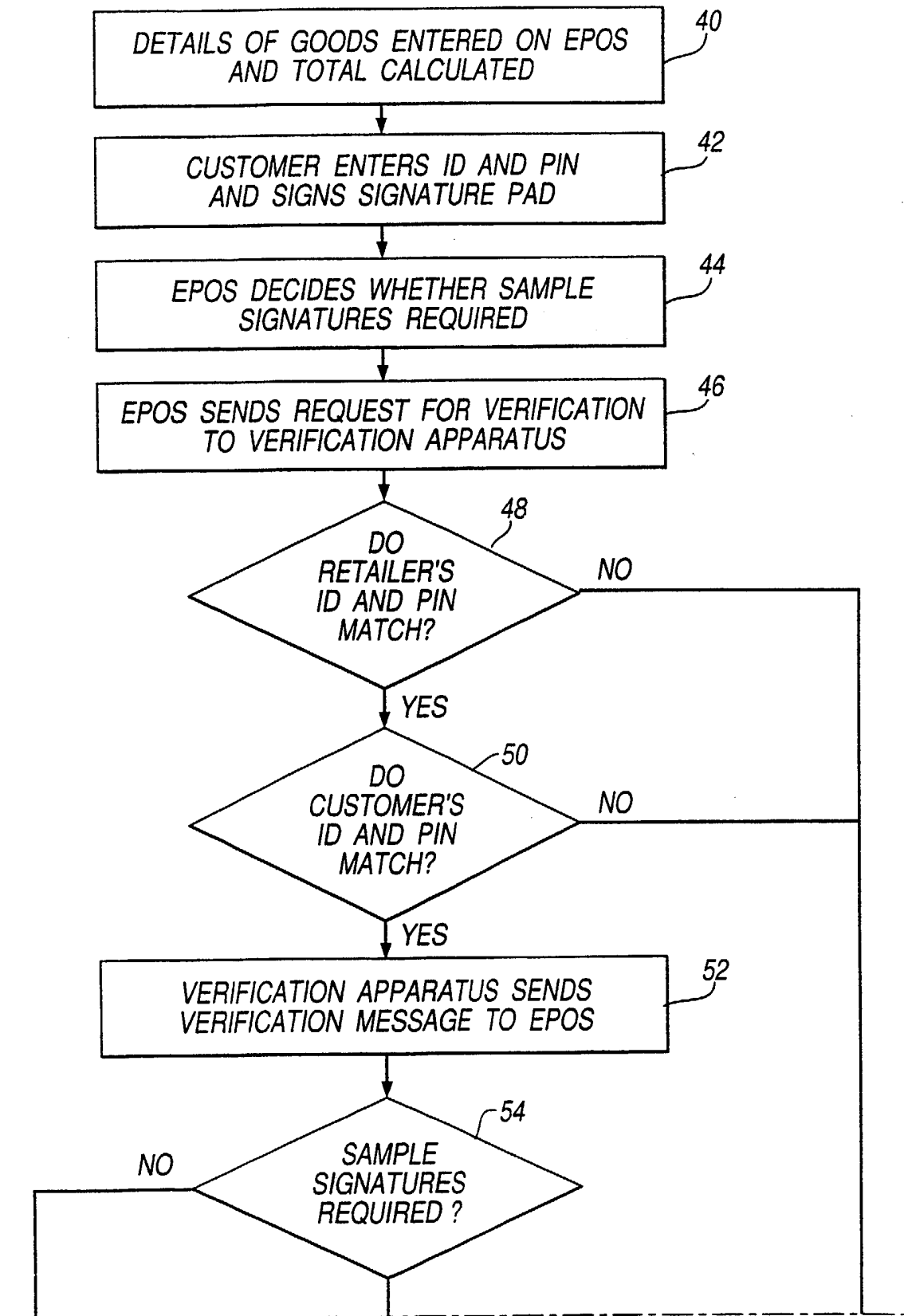


Fig.3A

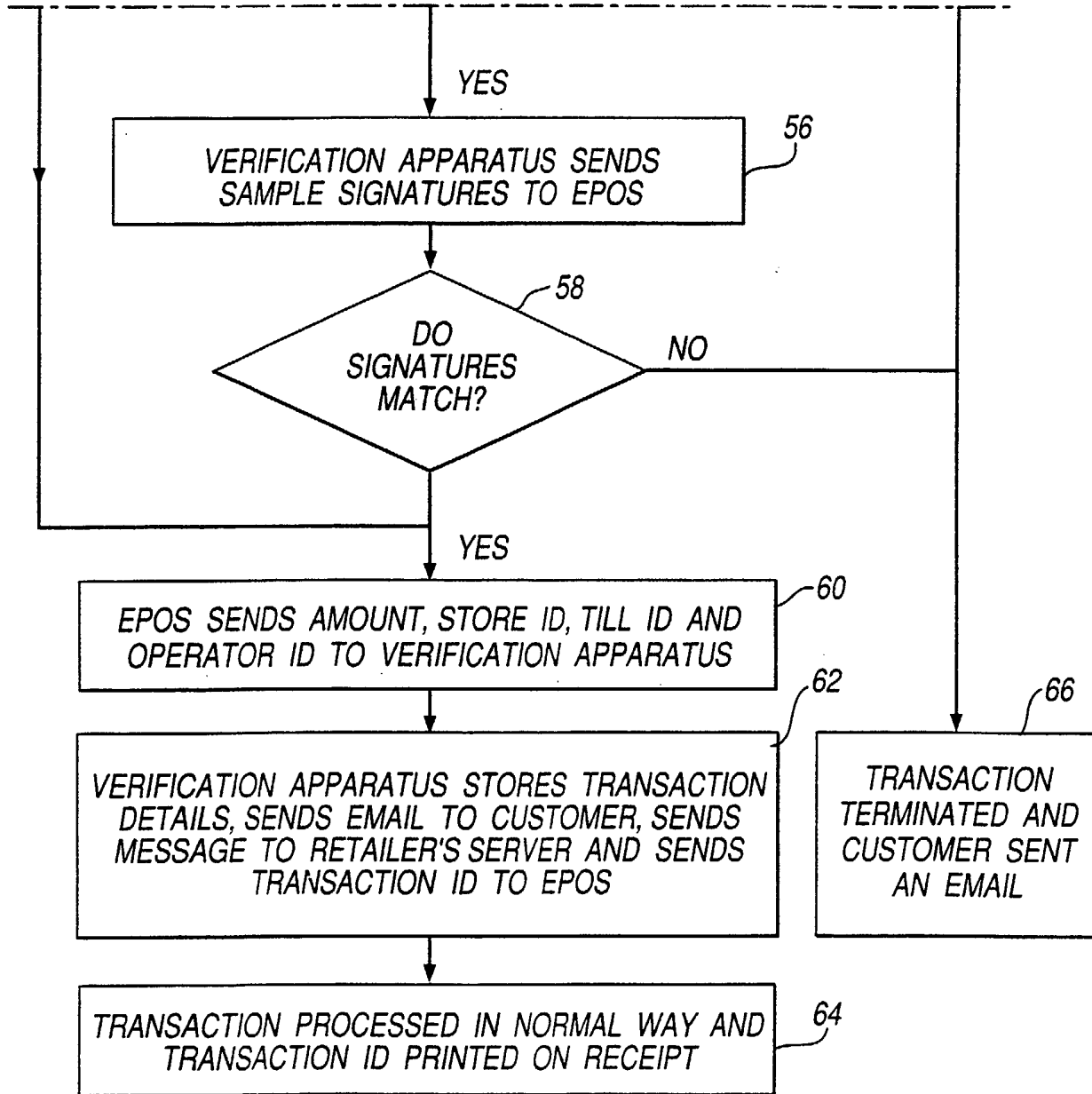


Fig.3B

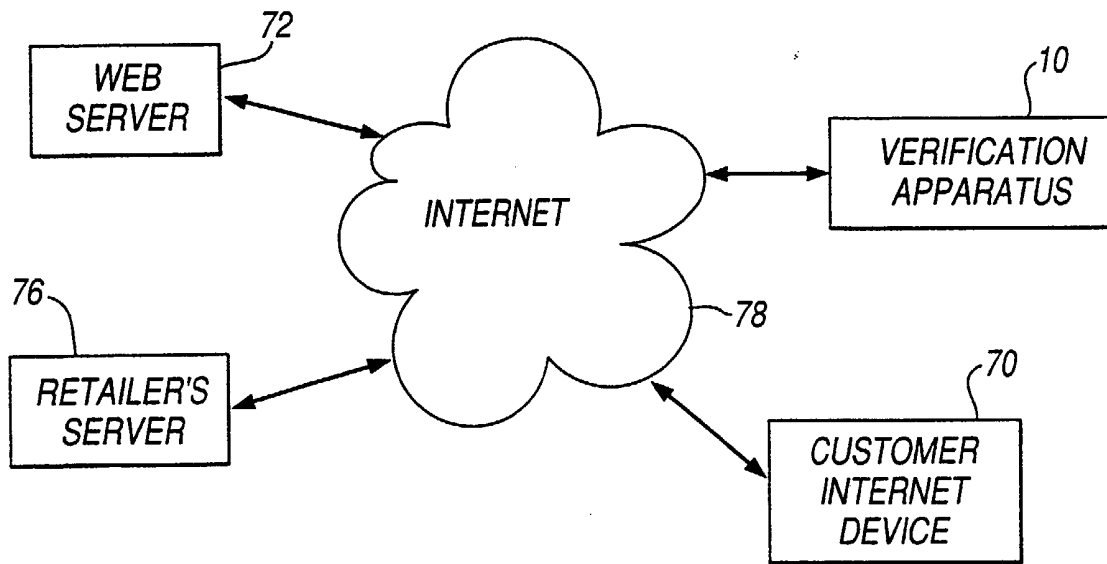


Fig.4

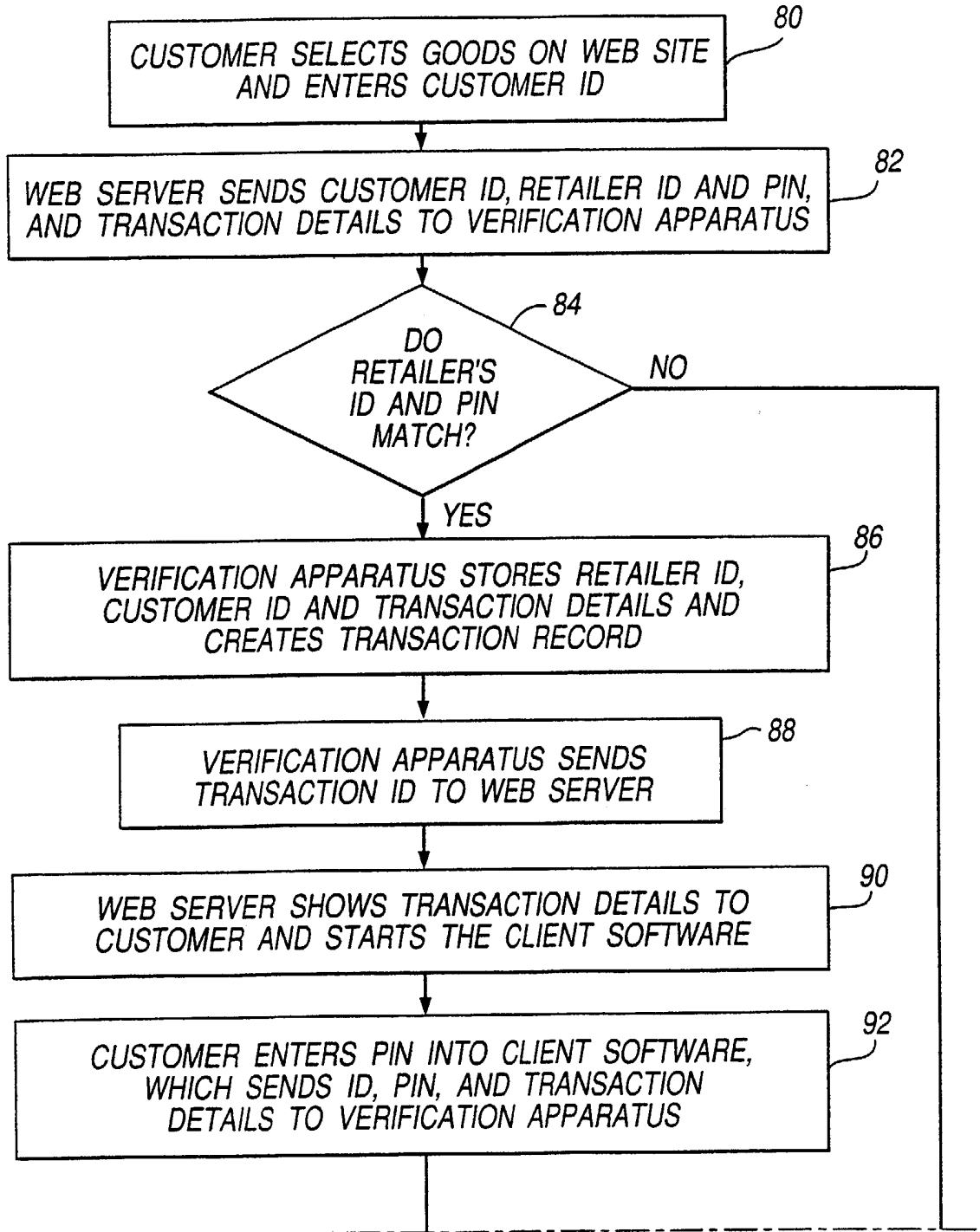


Fig.5A

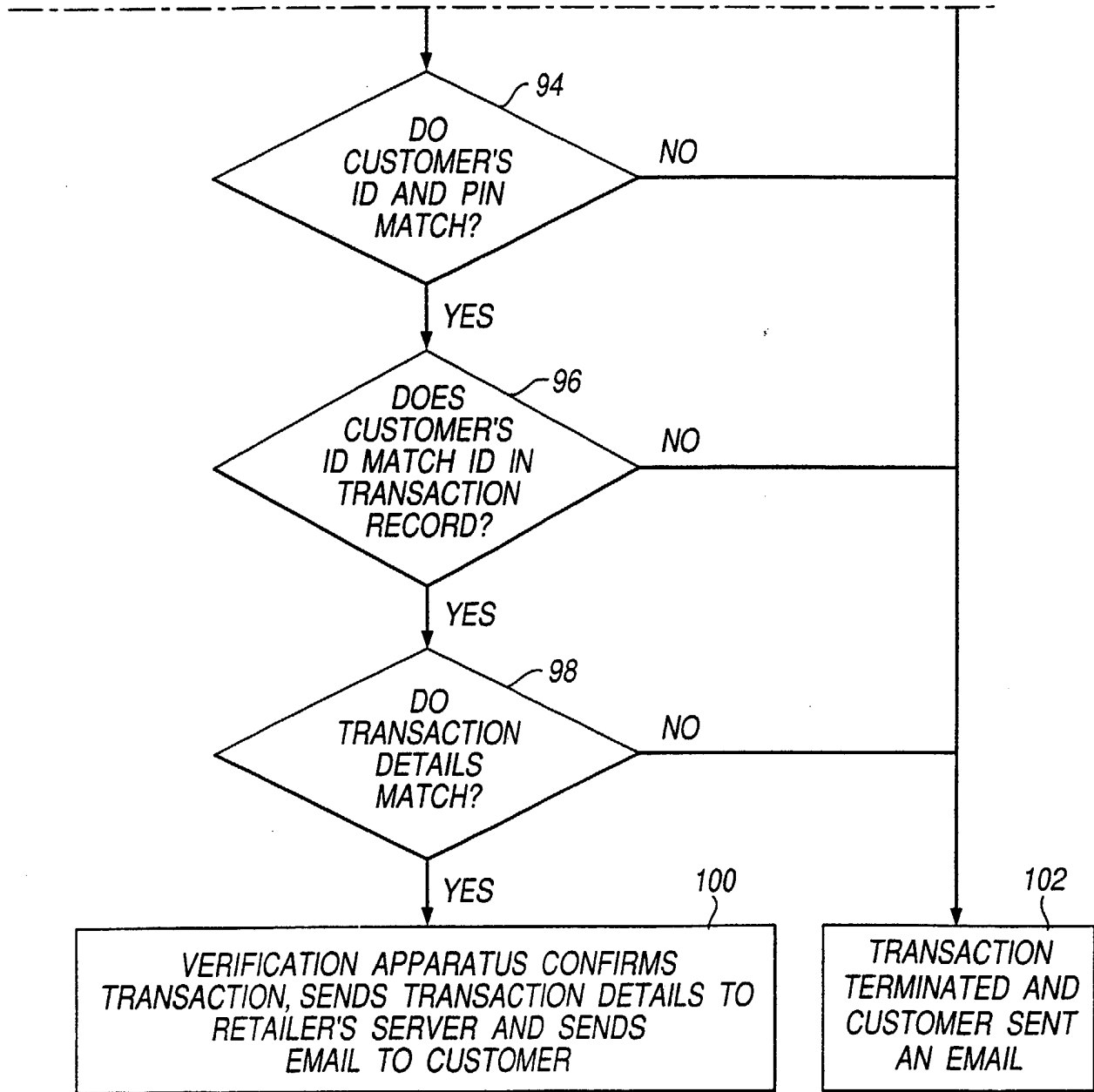


Fig.5B

APPARATUS FOR AND METHODS OF VERIFYING IDENTITIES

The invention relates to apparatus for and methods of verifying the identity of an entity, such as an individual or a company. The invention has particular (but not exclusive) application in the verification of parties to a retail or an electronic commerce (e-commerce) transaction, to enable the transaction to be authorised.

In known systems for authorising transactions, a party to the transaction maintains its own database of entities which have previously registered with that party. The entities may be, for example, individuals, companies or other organizations.

As an example, if a company offers goods or services via the Internet, the company may require that customers to whom the goods or services are to be supplied first register with the company. When an customer registers with the company, the customer is assigned a unique identification code (referred to herein as an "ID") and a password. The company maintains a database which stores the IDs and passwords of all customers which are registered with the company. If a customer wishes to purchase a product from the company, the customer sends his ID and password to the company via the Internet. The company is able to verify the identity of the customer by checking that the customer is registered and that the password matches the password held in the database for the customer.

A problem in the system described above is that, while the system offers some level of security to the company, it offers little security to the customer,

since the customer is not able to verify the identity of the company. Furthermore, the company must maintain a database of all customers with their IDs and passwords, which may be expensive and time consuming.

5 In addition, the requirement for new customers to register with the company, together with the lack of security for the customer, may discourage customers from purchasing from the company. Also, if a customer is to obtain goods or services from a number of
10 companies, he may be required to register with all those companies, which may be cumbersome and time consuming for the customer, especially if he/she has chosen a different password for each different company.

15 According to a first aspect of the present invention there is provided apparatus for verifying the identity of an entity, comprising:

a database comprising, for each of a plurality of entities, identification information for identifying
20 the entity, and verification information for verifying the identity of the entity;

means for receiving a request from a first entity, being one of the plurality of entities, for verification of the identity of a second entity, being
25 another of the plurality of entities;

means for receiving identification information and verification information relating to the second entity;

means for determining whether the received identification information and verification information
30 match identification information and verification information relating to the second entity stored in the database; and

means for issuing, in dependence on an output from the determining means, an indication to the first
35 entity of whether the identity of the second entity is verified.

