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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2339564 A1 2002/09/05

(21) 2 339 564

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2001/03/05

(41) Mise à la disp. pub./Open to Public Insp.: 2002/09/05

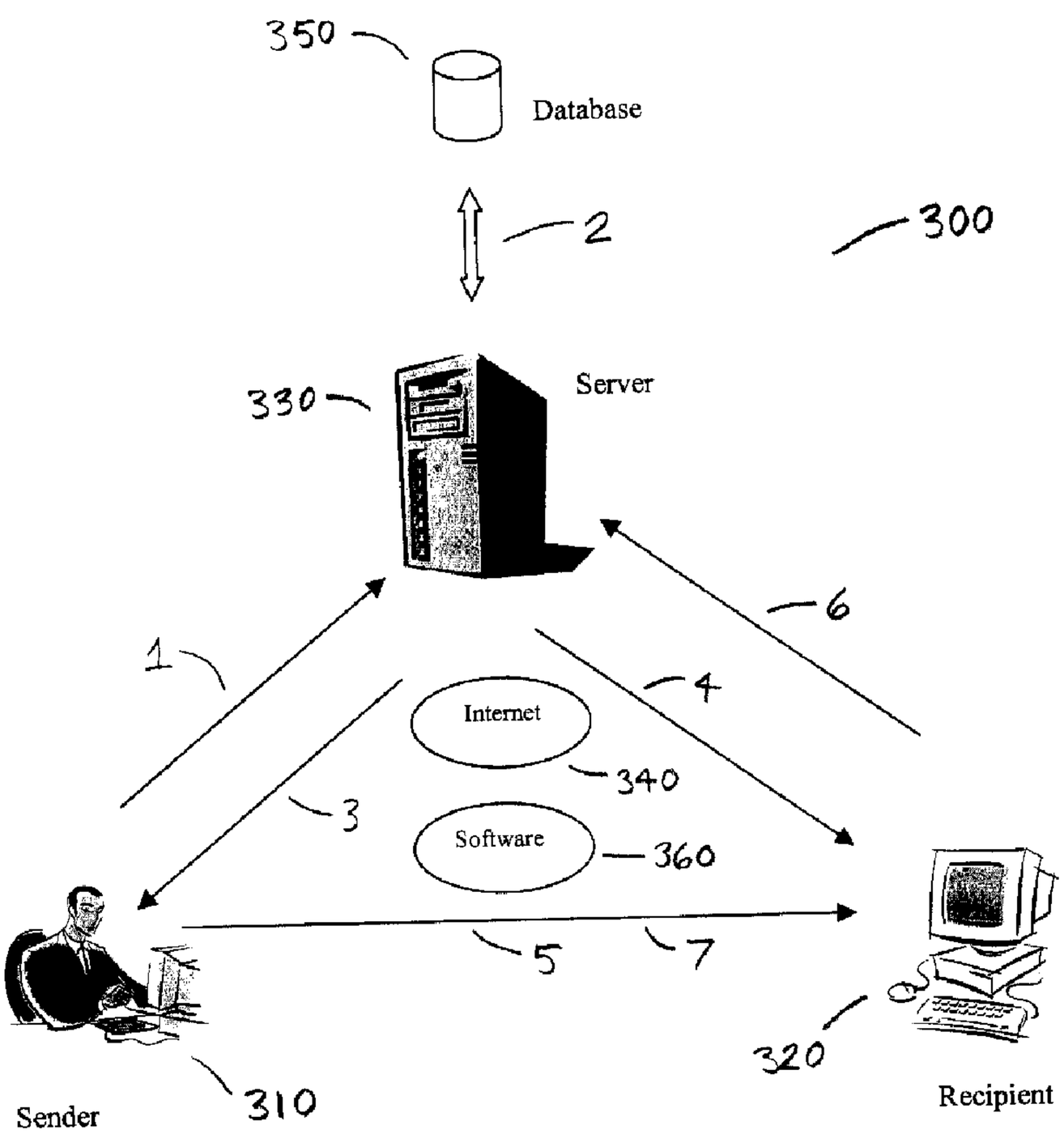
(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 9/00, H04L 9/32

(71) Demandeurs/Applicants:
WIEBE, DAVID PAUL, CA;
WILLIAMS, WHITNEY, CA

(72) Inventeurs/Inventors:
WIEBE, DAVID PAUL, CA;
WILLIAMS, WHITNEY, CA

(74) Agent: FASKEN MARTINEAU DUMOULIN LLP

(54) Titre : METHODE ET SYSTEME DE CHIFFREMENT DES MESSAGES NUMERIQUES
(54) Title: A METHOD AND SYSTEM FOR ENCRYPTING DIGITAL MESSAGES



(57) Abrégé/Abstract:
In data processing system that executes a program of instructions and that includes a sender client, a recipient client, a server, a plurality of databases, and a plurality of interconnections, a method of message encryption and transmission comprising the steps of requesting a Digital ID on behalf of a recipient from a server by a sender, creating a Digital ID by the server, transmitting

CA 2339564 A1 2002/09/05

(21) 2 339 564

(13) A1

(57) Abrégé(suite)/Abstract(continued):
the Digital ID to the sender from the server, transmitting a first message to the recipient from the server informing the recipient that the sender has initiated the creation of a Digital ID for the recipient thereby enabling the sender and said recipient to exchange encrypted messages, transmitting the Digital ID to the recipient from the server, encrypting a second message by the sender using the recipient's Digital ID and sending the encrypted second message directly to the recipient, receiving the encrypted second message from the sender by the recipient and decrypting the encrypted second message by the recipient using the Digital ID.

ABSTRACT

In data processing system that executes a program of instructions and that includes a sender client, a recipient client, a server, a plurality of databases, and a plurality of interconnections, a method of message encryption and transmission comprising the steps of requesting a Digital ID on behalf of a recipient from a server by a sender, creating a Digital ID by the server, transmitting the Digital ID to the sender from the server, transmitting a first message to the recipient from the server informing the recipient that the sender has initiated the creation of a Digital ID for the recipient thereby enabling the sender and said recipient to exchange encrypted messages, transmitting the Digital ID to the recipient from the server, encrypting a second message by the sender using the recipient's Digital ID and sending the encrypted second message directly to the recipient, receiving the encrypted second message from the sender by the recipient and decrypting the encrypted second message by the recipient using the Digital ID.

A METHOD AND SYSTEM FOR ENCRYPTING DIGITAL MESSAGES

The invention relates to the field of data processing systems. More specifically, the invention relates to message encryption and transmission.

BACKGROUND OF THE INVENTION

Most businesses take steps or put procedures in place to ensure the confidentiality and security of physical documents they deal with. For example, such documents may be locked in file cabinets, have restricted access, or be protected by code words. However, in many cases, these same businesses may use no safeguards whatsoever when transmitting confidential documents over the Internet by email or by another form of electronic or digital messaging. Typically, protection is provided for email through the use of encryption. Sending confidential documents over the Internet by email, without encryption protection, is tantamount to mailing those documents without an envelope. However, more than 95% of emails are currently sent unencrypted. This is so despite the fact that encryption capability, based on the defacto SMIME (Secure Multi-Purpose Internet Mail Extension) and X.509 (i.e. X.509 v3 Public Key Certificates under RFC 2459) standards, is built into many of today's most popular email programs including Microsoft's Outlook and Outlook Express, Netscape's Messenger, and Lotus's cc:Mail.

Encryption is not used to the extent that it could be because current email programs require the sender to obtain the recipient's public key or "Digital ID", as Microsoft refers to it. Very few email users today have such a Digital ID. In fact, the current process of

obtaining a Digital ID has been an impediment to widespread adoption of email encryption.

A Public Key Infrastructure (PKI), which forms the basis of present Internet encryption standards, is a system for allowing users to exchange information over an unsecure public network through the use of private and public key pairs in an asymmetric encryption system. The key pairs are obtained and shared through a trusted authority (i.e. Certificate Authority or CA). In public key encryption, it is the recipient's public key that determines the encryption algorithm and strength (e.g. key length). Without the sender having the recipient's Digital ID beforehand, encryption via PKI is not possible.