By providing a database comprising identification information and verification information, and means for allowing the identity of an entity to be verified, and either or both parties to a transaction may verify the identity of the other party before the transaction is carried out. The apparatus may receive requests from a plurality of entities for the verification of the identity of a single entity. Thus the invention avoids the need for an entity to register with a plurality of other entities, since in effect an independent repository of identification and verification information is provided which may be accessed by all entities that are registered therewith. Furthermore, an entity (such as a company) does not need to maintain its own database of identification information of other entities (such as customers), since the independent database may be used for verification.

The database may be an database running on a single server, or it may be a distributed database running on a plurality of servers. The database may be physically stored on one or more computer storage devices. In the case of a distributed database, the servers may be of different types using different platforms running different database engines, communicating using common threads and methods.

The apparatus may further comprise means for receiving identification information and verification information relating to the first entity, and means for determining whether the received identification information and verification information relating to the first entity match identification information and verification information relating to the first entity stored in the database. In this way, the identity of the first

entity may be verified before any information is issued to the first entity, which increases the security of the apparatus.

5 In one implementation, the identification information and verification information relating to the second entity are received from the first entity. For example, the identification information and verification information relating to the second entity
10 could be sent as part of the request. This might be appropriate where, for example, the second entity (such as an individual) is physically present with the second entity (such as a retailer) so that the second entity is able to pass its identification information and
15 verification information directly to the second entity without risk of interception.

In another implementation, the identification information relating to the second entity is received
20 from the first entity, and the verification information is received separately. This might be appropriate where the first and second entities are physically remote from each other. In this case, the second entity might pass its identification information to the
25 first entity so that the first entity can request verification of the identity of the second entity, and the second entity might pass its verification information directly to the verification apparatus. In this way, the second entity does not pass both its
30 identification information and verification information to the first entity, which increases the security of the system. Furthermore, an indication of the fact that the identity of the first entity has been verified may be sent to the second entity, for example by email,
35 giving added security to the second entity.

The apparatus may further comprise means for issuing an indication to the second entity that the request has been received. In this way, the second entity is informed that its identity has been checked, and if the second entity's identity has been used fraudulently, the second entity is warned.

The database may include distinctive information relating to at least the second entity, and the apparatus may further comprise means for sending distinctive information relating to the second entity to the first entity. The distinctive information may comprise, for example, a digital version of a signature, a photograph, a fingerprint, a voice sample or a retina image. In this way a further check on the identity of the second entity may be carried out. For example, where the second entity is an individual, a photograph sent by the verification apparatus could be visually compared with the appearance of the individual, or a signature which has been transmitted could be compared with a signature provided by the individual, or automatic recognition software could be used.

The apparatus may be apparatus for verifying the identities of parties to a transaction, in which case the apparatus may further comprise means for storing details of the transaction. The apparatus may also comprise means for sending the details of the transaction to a party to the transaction. In this way, a record of transactions may be kept, which may allow transactions to be reported and audited at a later date.

The invention extends to apparatus for use by the first entity in conjunction with the apparatus described

above, and therefore in a second aspect of the invention there is provided apparatus for use by a first entity in the verification of the identity of a second entity, comprising:

- 5 means for receiving identification information and verification information relating to the second entity;
- means for transmitting a request for verification of the identity of the second entity to a verification apparatus;
- 10 means for transmitting to the verification apparatus identification information and verification information relating to the second entity; and
- means for receiving an indication from the verification apparatus that the identity of the second
- 15 entity is verified by the verification apparatus.

This aspect of the invention allows the first entity to verify the identity of the second entity by receiving information such as an ID and PIN from the second

20 entity, and then checking that the second entity has registered with the verification apparatus and that the ID and PIN correspond.

The apparatus may further comprise means for indicating

25 that the identity of the second entity has been verified, such as a visual display or an audible indication, or the fact that the identity of the second entity has been confirmed may be implicit, for example because a transaction is allowed to continue.

30 The apparatus may be, for example, an electronic point-of-sale (EPOS) device for processing a transaction. In this case, the apparatus may be adapted only to process a transaction if the identity of the second entity is

35 verified.

Preferably the apparatus further comprises means for transmitting to the verification apparatus identification information and verification information relating to the first entity. In this way, the identity of the first entity may be verified before any information is issued to the first entity, which increases the security of the system.

The apparatus may further comprise means for receiving from the verification apparatus distinctive information relating to the second entity. The distinctive information may comprise, for example, a digital version of a signature, a photograph, a fingerprint or a retina image. In this way a further check on the identity of the second entity may be carried out. For example, where the second entity is an individual, a photograph sent by the verification apparatus could be visually compared with the appearance of the individual. Alternatively the apparatus may further comprise means for comparing the distinctive information received from the verification apparatus with corresponding information input by the second entity. The comparing means may be, for example, a processor programmed with software that can compare signatures, or facial images or retina images, or fingerprints. In this case the apparatus may include means for receiving the corresponding distinctive information, such as a signature pad which captures and digitizes a signature for further processing, or a digital camera for capturing a facial image or a retina image.

In either of the above aspects of the invention, the apparatus is preferably adapted to communicate over a distributed network such as the Internet, although it may be used with other networks such as an intranet or

a purpose built network.

The invention has particular (but not exclusive)
application in e-commerce, and thus in a third aspect
of the invention there is provided a web server which,
when in use, provides a web site for carrying out
transactions over the Internet, the web site
comprising:

means for proposing a transaction to an Internet
device;

means for receiving an acceptance of the
transaction from the Internet device;

means for receiving identification information
identifying a user of the Internet device;

means for sending the identification information
identifying the user to a verification apparatus;

means for receiving from the verification
apparatus an indication of whether the user's identity
has been verified; and

means for carrying out the transaction in
dependence on the indication of whether the user's
identity has been verified.

In this way, security may be enhanced in online
transactions, since the identity of the user of the
Internet device may be verified by reference to an
independent repository of verification information.

The transaction may involve any type of interaction
between the two parties; for example it might involve
the supply of goods or services by the web site to the
user of the Internet device, or some form of
communication or dissemination of information between
the two parties.

Preferably the web site further comprises means for

sending identification information identifying the web site and verification information verifying the identity of the web site to the verification apparatus. In this way, the identity of the web site provider may also be verified, giving extra security to the user of the web site and encouraging use of the web site.

The web site may further comprise means for sending details of the transaction to the verification apparatus. The verification apparatus may then keep a record of transactions for reporting or auditing at a later date.

The invention extends to an Internet device when suitably programmed for use with a web site as described above, and thus in a fourth aspect of the invention there is provided an Internet device adapted to carry out transactions via the Internet, the Internet device comprising:

means for sending an acceptance of a proposed transaction to a web site provided by a web server;

means for sending identification information identifying a user of the Internet device to the web site;

means for receiving from the user of the Internet device verification information verifying the identity of the user;

means for sending the verification information to a verification apparatus;

means for receiving an indication of whether the transaction has been processed; and

means for indicating to the user whether the transaction has been processed.

In this way the user of the Internet device may carry out a transaction with a web site (for example the

purchase of goods or services) without having
previously registered with that web site. The web site
is able to verify the identity of the user by reference
to an independent repository of information, thus
5 making it unnecessary for the user to pre-register with
the web site.

The Internet device may be any device that can send and
receive over the Internet and run appropriate software,
10 for example a personal computer, a WAP (Wireless
Application Protocol) telephone, or a digital
television with an Internet box. The Internet device
may have a screen for displaying information to a user
and/or means for producing audible sounds for passing
15 information to the user. Information may be input by
the user to the Internet device via a keyboard, a key
pad, a writing recognition pad, a mouse, a remote
control unit, or any other suitable device.

20 Preferably, in order to increase the security for the
user, the web site's identification is also verified by
the verification apparatus. Thus the Internet device
may further comprise means for receiving from the
verification apparatus an indication of whether the web
25 site's identification has been verified. The Internet
device may further comprise means for aborting the
transaction in dependence on the indication of whether
the web site's identification has been verified. For
example, the indication may be communicated to the
30 user, and the user may abort the transaction if the web
site's identification has not been verified, or the
transaction may be aborted automatically if the web
site's identification has not been verified.

35 The Internet device may further comprise means for
indicating to the user that the transaction has been

processed. The indication that the transaction has been processed may include details of the transaction. This may allow the user of the Internet device to keep a record of transactions. The Internet device may also
5 comprise means for requesting details of transactions from the verification apparatus, and means for receiving such details. This may allow the user to analyse transactions at a later date.

10 In any of the aspects described above, the various means may be software modules running on an appropriate processor.

The invention also provides corresponding method
15 aspects. Thus the invention may provide a method of verifying the identity of an entity comprising:

storing in a database, for each of a plurality of entities, identification information for identifying the entity, and verification information for verifying
20 the identity of the entity;

receiving a request from a first entity, being one of the plurality of entities, for verification of the identity of a second entity, being another of the plurality of entities;

25 receiving identification information and verification information relating to the second entity;

determining whether the received identification information and verification information match identification information and verification information relating to the second entity stored in the database;
30 and

issuing, in dependence on the determining step, an indication to the first entity of whether the identity of the second entity is verified.

35

Other method aspects corresponding to the various

apparatus, web server and Internet device aspects described above may also be provided within the scope of the invention.

5 The invention is preferably implemented in the form of computer programs running on suitable processors. Thus the invention may provide a computer program which, when run on a computer that is connected to the Internet, causes the computer to provide a web site for
10 carrying out transactions over the Internet, the program comprising:

a program portion for proposing a transaction to an Internet device;

15 a program portion for receiving an acceptance of the transaction from the Internet device;

a program portion for receiving identification information identifying a user of the Internet device;

20 a program portion for sending the identification information identifying the user to a verification apparatus;

a program portion for receiving from the verification apparatus an indication of whether the user's identity has been verified; and

25 a program portion for carrying out the transaction in dependence on the indication of whether the user's identity has been verified.

The invention may also provide a computer program which, when run on a computer that is connected to the
30 Internet, causes the computer to function as an Internet device for carrying out transactions via the Internet, the program comprising:

35 a program portion for sending an acceptance of a proposed transaction to a web site provided by a web server;

a program portion for sending identification

information identifying a user of the Internet device to the web site;

5 a program portion for receiving from the user of the Internet device verification information verifying the identity of the user;

a program portion for sending the verification information to a verification apparatus;

a program portion for receiving an indication of whether the transaction has been processed; and

10 a program portion for indicating to the user whether the transaction has been processed.

The invention also extends to computer programs which, when run on a computer, would cause the computer to
15 function as an apparatus as described above, or a web server as described above, or an Internet device as described above. The invention also extends to a computer program or a computer program product for carrying out any of the methods described herein, or a
20 computer readable medium having stored thereon a computer program for carrying out any of the methods described herein.

25 Features of one aspect may be applied to any other aspect where appropriate; apparatus features may be applied to method aspects and *vice versa*.

30 Preferred features of the present invention will now be described, purely by way of example, with reference to the accompanying drawings, in which:-

Figure 1 shows a verification device embodying the invention;

35 Figure 2 shows a verification system according to a first embodiment of the invention;

Figure 3 illustrates the operation of the first

embodiment of the invention;

Figure 4 shows a verification system according to a second embodiment of the invention; and

5 Figure 5 illustrates the operation of the second embodiment of the invention.

Referring to Figure 1, a verification apparatus 10 embodying the invention is shown. The verification apparatus 10 provides an independent repository of
10 identification and verification information, so that the identity of entities registered with the apparatus can be verified. Entities registered with the apparatus may be individuals, companies or other organisations or undertakings.

15 The verification apparatus 10 comprises a relational database 12 which stores information relating to each of a plurality of entities. For each entity the database stores identification information,
20 verification information, and, optionally, distinctive information. Identification information may include information such as the name, address and email address of the entity, and an ID number. Verification
25 information may include information such as a password or a PIN (personal identification number) number. This information is kept secret by the entity and is used in verifying the identity of the entity. The verification information may be encrypted for transmission and when stored in the database 12, for added security.
30 Distinctive information may include a signature, a photograph, a fingerprint, a voice sample, a retina image, or other forms of biometric information. The distinctive information may be used as a further check on the identity of the entity. The type of information
35 stored in each category need not be the same for all entities.

The verification apparatus 10 also comprises an interface 18 which interfaces the verification apparatus to a network such as the Internet, a database manager 14 which manages the database in response to requests to update the database, a verification manager 16, which manages verification requests, and a store 20 which stores details of transactions.

When an entity, for example an individual or company, first registers with the verification apparatus 10, the entity passes information about itself to the verification apparatus through a secure source. The information includes details of the entity such as name, address and email address, and information which can be used to verify the entity's identity, such as a password, a signature or a photograph. This information may be input through input device 22, or via interface 18. Input device 22 may include, for example, a keyboard, and/or a scanner for converting an image, such as a signature or a photograph, into a digitized version of the image, and/or an analogue-to-digital converter for converting analogue information such as a voice sample into digital form. The identity of the entity may be checked, for example against an electoral register in the case of an individual or a company register in the case of a company. Database manager 14 may assign further identification information or verification information to the entity; for example the database manager may assign an ID number and a PIN number to the entity. The database manager 14 then updates the database with the information relating to the entity.