Currently available email encryption systems have several drawbacks. First, they often use a proprietary encryption method which requires both the sender and receiver to have special software for encryption and decryption. This special software is often not interoperable with the SMIME email encryption standard. Second, these systems often require a separate mail client (i.e. proprietary and non-SMIME compliant) for the sender and receiver as opposed to leveraging off of the installed based of common SMIME compliant mail clients such as Microsoft's Outlook and Outlook Express, Netscape's Messenger, and Lotus's cc:Mail. Third, the email message (including attachments) is not effectively encrypted in several of these systems. That is, while the email transmission may be encrypted, the email content itself is not. The result is that the email message may remain in an unencrypted form in both the sender's and recipient's computer systems. Fourth, encrypted messages are often forwarded to, stored on, and retrieved from a server located on the Internet, as opposed to going directly from the sender to the recipient. Finally, encryption is often password based (i.e. symmetric, private key) rather than

public key based (i.e. asymmetric). Again, asymmetric encryption is the defacto PKI standard which includes the use of secure and reliable digital certificates.

Several systems are known which circumvent or work around the PKI standard. In United States Patent Number 6,151,675 (Smith), a system is disclosed wherein documents are encrypted with the public key of a server associated with the recipient of the document instead of directly with the public key of the intended recipient. In United States Patent Number 6,041,123 (Colvin, Sr.), a secured central router with access to a master secure key (i.e. private key) database acts as a conduit for secured communications between senders and recipients by translating encrypted messages from senders for recipients using their respective secure keys. By doing so, the need for the exchange of public keys is essentially eliminated. A similar approach is evident in United States Patent Numbers 5,812,671 (Ross, Jr.), 5,781,632 (Odum), 5,768,391 (Ichikawa), and 5,751,813 (Dorenbos).

A need therefore exists for a method and system that will allow email senders to initiate and control the process of encryption, without any prior actions by the recipient, while using the PKI infrastructure and standards. In other words, there is a need for a method and system that will allow an email sender (i.e. Registration Authority in the PKI model) to obtain (i.e. from a Certificate Authority) a Digital ID on behalf of the email recipient. There is a further need for a method and system that is PKI based, wherein the actual message is encrypted, and neither the sender nor recipient require special additional software other than their existing SMIME compliant email program. Finally, there is a need for a method and system wherein the encrypted message is not stored and forwarded but rather is transmitted directly from the sender to the recipient and remains encrypted

on both the sender's and recipient's computer systems. The required method and system should facilitate other forms of electronic or digital messaging including voice, peer-to-peer, and instant messaging.

SUMMARY OF THE INVENTION

The invention provides a method and system for sending encrypted email. According to one aspect of the invention, a method is described that allows a sender to transmit encrypted email over the Internet following PKI standards but without prior knowledge of the recipient's public key. The method comprising the steps of requesting a Digital ID on behalf of a recipient from a server by a sender, creating a Digital ID by the server, transmitting the Digital ID to the sender from the server, transmitting a first message to the recipient from the server informing the recipient that the sender has initiated the creation of a Digital ID for the recipient thereby enabling the sender and said recipient to exchange encrypted messages, transmitting the Digital ID to the recipient from the server, encrypting a second message by the sender using the recipient's Digital ID and sending the encrypted second message directly to the recipient, receiving the encrypted second message from the sender by the recipient and decrypting the encrypted second message by the recipient using the Digital ID.

According to another aspect of the invention, a data processing system is described. This data processing system has stored therein data representing sequences of instructions which when executed cause the above described method to be performed. The data processing system generally has a Digital ID Server, a sender client, a recipient client, Internet access, databases, and Digital ID Manager software. The method and system

may facilitate other forms of electronic or digital messaging including voice, peer-to-peer, and instant messaging.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may best be understood by referring to the following description and accompanying drawings which illustrate the invention. In the drawings:

FIG. 1 is a screen capture illustrating the first step used by Microsoft's Outlook Express for encrypting an email;

FIG. 2 is a screen capture illustrating an error message received by an email sender using Microsoft's Outlook Express when there is no digital ID for the intended encrypted email recipient;

FIG. 3 is a block diagram of the digital ID server and manager system and method in accordance with the preferred embodiment;

FIG. 4 is a screen capture illustrating the first step in creating a digital ID using a digital ID manager in accordance with the preferred embodiment;

FIG. 5 is a screen capture illustrating the results of a successful digital ID request using a digital ID manager in accordance with the preferred embodiment;

FIG. 6 is a screen capture illustrating the addition of a recipient's digital ID to a sender's email address book in accordance with the preferred embodiment;

FIG. 7 is a screen capture illustrating the results of a successful addition to a sender's email address book of a recipient's digital ID in accordance with the preferred embodiment;

FIG. 8 is a screen capture illustrating a recipient's digital ID icon in a sender's email address book in accordance with the preferred embodiment;

FIG. 9 is a screen capture illustrating an email log indicating that an encrypted email was sent in accordance with the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it is understood that the invention may be practiced without these specific details. In other instances, well-known software, circuits, structures and techniques have not been described or shown in detail in order not to obscure the invention. The term data processing system is used herein to refer to any machine for processing data, including the computer systems and network arrangements described herein. The term Digital ID is used herein to refer to public key or to a public and private key pair. The method and system described herein is applicable to the encryption of electronic or digital messages in general including email, voice, peer-to-peer, and instant messaging.

According to one aspect of the invention, a method is described that allows a sender to transmit encrypted email over the Internet following PKI standards but without prior knowledge of the recipient's public key.

According to another aspect of the invention, a data processing system is described. This data processing system has stored therein data representing sequences of instructions which when executed cause the above described method to be performed. In the following description, these software instructions will be referred to by the term "Digital ID Manager". The data processing system generally has a "Digital ID Server, a sender client, a recipient client, Internet access, databases, and Digital ID Manager software.

FIG. 1 is a screen capture **100** illustrating the first step used by Microsoft's Outlook Express for encrypting an email. In this prior art system, for example, if a user wants to send an encrypted email to a receiver named "Rick" **110**, then the after entering the email message **120**, the user would click the "Encrypt" button **130**. To successfully encrypt this message, the receiver "Rick" must have a public key, or a Digital ID as Microsoft calls it, and the sender must have a copy of this Digital Id in the sender's email address book.

FIG. 2 is a screen capture **200** illustrating the error message **210** the user receives from Outlook Express if there is no digital ID for the intended recipient "Rick" **110** in the user's email address book. To send an encrypted email to the recipient "Rick", after receiving such an error message, the user would have to find out if "Rick" has a Digital ID. If "Rick" does have a Digital ID, then the user would have to obtain a copy of it from "Rick" and place this copy in the user's email address book. If "Rick" does not have a Digital ID, which is very often the case at present, the user would have to ask "Rick" to obtain one from a public key provider (i.e. Certificate Authority) and then forward a copy of Digital ID received to the user. Even if "Rick" is prepared to obtain a digital ID, the process for doing so is not simple and may take days or even weeks to complete. The

result is often the user's selection of the "Don't Encrypt" button **220** and the sending of an unencrypted email to the recipient "Rick".

One solution to this problem as contemplated by the present invention is to enable a sender to generate a Digital ID on behalf of the recipient and to place this Digital ID in the sender's email address book. This solution is accomplished in a data processing system using a Digital ID Server and Digital ID Manager software according to one embodiment of the invention. In this data processing system, upon creation of the Digital ID, the Digital ID Server notifies the recipient, via email, that the sender has created a Digital ID for the recipient. The recipient then downloads the Digital ID from the Digital ID Server by simply clicking a secure link (i.e. SSL –secure socket layer) embedded in the email message provided by the Digital ID Server. For added security, password authentication may be provided for this email message. This password is known only by the sender until the sender informs the recipient of the password by a subsequent communication. The Digital ID is downloaded from the Digital ID Server only once for a recipient rather than for each of the sender's subsequent emails. The Digital ID Manager software enables the sender to create Digital IDs for recipients and place them in the sender's email address book. The Digital ID Server issues Digital IDs to recipients and provides the sender with copies of these Digital IDs. The Digital ID Server facilitates the issuing of Digital IDs while the sender client's SMIME compliant email software performs email encryption using the issued Digital ID. In this data processing system, the sender acts as the Registration Authority and the Digital ID Server acts as the Certificate Authority in accordance with PKI terminology and standards.

Now, referring to FIG. 3, there is shown a block diagram of an exemplary data processing system **300** according to one embodiment of the invention. The data processing system **300** includes a sender **310**, a recipient **320**, a "Digital ID Server" **330**, the Internet **340**, and databases **350**. The sender client **310**, recipient client **320**, and digital ID server **330** have stored therein data representing sequences of instructions which when executed cause the method described herein to be performed. In the following description, these software instructions will be referred to by the term "Digital ID Manager" **360**. Of course, the data processing system **300**, the sender **310**, recipient **320**, and Digital ID Server **330** may contain additional software and hardware a description of which is not necessary for understanding the invention.

Referring to FIGURES 3 to 9, the method of one embodiment of the invention will now be described. At step **1**, the sender **310** initiates a secure session with the Digital ID Server **330** and requests a Digital ID (i.e. a X.509 digital certificate) on behalf of the recipient **320** using Digital ID Manager software **360**. An exemplary screen **400** presented to the sender **310** by the Digital ID Manager **360** illustrating this step is shown in FIG. 4. In FIG. 4, the recipient's **320** common name **410** is "Rick" **420**. The sender **310** requests a Digital ID by clicking on the "Generate Certificate" button **430**. The sender **310** may also request a Digital ID from the Digital ID Server **330** if the sender **310** does not already have its own Digital ID.

At step **2**, the Digital ID Server **330** processes the sender's **320** Digital ID request. This processing includes validation of the sender **320** which may include a check that the sender **310** has paid any required Digital ID Server annual service fees. Typically, as part of a sender's **310** annual service fee the sender **310** will receive a Digital ID allowing the

sender **310** to apply digital signatures to email and to receive and open encrypted email sent by any email user using an X.509 and SMIME compliant email program. The Digital ID Server also performs a database **350** lookup to check if a Digital ID has already been created for the recipient **320**. This lookup may include accessing third party digital certificate registries such as that maintained by Verisign, for example. If the sender's **310** request is validated or approved by the Digital ID Server **330**, then the Digital ID Server **330** creates a Digital ID (i.e. X.509 digital certificate) for the recipient **320**. If the recipient **320** already has a Digital ID, then the Digital ID Server **330** will create a link to this Digital ID.

At step **3**, the Digital ID Server **330** returns the newly created Digital ID or link for the recipient **320** to the sender **310**. FIG. 5 shows an exemplary screen **500** presented to the sender **310** by the Digital ID Manager **360** illustrating a successful Digital ID request message **510**. At this point, the Digital ID Manager **360** may provide the sender with instructions for installing the recipient's **320** Digital ID in the sender's **310** email address book. For example, FIG. 6 shows an exemplary screen **600** presented to the sender **310** illustrating a Digital ID download instruction. It is a unique feature and advantage of the exemplary embodiment that the instructions provided by the Digital ID Manager **360** are easy to understand and follow by users. FIG. 7 shows an exemplary screen **700** presented to the sender **310** illustrating the results of a successful addition to the sender's email address book of the Digital ID for the recipient **320** "Rick" **710**. FIG. 8 shows an exemplary screen **800** presented to the sender **310** illustrating the Digital ID icon for the recipient **310** "Rick" **810** in the sender's **310** email address book.

At step **4**, the Digital ID Server **330** sends an email to the recipient **320** informing the recipient **320** that the sender has created a Digital ID for the recipient **320** thereby enabling the sender **310** and the recipient **320** to exchange encrypted emails.

At step **5**, the sender **310** provides the recipient **320** with a password that has been assigned to the recipient **320** by the Digital ID Manager **360** at the sender's **310** end. Typically, the sender **310** provides this password to the recipient **320** by verbal communications using the telephone. The password is provided as a measure of security to ensure that only the intended recipient receives the Digital ID, which typically includes the recipient's **320** private key, from the Digital ID Server **330**. Alternatively, the password may consist of information known to and verifiable by the Digital ID Server **330**.

At step **6**, the recipient **320** provides the password obtained from the sender in step **5** to the Digital ID Server **300**. If the password is accepted by the Digital ID Server **330**, then the recipient **320** downloads the recipient's **320** new Digital ID from the Digital ID Server **330** by clicking on a secure link (i.e. SSL) in the email received from the Digital ID Server **330** in step **4**. Assuming the recipient **320** provides the correct password, the Digital ID Server **330** provides the recipient **320** with instructions for installing the new Digital ID (including a private key). This Digital ID is a fully functional X.509 digital certificate (i.e. PKI standards compliant) and enables the recipient **320** to subsequently apply digital signatures to email and to receive and open encrypted email sent by any email user using an X.509 and SMIME compliant email program. Typically, this new Digital ID will remain valid for one year from the date of its receipt.

At step **7**, the sender **310** is now able to encrypt and send an email, including attachments, to the recipient **320**. The recipient **320** is now capable of decrypting the received email using the Digital ID obtained in step **6**. FIG. 9 shows an exemplary screen **900** presented to the sender **310** by the Digital ID Manager **360** illustrating an email log message indicating that an encrypted email was sent to the recipient **320** "Rick" **910**.

To reiterate and expand, the system and method of the exemplary embodiment of the invention described has the following unique features and advantages: empowers a user to send an encrypted email, following PKI standards, to a recipient without the recipient's prior possession of a Digital ID; allows a user to request a Digital ID from a Digital ID Server rather than from the recipient; allows both the sender and recipient to use their normal (i.e. SMIME compliant) email programs and leverage off of the encryption capabilities already built into such programs rather than having to install additional applications to facilitate encrypted email communications; neither the sender nor receiver have to learn a new email program; messages sent appear in the sender and recipient's "normal" message store, that is, there is only one set or instance of send and receive logs; Digital IDs issued by the Digital ID Server are interoperable with other X.509 compliant digital certificates; simplifies the process of obtaining, distributing, and installing Digital IDs (i.e. digital certificates); provides users with instructions for installing Digital IDs that are easy to understand and follow; shifts the focus off the Digital ID issue and onto the more important issue of email security through encryption; and, encourages the use of encrypted email and the security it provides. The method and system may facilitate other forms of electronic or digital messaging including voice, peer-to-peer, and instant messaging.

Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. In a data processing system that executes a program of instructions, a method of message encryption and transmission comprising the steps of:

a) requesting a Digital ID on behalf of a recipient from a server by a sender;

b) creating said Digital ID by said server;

c) transmitting said Digital ID to said sender from said server;

d) transmitting a first message to said recipient from said server informing said recipient that said sender has initiated the creation of said Digital ID for said recipient thereby enabling said sender and said recipient to exchange encrypted messages;

e) transmitting said Digital ID to said recipient from said server;

f) encrypting a second message by said sender using said recipient's said Digital ID and sending said encrypted second message directly to said recipient;

g) receiving said encrypted second message from said sender by said recipient and decrypting said encrypted second message by said recipient using said Digital ID.

2. The method of claim 1 and further comprising the step of initiating a session between said sender and said server before said request for said Digital ID from said server is made by said sender.

3. The method of claim 1 and further comprising the step of validating said request for said Digital ID from said sender by said server to ensure that said sender is authorized to make said request of said server.

4. The method of claim 3 wherein said validation includes a database lookup to check if said sender has paid required service fees.

5. The method of claim 3 wherein said validation includes a database lookup to check if said recipient already has a Digital ID.

6. The method of claim 5 wherein said database is a third party digital certificate registry.

7. The method of claim 1 and further comprising the step of generating a password to ensure that only the intended recipient receives said Digital ID from said server.

8. The method of claim 7 wherein said password is generated by said sender.

9. The method of claim 7 wherein said password is generated by said server.

10. The method of claim 7 and further comprising the step of transmitting said password to said recipient from said sender.

11. The method of claim 10 wherein said password is transmitted to said recipient from said sender by spoken word via a telephone network.