In operation, if a first party wishes to verify the identity of a second party, the first party sends a request for verification to the verification apparatus

10. The request is received by the interface 18 and passed to the verification manager 16. The request must include both identification information and verification information relating to the first party, and at least identification information relating to the second party. When a request is received, the verification manager 16 first checks the identity of the first party, that is, the party making the request. This is done by consulting the database 12 to check that the identification information and the verification information relating to the first party are correct. If they are not correct, then the verification manager 16 sends a warning to the entity whose identity has been used, and the verification process is halted.

Once the identity of the first party has been confirmed, verification of the second party can be carried out. If the verification request included both identification information and verification information relating to the second party, then the identity of the second party can be checked immediately by consulting the database 12. If only identification information relating to the second party was present, then the verification manager sends a request for verification information. This request may either be sent to the second party directly, or to the first party, if it is believed that the first party has this information available, for example because the second party is physically present with the first party. In response to this request, verification information relating to the second party is sent to the verification apparatus and is received by the verification manager 14. The verification manager then consults the database 12 to check that the identification information and the verification information relating to the second party

are correct.

5 If the identification information and verification
information relating to the second party are correct,
then a message confirming the identity of the second
party is sent to the first party. If the information
is not correct, then a message indicating that the
identity of the second party has not been confirmed is
sent to the first party, and a warning is also sent to
10 the entity whose identity has been used.

If requested by the first party, distinctive
information, such as a photograph, signature or voice
sample, may also be sent by the verification apparatus
15 to the first party to allow the first party to carry
out a further check on the identity of the second
party. The first party may manually compare the
distinctive information sent by the verification
apparatus with a sample of the distinctive information
20 submitted by the second party to the first party, or an
automatic comparison could be carried out using
automatic recognition software, such as signature
recognition, voice recognition or image recognition
software.

25 A first embodiment of a verification system will now be
described with reference to Figure 2. The verification
system of the first embodiment is designed to operate
within a retail environment. Referring to Figure 2,
30 the customer 30 is an individual who is registered with
the verification apparatus 10. In this embodiment it
is assumed that the customer has submitted sample
signatures to the verification apparatus, and that he
has been assigned an ID number and a PIN number. The
35 ID may be taken from his credit card, chip card or
similar device.

The retailer is equipped with an electronic point of sale (EPOS) device 32. The EPOS 32 may take the form of an electronic cash register, a personal computer or another similar device comprising a digital processor. The EPOS 32 is provided with an input device 33 for receiving information from the customer. The input device may be, for example, a keypad, a signature tablet for capturing a signature, a microphone for capturing a voice sample, or any other suitable input device. Additional input devices may be provided where required. The input devices may be internal or external to the EPOS 32. The EPOS 32 also has a screen 35 for displaying information such as a signature or a photograph; the screen may be either external or integral with the EPOS. The EPOS 32 may be provided with software which can compare signatures, finger prints, voice samples or other forms of biometric information. The EPOS 32 is also provided with software that enables a secure TCP/IP (Transport Control Protocol/Internet Protocol) socket connection with the verification apparatus 10 via the Internet. The file layouts and the method of connection of the EPOS 32 are such as to enable it to communicate with the verification apparatus 10. In this embodiment, the EPOS 32 also has an ID and a PIN number that are registered with the verification apparatus 10.

Retail server 34 is a server which in this embodiment links several EPOS tills together. Retail server 34 processes transactions involving the retailer's financial systems and also processes credit card payments and other types of electronic payments.

The verification apparatus 10 in this embodiment is a computer of appropriate resources (memory, capacity,

speed etc.) to suit the environment in which it is running. It is able to communicate with other computers and devices using TCP/IP. The verification apparatus may be implemented as a single server, or as
5 a plurality of servers all running as part of a distributed database.

The customer's email reader 36 is a device such as a personal computer, a personal organizer or a mobile
10 telephone that is able to read email. The email reader may be designed to use the SMTP (Simple Mail Transfer Protocol) system.

Figure 3 is a flow chart illustrating operation of the
15 first embodiment of the verification system. It is assumed that the customer has selected his goods as he would normally in a retail environment. In step 40, the prices, and optionally other details of the goods, are entered on the EPOS 32. This may be done, for
20 example, by manually entering the details, or by scanning the goods and referring to a stock database on the retailer's server. The goods are totalled by the EPOS as they would normally be.

25 In step 42, the customer enters his ID number and his PIN number into EPOS 32 and signs a signature pad. The ID number may be entered on a keypad, or the ID number may be entered automatically using a device such as a payment card, chip card or identity card. In either
30 case, the PIN is entered by the customer manually. In step 44 it is decided whether the retailer requires samples of the customer's signatures for additional verification of the customer's identity. This may be decided automatically by the EPOS 32, for example if
35 the total value of the goods is above a predetermined amount, or the cashier may decide whether additional

verification is required, in which case the cashier
inputs the decision to the EPOS manually in response to
a prompt from the EPOS. In alternative embodiments
additional verification may be by means of a photograph
5 or a fingerprint or other distinctive information.

In step 46 the EPOS 32 sends a request for verification
of the customer's identity to the verification
apparatus 10. The request includes the retailer's ID
10 and PIN number and the customer's ID and PIN. The
request also includes an indication of whether the
retailer requires additional verification of the
customer's identity, and the type of verification that
is required, for example signature, photograph, voice
15 sample or finger print.

In response to the request, in step 48 the verification
apparatus 10 verifies that the retailer's ID and PIN
match, thus confirming that the retailer is registered
20 with the verification apparatus, giving the customer
added confidence about the identity of the retailer. If
the retailer's ID and PIN do not match, the transaction
is aborted and an email is sent to the customer (step
66). An email may also be sent to the retailer whose
25 identity was used. In step 50 the verification
apparatus 10 verifies that the customer's ID and PIN
match. If the customer's ID and PIN do not match, the
transaction is aborted and an email is sent to the
customer and other designated parties (step 66).

30

If the both the retailer's ID and PIN and the
customer's ID and PIN do match, then in step 52 the
verification apparatus sends a message to the EPOS 32
confirming the identity of the customer.

35

In step 54 the verification apparatus 10 checks whether

samples of the customer's signature (or other distinctive information) are required by the retailer for additional verification of the customer's identity. If the retailer does required additional verification, then in step 56 the verification apparatus sends the appropriate information, such as one or more digitized samples of the customer's signature, to the EPOS 32. In step 58, the distinctive information is compared with a sample of the distinctive information submitted by the customer. For example, if a sample signature is sent, then in step 58 it is determined whether the sample signatures match the signature that the customer has entered on the signature pad. This may be done either by visual comparison, or the signatures may be compared automatically using a signature comparison program running on the EPOS 32. If the signatures do not match, the transaction is terminated and an email is sent to the person whose ID and PIN were used informing them that there may have been an attempt to use their identity fraudulently (step 66). If the signatures match, the transaction continues.