12. The method of claim 10 and further comprising the step of transmitting said password to said server from said recipient.

13. The method of claim 12 wherein said transmission of said password from said recipient to said server is initiated by clicking on a secure SSL link in said first message.

14. The method of claim 12 and further comprising the step of validating said password by said server prior to transmitting said Digital ID to said recipient from said server.

15. The method of claim 13 wherein said validation includes checking the said password against the password previously generated.

16. The method of claim 1 wherein said transmission of said Digital ID to said recipient from said server is initiated by clicking on a secure SSL link in said first message.

17. The method of claim 1 and further comprising the step of transmitting installation instructions from said server to said recipient for installing said Digital ID at said recipient.

18. The method of claim 1 and further comprising the step of requesting a Digital ID from said server by said sender for use by said sender.

19. The method of claim 1 wherein said first message is an email message.

20. The method of claim 1 wherein said second message is an email message.

21. The method of claim 1 wherein said first message is a voice message.

22. The method of claim 1 wherein said second message is a voice message.

23. The method of claim 1 wherein said first message is a peer-to-peer message.

24. The method of claim 1 wherein said second message is a peer-to-peer message.

25. The method of claim 1 wherein said first message is an instant messaging type message.

26. The method of claim 1 wherein said second message is an instant messaging type message.

27. The method of claim 1 wherein said Digital ID is a public key.

28. The method of claim 1 wherein said Digital ID is a public and private key pair.

29. The method of claim 1 wherein said Digital ID is a link to an existing Digital ID.

30. The method of claim 1 wherein transmissions between said sender, said recipient, and said server is via the Internet.

31. The method of claim 1 wherein transmissions are between a plurality of said senders, said recipients, and said servers.

32. The method of claim 7 wherein said password consists of information known to and verifiable by said server.

33. A data processing system for message encryption and transmission including a sender client, a recipient client, a server, a plurality of databases, and a plurality of interconnections wherein the said sender client, said recipient client, and said server have stored therein data representing sequences of instructions which when executed cause the method of claim 1 to be performed.

34. The data processing system of claim 33 wherein said interconnections are via the Internet.

35. The data processing system of claim 34 wherein said system includes a plurality of said sender clients, said recipient clients, and said servers.

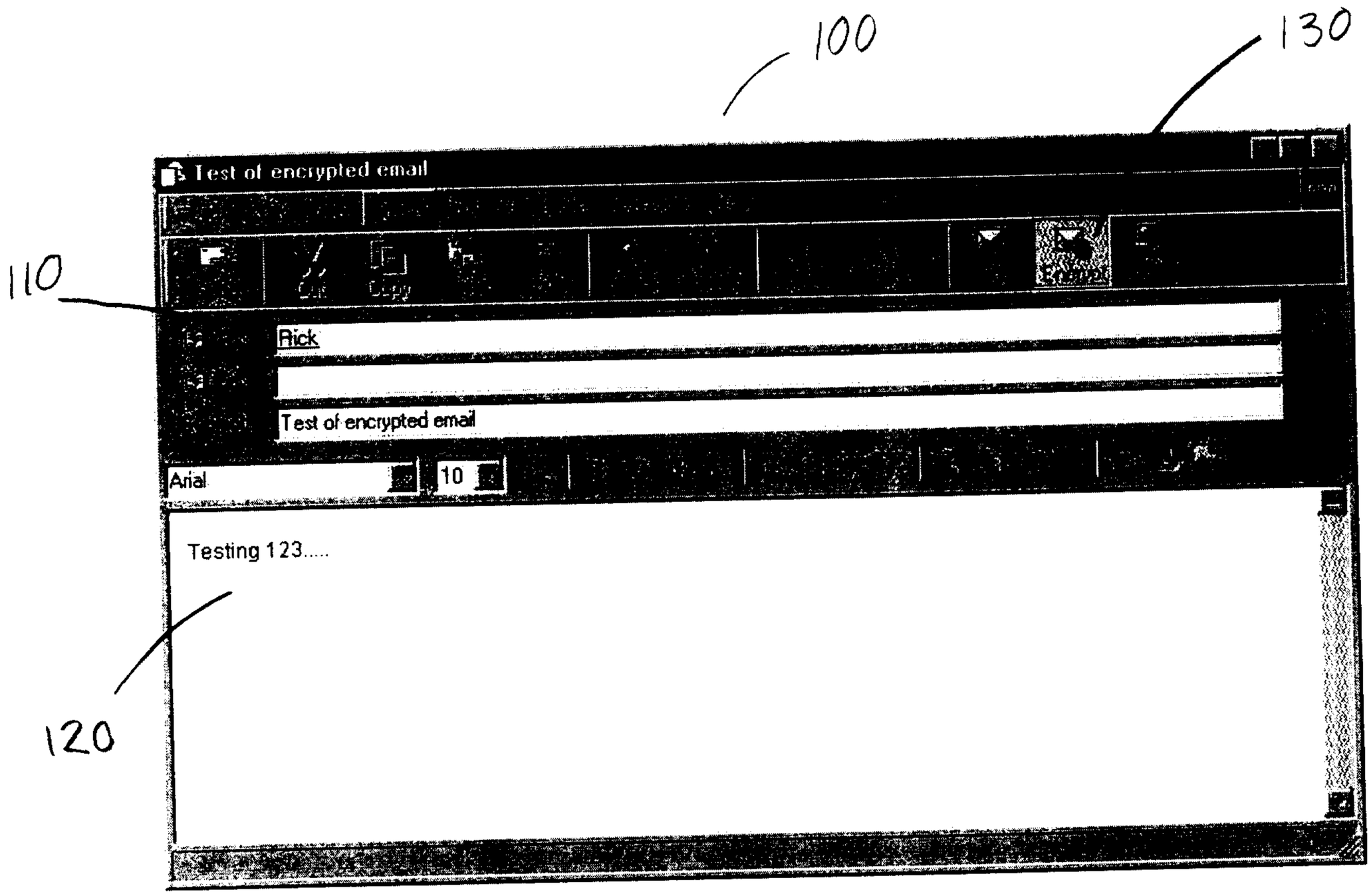

100
130
110
Test of encrypted email
Cut
Copy
Rick
Test of encrypted email
Arial
10
Testing 123.....
120

FIG. 1

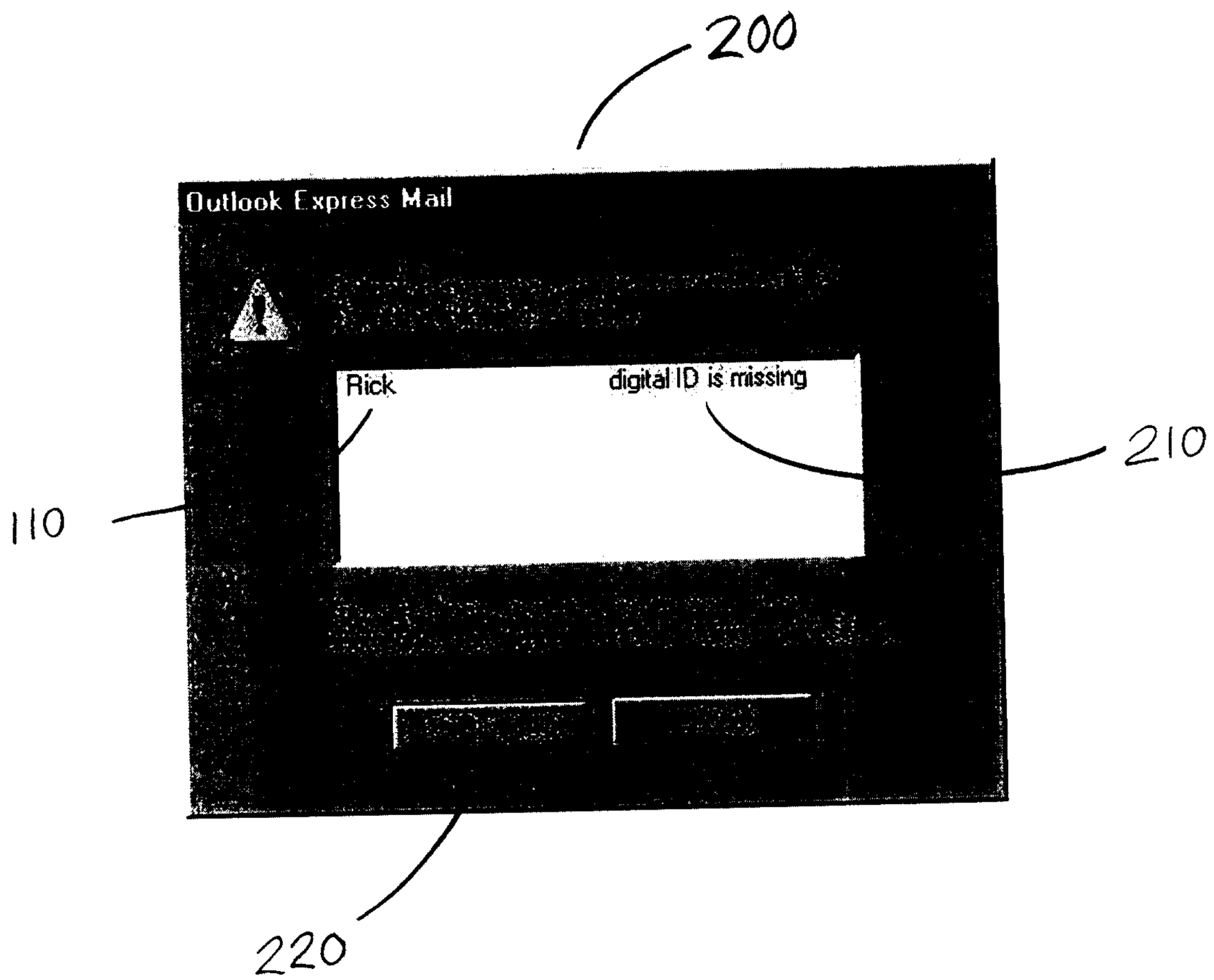

200
Outlook Express Mail
Rick
digital ID is missing
110
210
220

FIG. 2

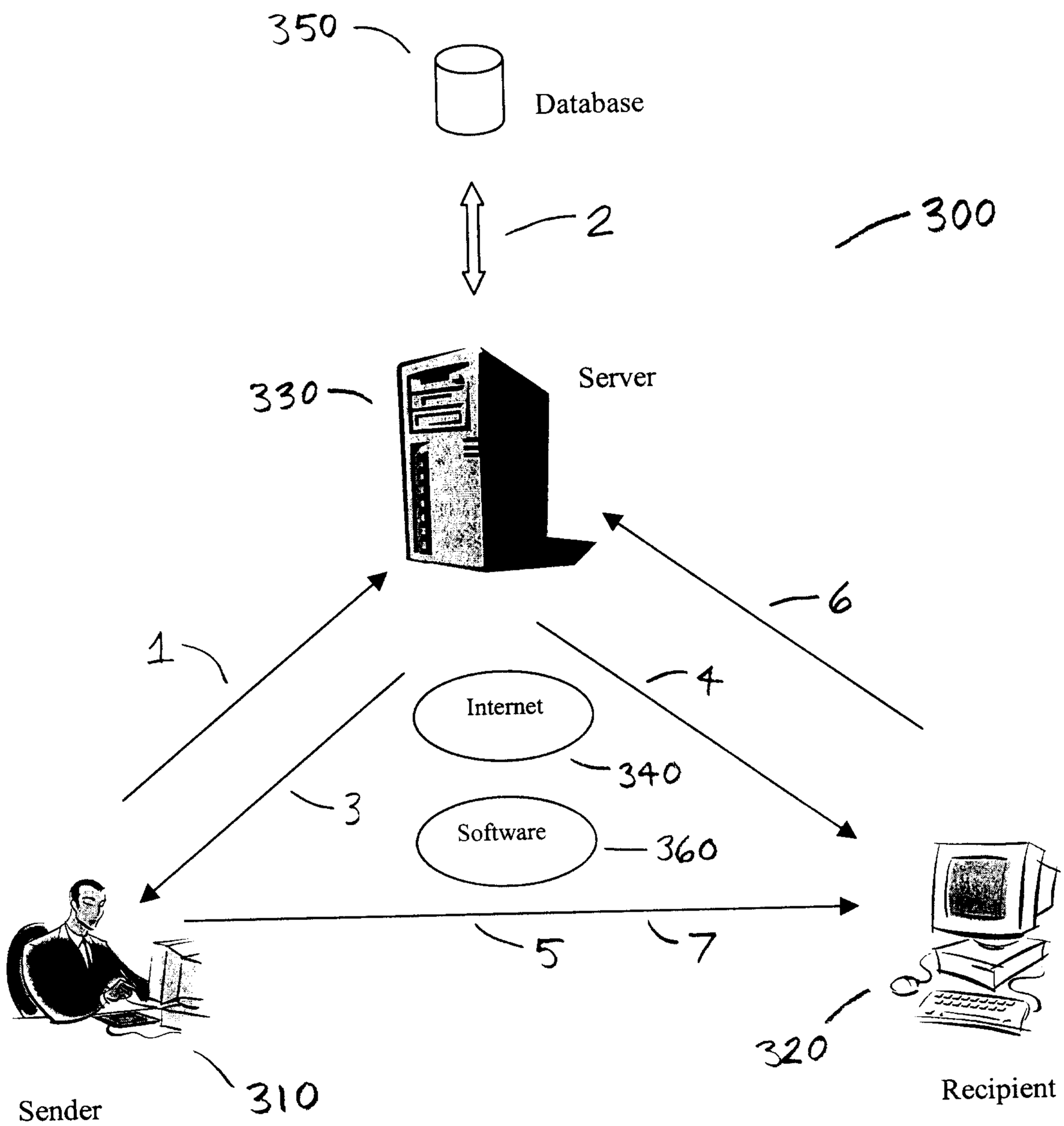

350
Database
2
300
330
Server
1
6
4
Internet
340
3
Software
360
5
7
320
Sender
310
Recipient

FIG. 3

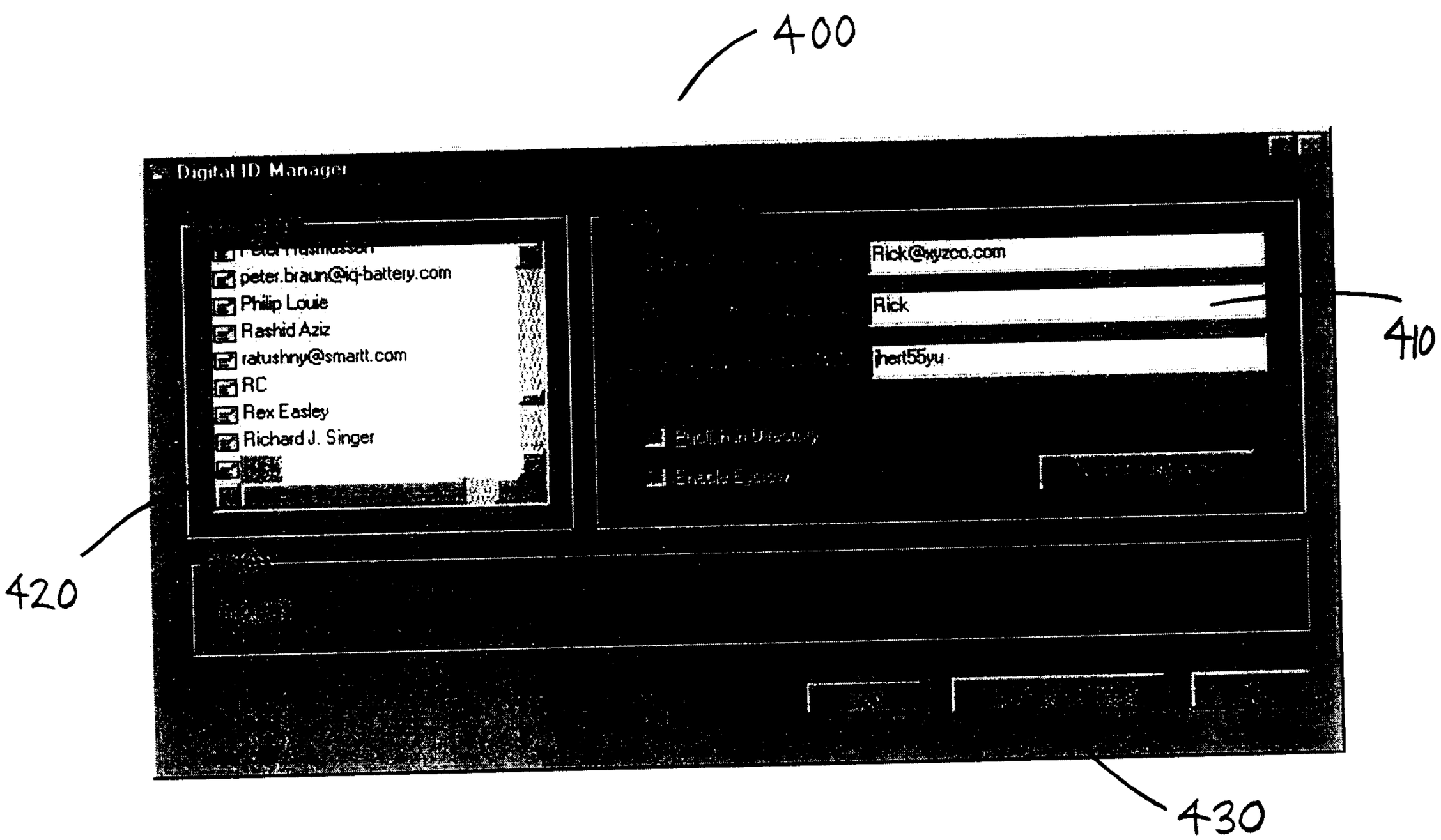

400
Digital ID Manager
peter.braun@iq-battery.com