Distinctive information other than a signature may be used in the verification. For example the verification apparatus may store a voice sample of the customer speaking a password, and this could be sent on request to the EPOS 32. The customer may then speak the password into a microphone at the EPOS. The EPOS then digitizes the spoken password and compares it with the voice sample sent by the verification apparatus using voice recognition software to check the identity of the customer.

In step 60 the EPOS 32 sends the store ID, the till ID and the operator ID to the verification apparatus 10. Optionally, details of the type of purchase are also

sent. This information is stored by the verification apparatus, and may be used at a later date, for example, to provide an analysis of expenses to the customer.

5

In step 62 the verification apparatus 10 stores the transaction details and sends a transaction ID to the EPOS to give an audit trail of the transaction. A message is sent to the retailer's server (if present) and an email is sent to the customer informing him of the transaction.

10

In step 64 the transaction is completed in the normal way, and the transaction ID is added to the customer's receipt. The customer is thus provided with a transaction ID that matches the details that were sent to the customer by email, and the details stored at the verification apparatus.

15

20

Step 66 is carried out if the transaction is terminated for any reason. In step 66 the customer is sent an email informing him of the reason why the transaction was aborted, or warning him that they may have been an attempt to use his identity fraudulently. Since the customer is always sent an email when his identification is used, the customer will be informed of any fraudulent use of his credit cards etc.

25

30

A second embodiment of a verification system will now be described with reference to Figure 4. The verification system of the second embodiment is designed to operate within an e-commerce environment over the Internet. Referring to Figure 4, the customer's Internet device 70 is a device that is able to communicate over the Internet and has the ability to send and receive information. For example, the

35

Internet device 70 might be a personal computer, a WAP (Wireless Application Protocol) telephone, a digital television with an Internet box (set-top box), or any other suitable data processing device. Typically the Internet device runs commercially available Internet browser software such as Internet Explorer supplied by Microsoft or Navigator supplied by Netscape. Specially designed client software is also installed on the Internet device 70.

Web server 72 is any type of computer that is capable of connection to the Internet and hosting applications that run over it. In this embodiment web server 72 hosts the retailer's web site. The retailer's web site allows goods or services to be purchased over the Internet.

Verification apparatus 74 is a server having appropriate resources (memory, capacity, speed etc.) to suit the environment in which it is running. It is able to communicate with other devices via the Internet. Details of registered entities are held in a database appropriate to the platform that the server runs. The server may in practice be several servers all running as part of a distributed database.

The retailer's server 76 is a computer that processes transactions in the retailer's financial systems and also processes credit card or other types of payment.

Operation of the second embodiment will now be described with reference to Figure 5. In step 80 the customer uses his Internet device 70 to select goods that he wishes to purchase on the retailer's web site, under control of the web site. The customer also enters his ID, which is sent to the web site.

In step 82 the web server sends the customer's ID, the retailer's ID and PIN, and details of the transaction (such as the amount) to the verification apparatus. In step 84 the verification apparatus checks whether the retailer's ID and PIN are valid. If they are not the transaction is aborted and an email sent to the customer (step 102). If the retailer's ID and PIN are valid then the transaction continues.

10 In step 86 the verification apparatus stores the retailer's ID, the customer's ID and the details of the transaction and creates a transaction record. The transaction record includes a transaction ID and other details of the transaction, such as the customer ID.
15 The transaction record is used to ensure that the transaction stays the same during the process of the transaction. This stops the transaction being altered or interfered with. In step 88 the verification apparatus sends the transaction record to the web
20 server.

In step 90 the web server shows the transaction details to the customer and starts the client software running on the customer's Internet device. In step 92, the customer enters his PIN using the client software. The client software then sends the customer ID (entered in step 80) and PIN, and the transaction details (as shown to the customer) to the verification apparatus.

30 In step 94 the verification apparatus checks whether the customer's ID and PIN are valid. If they are not the transaction is aborted and an email sent to the person whose ID was used warning him that an attempt may have been made to use his identity fraudulently
35 (step 102). If the customer's ID and PIN are valid then the transaction continues.

In step 96 the verification apparatus checks that the customer ID sent by the client software in the customer's Internet device matches the customer ID in the transaction record, in order to check that the right transaction is being used. If the two customer IDs do not match, the transaction is terminated and the customer is sent an email (step 102). If they do match, the transaction continues.

10 In step 98 the verification apparatus checks that the transaction details sent by the customer match the transaction details sent by the web server, to ensure that nothing has been altered. If the details vary, the transaction is terminated and an email is sent to the customer (step 102), and a message is sent to the web site. If the details match, the transaction continues.

20 In step 100 the verification apparatus sends a message to the web server confirming the transaction, sends an email to the customer confirming that the transaction has taken place, and sends details of the transaction to the retailer's server.

25 Step 102 is carried out if the transaction is terminated for any reason. In step 102 the customer is sent an email informing him of the reason why the transaction was aborted, or warning him that they may have been an attempt to use his identity fraudulently. A message may also be sent to the web site identifying the reason for the termination.

35 The functions described above with reference to the first and second embodiments may be implemented using software written in any appropriate programming language. The programming of such software will be

apparent to the skilled person from the above descriptions of the various functions.

5 It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

10 Although the invention has been illustrated with reference to specific examples of transactions taking place in a retail environment and via the Internet, the invention is not limited to these situations, and may be used in any situation where it is desired to verify the identity of an entity. For example, the invention
15 may be used for purposes such as identification for legal or financial matters, for voting or for document verification, for drugs allocation, or for fraud prevention such as social security fraud prevention. The invention may also be used for holding records such
20 as proof of purchase, proof of work done, guarantees or warrantees, or as an intermediary for bill paying or ticket allocation, or for registered email.

25 The invention is also not limited to use with the Internet, but may be used with any form of network such as an Intranet (private network), a local area network, or any form of distributed network.

30 The present invention may be embodied in a computer program. The computer program may be stored on a computer-readable medium, or it could, for example, be in the form of a signal such as a downloadable data signal provided from an Internet web site. The
35 appended computer program claims are to be interpreted as covering a computer program by itself, or as a record on a carrier, or as a signal, or in any other

form.

Each feature disclosed in the description, and (where
appropriate) the claims and drawings may be provided
5 independently or in any appropriate combination.

CLAIMS

1. Apparatus for verifying the identity of an entity, comprising:

5 a database comprising, for each of a plurality of entities, identification information for identifying the entity, and verification information for verifying the identity of the entity;

10 means for receiving a request from a first entity, being one of the plurality of entities, for verification of the identity of a second entity, being another of the plurality of entities;

means for receiving identification information and verification information relating to the second entity;

15 means for determining whether the received identification information and verification information match identification information and verification information relating to the second entity stored in the database; and

20 means for issuing, in dependence on an output from the determining means, an indication to the first entity of whether the identity of the second entity is verified.