Philip Louie
Rashid Aziz
ratushny@smartt.com
RC
Rex Easley
Richard J. Singer
Rick@xyzco.com
Rick
jhert55yu
410
420
430

FIG. 4

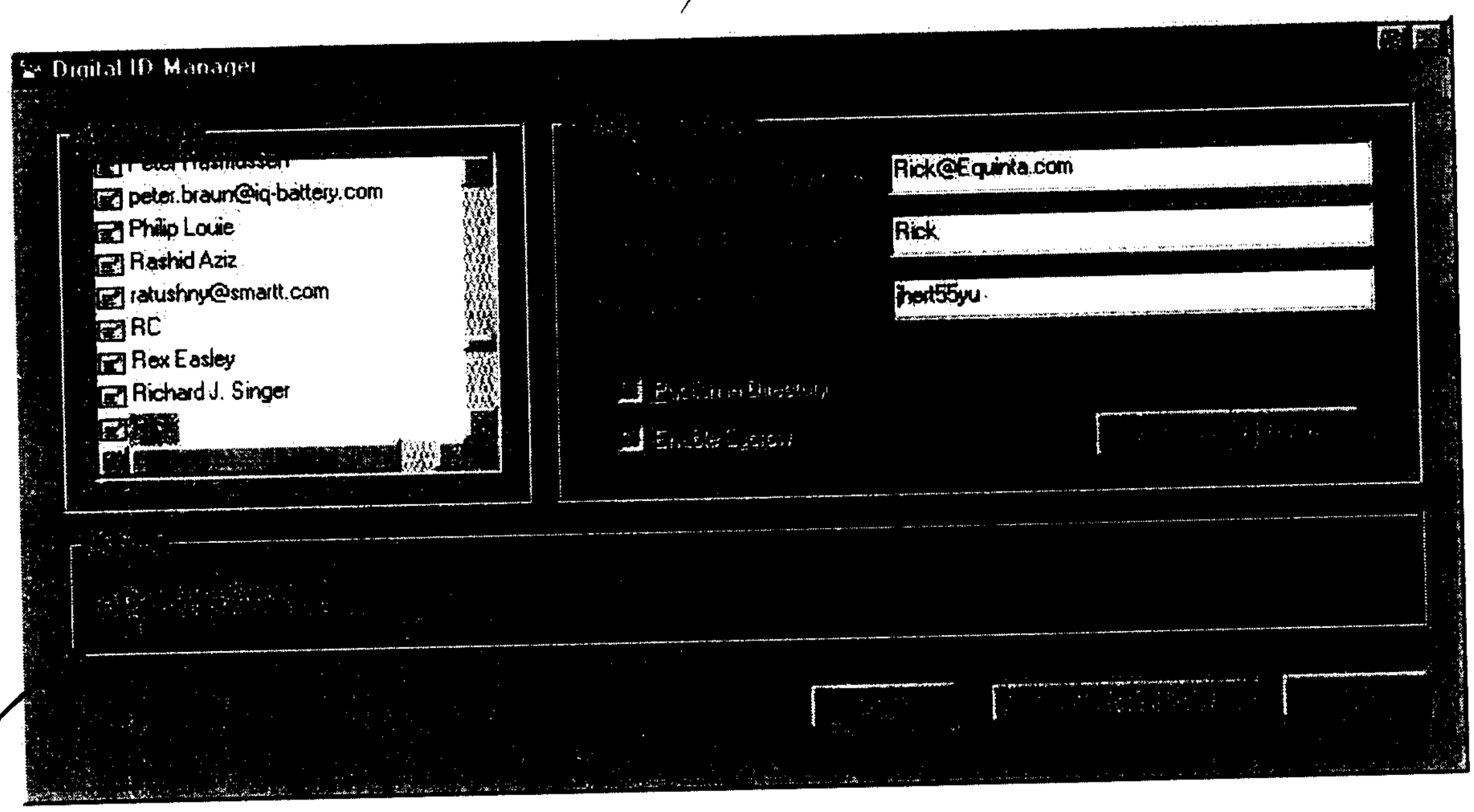

500
Digital ID Manager
peter.braun@iq-battery.com
Philip Louie
Rashid Aziz
ratushny@smartt.com
RC
Rex Easley
Richard J. Singer
Rick@Equinta.com
Rick
jhext55yu
510

FIG. 5

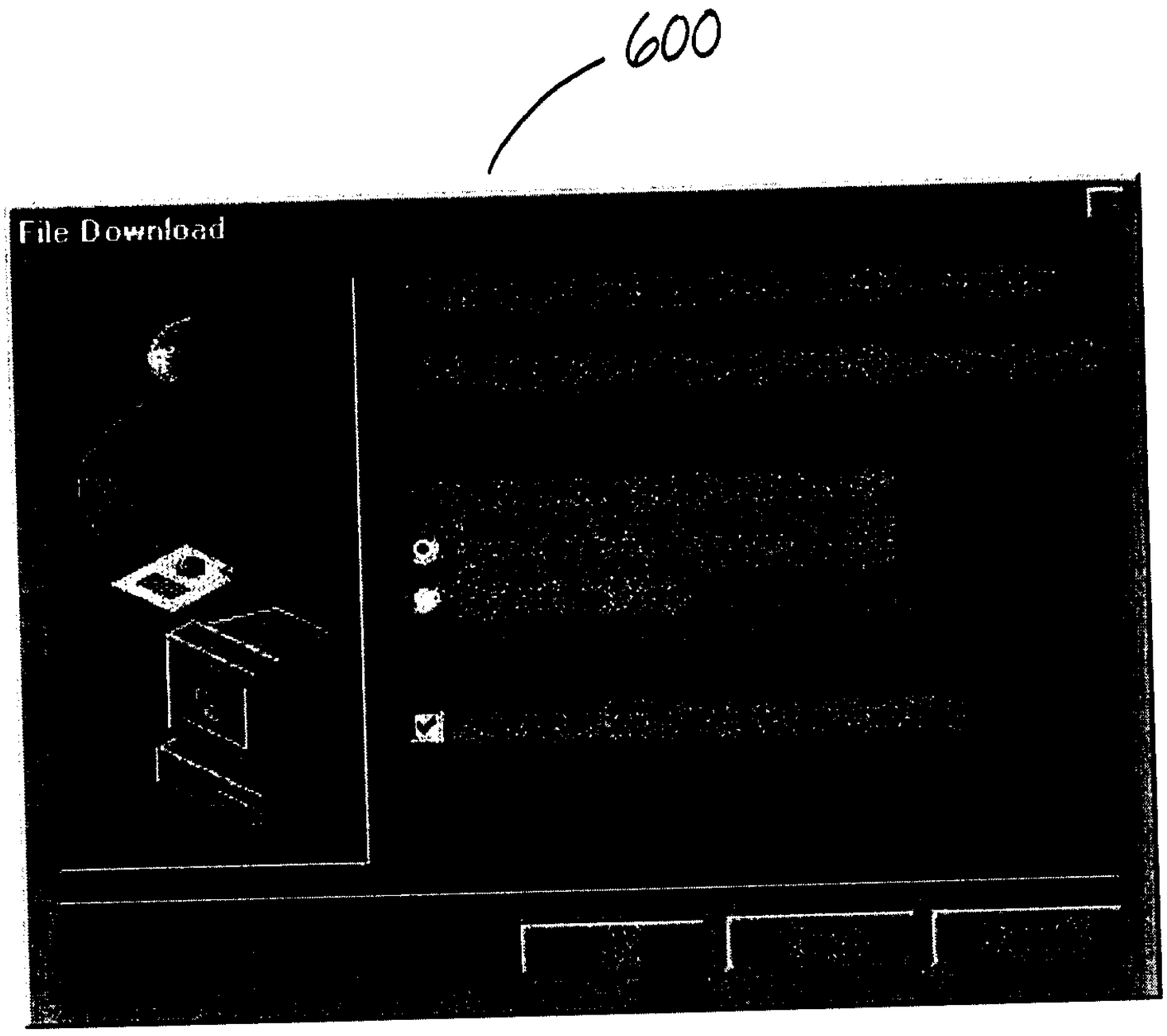


FIG. 6

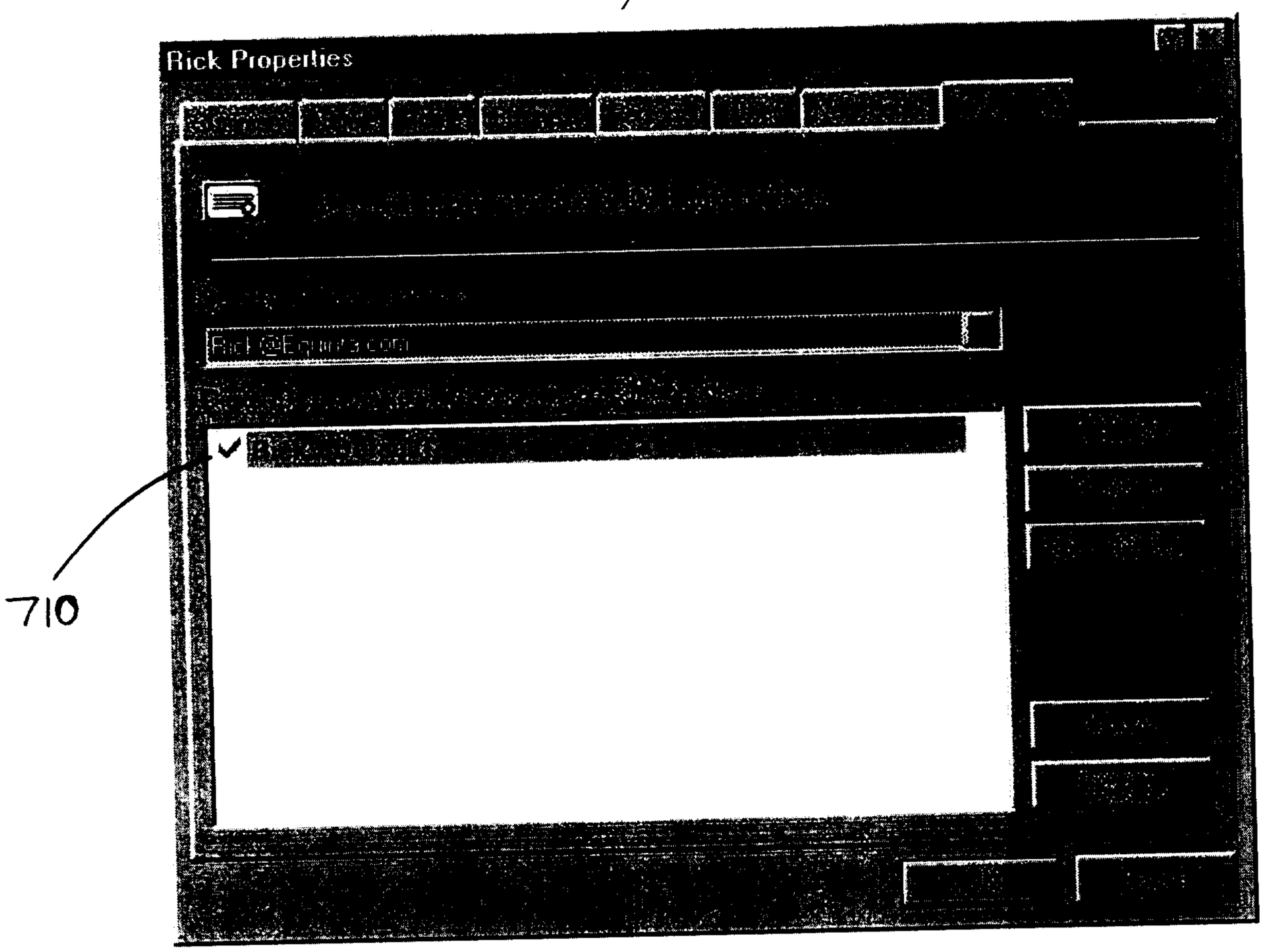


FIG. 7

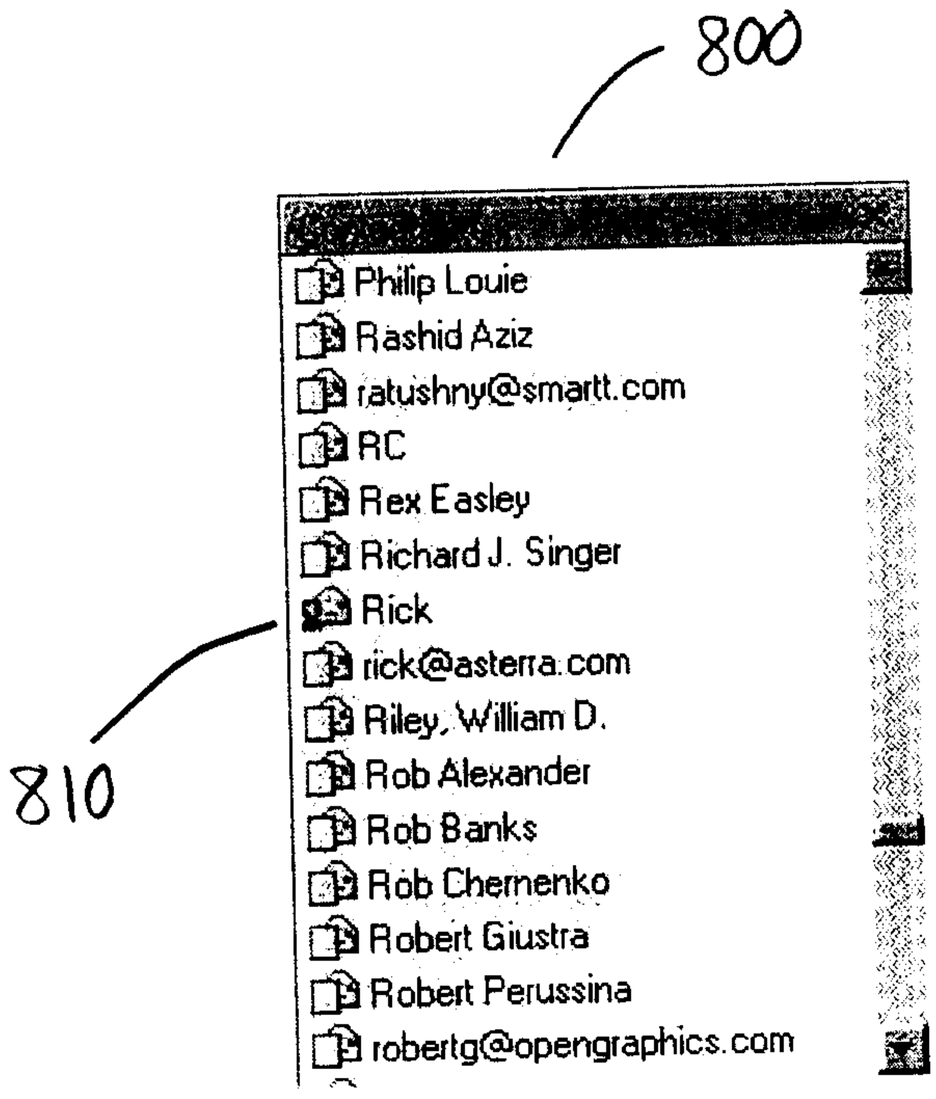

800
Philip Louie
Rashid Aziz
ratushny@smartt.com
RC
Rex Easley
Richard J. Singer
Rick
rick@asterra.com
Riley, William D.
Rob Alexander
Rob Banks
Rob Chernenko
Robert Giustra
Robert Perussina
robertg@opengraphics.com
810

FIG. 8

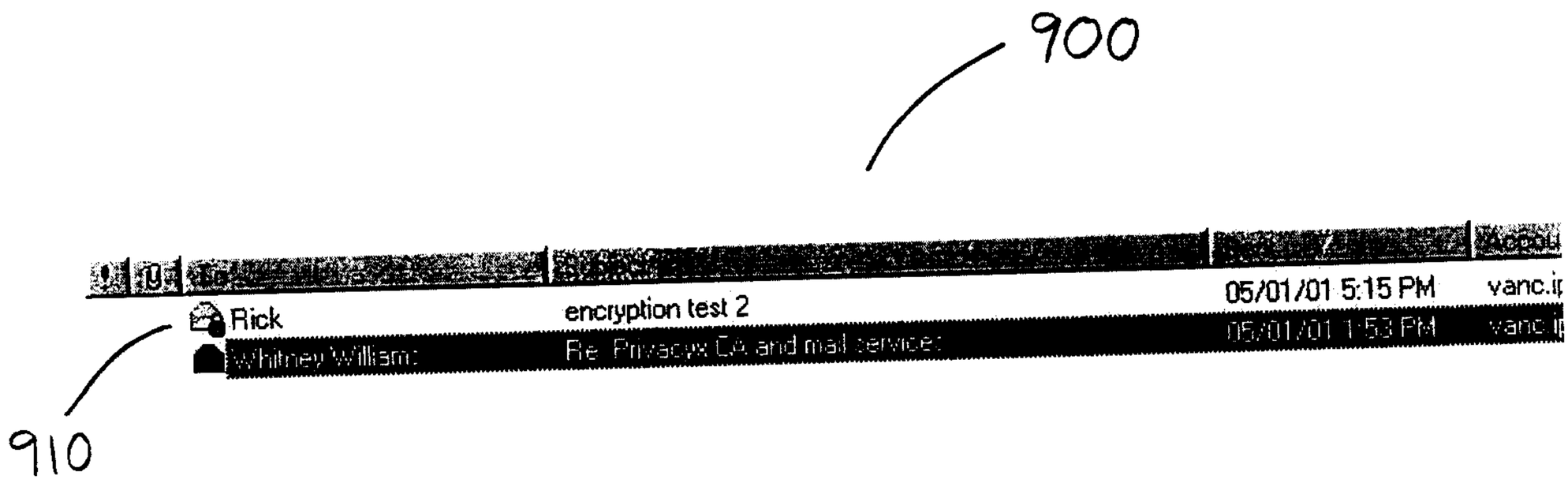
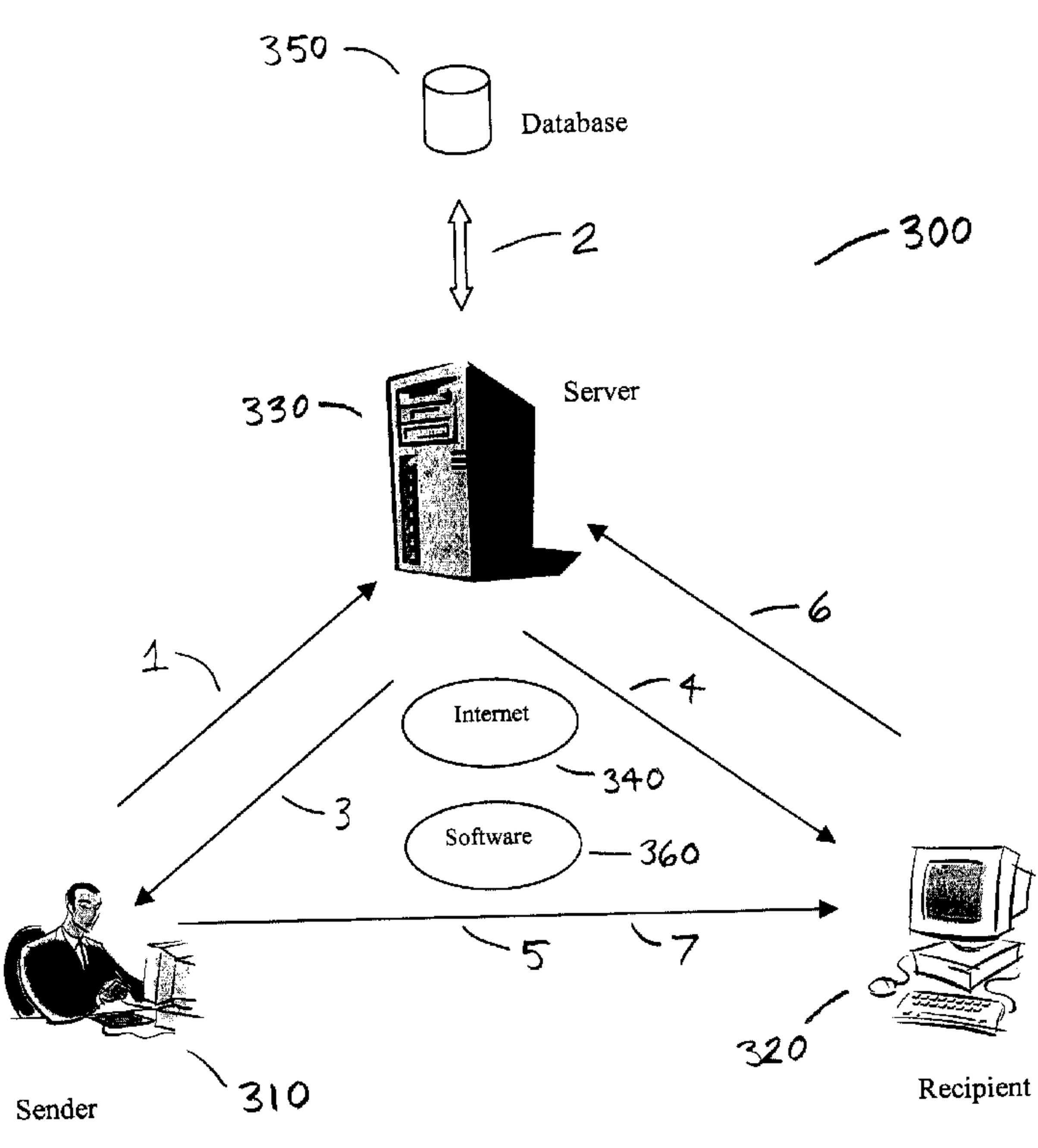

900
Rick
encryption test 2
05/01/01 5:15 PM
Whitney Willism
Re: Privacyx CA and mail service
05/01/01 1:53 PM
910

FIG. 9


350
Database
2
300
330
Server
1
6
4
Internet
340
3
Software
360
5
7
320
310
Sender
Recipient