25 2. Apparatus according to claim 1, further comprising means for receiving identification information and verification information relating to the first entity, and means for determining whether the received identification information and
30 verification information relating to the first entity match identification information and verification information relating to the first entity stored in the database.

35 3. Apparatus according to claim 1 or 2 wherein the identification information and verification

information relating to the second entity are received from the first entity.

5 4. Apparatus according to claim 1 or 2 wherein the identification information relating to the second entity is received from the first entity, and the verification information is received separately.

10 5. Apparatus according to any of the preceding claims further comprising means for issuing an indication to the second entity that the request has been received.

15 6. Apparatus according to any of the preceding claims wherein the database includes distinctive information relating to at least the second entity, and the apparatus further comprising means for sending distinctive information relating to the second entity to the first entity.

20 7. Apparatus according to any of the preceding claims, being apparatus for verifying the identities of parties to a transaction, and further comprising means for storing details of the transaction.

25 8. Apparatus according to claim 7 further comprising means for sending the details of the transaction to a party to the transaction.

30 9. Apparatus for use by a first entity in the verification of the identity of a second entity, comprising:

 means for receiving identification information and verification information relating to the second entity;

35 means for transmitting a request for verification of the identity of the second entity to a verification

apparatus;

means for transmitting to the verification apparatus identification information and verification information relating to the second entity; and

5 means for receiving an indication from the verification apparatus that the identity of the second entity is verified by the verification apparatus.

10 10. Apparatus according to claim 9, the apparatus being an electronic point-of-sale device for processing a transaction, wherein the transaction is only processed if the identity of the second entity is verified.

15 11. Apparatus according to claim 9 or 10 further comprising means for transmitting to the verification apparatus identification information and verification information relating to the first entity.

20 12. Apparatus according to any of claims 9 to 11 further comprising means for receiving from the verification apparatus distinctive information relating to the second entity.

25 13. Apparatus according to claim 12 further comprising means for comparing the distinctive information received from the verification apparatus with corresponding information input by the second entity.

30 14. Apparatus according to any of the preceding claims being adapted to communicate over a distributed network.

35 15. A web server which, when in use, provides a web site for carrying out transactions over the

Internet, the web site comprising:

means for proposing a transaction to an Internet device;

5 means for receiving an acceptance of the transaction from the Internet device;

means for receiving identification information identifying a user of the Internet device;

means for sending the identification information identifying the user to a verification apparatus;

10 means for receiving from the verification apparatus an indication of whether the user's identity has been verified; and

means for carrying out the transaction in dependence on the indication of whether the user's identity has been verified.

15

16. A web server according to claim 15, wherein the web site further comprises means for sending identification information identifying the web site and verification information verifying the identity of the web site to the verification apparatus.

20

17. A web server according to claim 15 or 16, wherein the web site further comprises means for sending details of the transaction to the verification apparatus.

25

18. An Internet device adapted to carry out transactions via the Internet, the Internet device comprising:

30

means for sending an acceptance of a proposed transaction to a web site provided by a web server;

means for sending identification information identifying a user of the Internet device to the web

35

site;

means for receiving from the user of the Internet

device verification information verifying the identity of the user;

means for sending the verification information to a verification apparatus;

5 means for receiving an indication of whether the transaction has been processed; and

means for indicating to the user whether the transaction has been processed.

10 19. An Internet device according to claim 18 further comprising means for receiving from the verification apparatus an indication of whether the web site's identification has been verified.

15 20. An Internet device according to claim 19 further comprising means for aborting the transaction in dependence on the indication of whether the web site's identification has been verified.

20 21. An Internet device according to any of claims 18 to 20 further comprising means for indicating to the user that the transaction has been processed.

25 22. An Internet device according to claim 21 wherein the indication that the transaction has been processed includes details of the transaction.

30 23. An Internet device according to any of claims 18 to 22 further comprising means for requesting details of transactions from the verification apparatus, and means for receiving such details

24. A method of verifying the identity of an entity comprising:

35 storing in a database, for each of a plurality of entities, identification information for identifying

the entity, and verification information for verifying the identity of the entity;

receiving a request from a first entity, being one of the plurality of entities, for verification of the identity of a second entity, being another of the plurality of entities;

receiving identification information and verification information relating to the second entity;

determining whether the received identification information and verification information match identification information and verification information relating to the second entity stored in the database; and

issuing, in dependence on the determining step, an indication to the first entity of whether the identity of the second entity is verified.

25. A computer program which, when run on a computer that is connected to the Internet, causes the computer to provide a web site for carrying out transactions over the Internet, the program comprising:

a program portion for proposing a transaction to an Internet device;

a program portion for receiving an acceptance of the transaction from the Internet device;

a program portion for receiving identification information identifying a user of the Internet device;

a program portion for sending the identification information identifying the user to a verification apparatus;

a program portion for receiving from the verification apparatus an indication of whether the user's identity has been verified; and

a program portion for carrying out the transaction in dependence on the indication of whether the user's identity has been verified.

26. A computer program which, when run on a computer that is connected to the Internet, causes the computer to function as an Internet device for carrying out transactions via the Internet, the program comprising:

5 a program portion for sending an acceptance of a proposed transaction to a web site provided by a web server;

10 a program portion for sending identification information identifying a user of the Internet device to the web site;

a program portion for receiving from the user of the Internet device verification information verifying the identity of the user;

15 a program portion for sending the verification information to a verification apparatus;

a program portion for receiving an indication of whether the transaction has been processed; and

20 a program portion for indicating to the user whether the transaction has been processed.

27. A computer program which, when run on a computer, causes the computer to function as an apparatus according to any of claims 1 to 14, or a web server according to any of claims 15 to 17, or an Internet device according to any of claims 18 to 23.

26. A computer program or a computer program product for carrying out any of the methods described herein, or a computer readable medium having stored thereon a computer program for carrying out any of the methods described herein.

27. A method or apparatus substantially as described herein with reference to the accompanying drawings.



Application No: GB 0020219.2
Claims searched: 1,24 & appendancies

Examiner: Mike Davis
Date of search: 2 November 2000

Patents Act 1977 Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): G4H (HTG)

Int Cl (Ed.7): G07F

Other:

Documents considered to be relevant:

| Category | Identity of document and relevant passage | Relevant to claims |
|----------|---|--------------------|
| A | GB 2331825 A (NEC) eg abstract | - |
| A | GB 2264377 A (DAHURA) eg abstract | - |

| | | | |
|---|---|---|--|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |