(12) UK Patent (19) GB (11) 2459202 (13) B

(45) Date of Publication: 19.10.2011

(54) Title of the invention: Methods and systems for preventing junk mails with measures of charge-payment-donation and authentication

(51) INT CL: ***H04L 29/06*** (2006.01) ***H04L 12/58*** (2006.01)

(21) Application No: **0907750.4**

(22) Date of Filing: **18.10.2006**

(86) International Application Data:
**PCT/CN2006/002745 Cn 18.10.2006**

(87) International Publication Data:
**WO2008/046246 Cn 24.04.2008**

(43) Date of Reproduction by UK Office: **21.10.2009**

(56) Documents Cited:
**EP 1705547 A**
**CN 001835434 A**
**CN 001665188 A**

(58) Field of Search:
As for published application 2459202 A *viz:*
INT CL **H04L, H04Q**
Other: **CNPAT, CNKI, PAJ, EPODOC, WPI**
updated as appropriate

(72) Inventor(s):
**Kamfu Wong**

(73) Proprietor(s):
**Kamfu Wong**
**Golden Villa, 3 Keng Han Road, Shatin, Hong Kong**

(74) Agent and/or Address for Service:
**Venner Shipley LLP**
**20 Little Britain, LONDON, EC1A 7DH, United Kingdom**

# Methods and Systems for Preventing Junk Mails with Measures of Charge-Payment-Donation and Authentication

## FIELD OF THE INVENTION

The invention relates to the technical field of internet communications, in particular, to systems and methods concerning email communication technology in the internet.

## BACKGROUND OF THE INVENTION

With the proliferation of internet, more and more people use electronic mails, which are also called emails or mails for short. The email already becomes one of the major communication way and an indispensable tool for correspondence especially in the business section nowadays. The email has almost replaced the way for conveying information through facsimile in the past, since the email is forwarded at faster speed with lower communication cost, and even with no charge of long distance call no matter where the email is forwarded. Nowadays, it is free to send emails, hence with this bug some people collect a large number of email addresses of other people through different ways and then spam these email addresses with business advertisements, personal advertisements even adult information unscrupulously without the recipient's permission. As to the email recipients, these emails are usually sent from strangers and the contents are usually useless advertisements i.e. the so-called junk mails, thus they will delete these emails directly without reading them. However, the number of junk mails is continually increasing, and is even more than the number of normal useful emails; besides, some junk mails even bring computer virus, once the user open

these junk mails, the user's computer would break down due to the computer virus.

The main effect from junk mail is the loss in productivity. The email user has to spend a lot of time to delete these junk mails since these mails always bombast the user's email box; besides, the junk mails also waste the network frequency width and the server memory capacity. Furthermore, when deleting these junk mails, the user may delete some important emails because of hasty, which severely affects the daily communication among people. Thus how to prevent junk mails and how to reduce its effect are urgent issues we have to solve.

## SUMMARY OF THE INVENTION



It is therefore an object of the invention to provide an email system and relevant method for preventing junk mails.

According to the present invention, there is provided a method for exchanging authenticated messages according to claim 1 and a system for exchanging authenticated messages between first and second email servers via an exchange centre according to claim 5.

By this manner, the invention is achieved.

As to advantages, this invention is able to effectively prevent junk mails and reduce junk mails at large scale, since the email sender has to pay fees to the recipients, the costs for sending emails thus increase, and consequently the email-spammer has to pay a large amount of money for sending these emails. While since the common personal email (4) communication and the email (4) communication in business between companies are usually mutual communications, that is to say, both the sender and the recipient pay for each other, and the money paid and the

money received would not be somewhat different, therefore, such an invention would not cause burden or effect on normal email (4) communicators.

## BRIEF OF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram structurally showing the email authentication system of the invention;

FIG. 2 is a diagram showing, when the system and method of the invention are applied, the email (4) communication through the email server (2) and the email authentication exchange center (1);

FIG. 3 is a diagram showing, when the system and method of the invention are applied, the email (4) communication between companies;

FIG. 4 is a diagram illustrating a messaging system without an exchange center;

FIG. 5 is a diagram showing the steps of the embodiment for the invention's system applying the charge mechanism;

FIG. 6 is a diagram structurally showing the embodiment of the invention's system applying the charge mechanism;

FIG. 7 is the diagram showing the embodiment of the invention where an email charge inquiry website (9) is added;

FIG. 8 is a diagram showing steps carried out in a messaging system that does not include an exchange center.

The signs in the Figures represent the same or corresponding system, device, or component part, wherein the email authentication exchange center (1) is abbreviated to exchange center (1), the email servers (2) comprise sending server (2-1) and receiving server (2-2), the digital certificates (5) comprise digital certificate (5-1) of the exchange center

(1), the digital certificates (5-2) of the email servers (4) and the digital certificate (5-3) of a certain company, as well as the user terminal (3), email (4), internet (6), payment gateway (7), a bank account computer system (8), charge inquiry website (9), bank card center (88), fee-charged email server (22).

## DETAILED DESCRIPTION OF THE EMBODIMENTS

The following describes the invention in detail with reference to the Figures.

Refer to FIG. 1. FIG. 1 is a diagram structurally illustrating the system and method for preventing junk mails with measures of charge-payment-donation and authentication.



The general structure of the system of the invention is already specified in the part of Summary of the Invention, and still with reference to FIG. 1, the exchange center (1) is the abbreviation for the email authentication exchange center (1); the exchange center (1) is an email server added with relevant account management and authentication programs, the exchange center (1) also stores the public key for digital certificate (5-2) of respective email server (2) and the private key for its own digital certificate (5-1); the exchange center (1) decrypts the encrypted email forwarded from the email server (2) with the public key for the digital certificate (5-2) corresponding to the email server (2), then encrypts the email (4), which has been already successfully decrypted, with the private key for its own digital certificate (5-1), and then forwards the email (4) to the recipient's email server (2).

The email server (2) is an email server added with relevant programs processing encryption and decryption, and stores the private key for its

own digital certificate (5-2) and the public key for the digital certificate (5-1) of the exchange center (1); when an email (4) sent by the a user is forwarded to the email server (2), the email server (2) encrypts the email (4) sent by the user with the private key for it's own digital certificate (5-2), and then forwards the email (4) to the exchange center (1); besides, when an email is forwarded from the exchange center (1), the email server (2) decrypts the email with the public key for the digital certificate (5-1) of the exchange center (1), then stores the email (4), which is successfully decrypted, into the recipient's email box, where the recipient may check the email (4) via the internet.

The user terminal (3) is a computer, a PDA or a cellular phone or the like that is able to access the internet, and is set up with a program for receiving and sending emails. The user accesses the internet and logs onto the email server (2) with a user terminal (3), then checks or downloads the emails (4) in his/her own email box through the program for receiving and sending emails, and sends emails (4) through the email server (2).



The email (4) represents the correspondence i.e. the mail (4) sent and received through the electronic communication system, and includes mail (4) conveyed via internet (6), or mail (4) conveyed via other communication networks, which all belong to the protection scope of the invention. For the sake of easy description, the electronic mail (4) is abbreviated to email (4) or mail (4) in this specification.

The internet (6) is a communication network such as the Internet network, local network and computer network; the internet is applied to forward emails (4) in the invention.

The digital certificates (5) comprise the digital certificate (5-1) of the exchange center (1) and the digital certificates (5-2) of the email servers

(2), wherein the digital certificates (5) utilize the public key and private key in PKI technology (Public Key Infrastructure) to encrypt and decrypt emails. PKI technology is the prior art, wherein the information sender encrypts the information with a private key of the digital certificate (5), and the encrypted information cannot be decrypted without the public key of the very digital certificate (5); in this manner, the exactness and completeness of the information can be ensured, and by the way, the identity of the information sender is also confirmed.

The invention characterizes mainly in that the exchange center (1) authenticates that the received email is forwarded from the email server (2) with the digital certificate (5-2) of the email server (2), and the email server (2) authenticates that the received email is forwarded from the exchange center (1) with the digital certificate (5-1) of the exchange center (1).



Wherein, the system is set up as follows:

firstly, arranging an exchange center (1) and a plurality of email servers (2), wherein the email servers (2) of the invention can be created by adding relevant program processing encryption and decryption to the some traditional email servers; the exchange center (1) needs to apply for a digital certificate (5-1) from relevant digital certificate authentication center, and the respective email server (2) also needs to apply for a digital certificate (5-2) from relevant digital certificate authentication center; besides, the respective email server (2) has to register and store at the exchange center (1) the public key of its own digital certificate (5-2) and the information such as its network domain name; the exchange center (1) also establishes a blacklist for the email servers that send junk mails, thus the exchange center (1) would not deal with the emails (4) sent from the

email server (2) listed on the blacklist.

When the user sends an email (4) via the email server (2), the email server (2) encrypts the email (4) sent by the user with the private key of its own digital certificate (5-2), then forwards the encrypted email to the exchange center (1), which decrypts the encrypted email with the public key of the digital certificate (5-2) of said email server (2), determines that the email is forwarded from said email server (2) if the decryption is successful; after verifying the email server (2) is not a server listed on the blacklist for junk mail servers, the exchange center (1) encrypts the email (4) with the private key for its own digital certificate (5-1), and then forwards the encrypted email to the recipient's email server (2), which decrypts the received email with the public key for the digital certificate (5-1) of the exchange center (1), and determines that the email is forwarded from the exchange center (1) if the decryption is successful, and then stores the decrypted email (4) into the recipient's email box.



When receiving an email forwarded without being encrypted with a digital certificate (5-2) or an email forwarded from the email server listed on the blacklist for junk mail servers, the exchange center (1) disposes the email at once, that is to say, the exchange center (1) only deals with the emails (4) sent from the email servers (2) which have already registered their digital certificates; moreover, even an email server (2) has not been blacklisted, once some people complain that this email server spams a large amount of junk mails and if the complaint is checked to be true, then the exchange center (1) will revoke the account of the complained email server (2) and list the information such as name of the email sever on the blacklist. As a result, this email server (2) can not forward emails (4) through the exchange center (1) any more.

As to the email server (2), when an email server (2) receives an email not being forwarded from the exchange center (1), namely, the email is not encrypted with the digital certificate (5-1) of the exchange center (1), the email server (2) promptly stores the mail into another email box i.e. junk mail box, since the mails stored there are mainly junk mails, the user may choose to check these mails.

When most or all email servers (2) register at the exchange center (1), and use the digital certificates (5) to authenticate their identities, all normal emails (4) are forwarded to the recipient's email servers (2) through the exchange center (1), while the junk mails cannot be forwarded through the exchange center (1) but be forwarded directly to the junk mail box within the recipient's email server (2). Since the normal emails (4) are stored within the recipient's email box, there is no necessary for the recipients to spend lots of time to check their junk mail boxes which contain a large amount of junk mails. Furthermore, the email server (2) is also able to revoke the user's junk mail box, that is, any email forwarded not through the exchange center (1) would be disposed directly, and therefore a lot of memory capacity can be saved.

Thus the invention is fulfilled in this way.

Refer to FIG. 2. FIG. 2 is the diagram showing the steps of the email server (2) forwarding email through the exchange center (1), and FIG. 2 illustrates an example that a sender sends an email (4) to a recipient, wherein the sender sends the email (4) through the email server (2) of the C service provider (i.e. ISP), while the recipient receives the email (4) through the email server (2) of the D service provider. For the sake of easy description, in the invention the email server (2) for the sender to sending email (4), namely the email server (2) of the C service provider

(i.e. ISP), is abbreviated to sending server (2-1), and the email server (2) for the recipient to receive email (4), namely the email server of D service provider (i.e. ISP), is abbreviated to receiving server (2-2). The embodiment illustrated in FIG. 2 comprises following steps:

A1. when a sender sends an email (4) to the recipient, the email (4) is forwarded to the sending server (2-1) via a user terminal (3);

A2. the sending server (2-1) encrypts this email (4) with the private key for its own digital certificate (5-2), then forwards the encrypted email to the exchange center (1);

A3. the exchange center (1) decrypts the received encrypted email with the public key for the digital certificate (5-2) of the sending server (2-1), determines that the email is forwarded from the sending server (2-1) if the decryption is successful, then promptly encrypts this email (4) with the private key for its own digital certificate (5-1), and then forwards the encrypted email to the receiving server (2-2);

A4. the receiving server (2-2) decrypts the received encrypted email with the public key for the digital certificate (5-1) of the exchange center (1), determines that the email is forwarded from the exchange center (1) if the decryption is successful, and then promptly stores the decrypted email (4) into the recipient's email box, where the recipient may read the email (4) via internet.

Refer to FIG. 3. FIG. 3 is the diagram showing, when the system and method of the invention are applied, the email (4) communication between companies. FIG. 3 illustrates the invention with an example of sending emails (4) to a recipient in company B from a sender in company A. Company A has to apply in advance a digital certificate (5-3) according to a predetermined system program, then registers and stores at

the exchange center (1) the public key for this digital certificate (5-3), and then stores the private key for the digital certificate (5-3) within the sending server (2-1); similarly, company B also has to apply in advance its own digital certificate (5-3), then registers and stores at the exchange center (1) the public key for its digital certificate (5-3), and then stores the private key for the digital certificate (5-3) at the receiving server (2-2). The embodiment illustrated in FIG. 3 comprises following steps:

B1. when a sender in company A sends an email (4) to the recipient in company B, the email (4) is forwarded to the sending server (2-1) via a user terminal (3);

B2. the sending server (2-1) encrypts the email (4) with the private key for the digital certificate of company A, then forwards the encrypted email to the exchange center (1);

B3. the exchange center (1) decrypts the received encrypted email with the public key for the digital certificate (5-3) of company A, determines that the email is sent from company A if the decryption is successful, then promptly encrypts this email (4) with the private key for the digital certificate (5-1) of its own, and then forwards the same to the receiving server (2-2);

B4. the receiving server (2-2) decrypts the received encrypted email with the public key for the digital certificate (5-1) of the exchange center (1), determines that the email is forwarded from the exchange center (1) if the decryption is successful, and then promptly stores the decrypted email (4) into the email box of the recipient in company B, where the recipient may check the email via internet.

In this embodiment, the digital certificate (5-3) of company A is applied to substitute for the digital certificate (5-2) of sending server (2-1),

that is to say, if company A spams a large amount of junk mails, the exchange center (1) would blacklist company A; as a result, company A cannot send emails (4) through the exchange center (1) any more. In this manner, even if some people establish a shell company so as to apply a digital certificate (5-3) for company to send junk mails, the exchange center (1) is also able to eradicate such activities with administrative measures. For example, a certain amount of service fee or deposit can be charged for applying the digital certificate (5-3) for company or for registering at the exchange center (1), the company would be blacklisted when it is found spamming a large amount of junk mail and its deposit would be confiscated too. In this way, the junk mails will be largely reduced since the cost for sending junk mails is increased.



FIG. 4 is a diagram for a messaging system that does not have an exchange center (1). Thus the email servers (2) for respective company authenticate each other directly, each company's email server (2) has to register in advance the names of email servers (2) of other companies with which they contact by emails (4), and stores the public keys for the digital certificates (5-3) for the email servers (2) of these companies; when the email server (2) of a company receives an email from those registered email servers (2), it decrypts the email with the public key for the digital certificate (5-3) of the sender's email server (2), then determines that the email is sent from the registered email server (2) if the decryption is successful, and then promptly stores the decrypted email (4) into the recipient's email box, otherwise, the emails sent from other email servers are stored into the junk mail box. Since the mails are classified, the staff of the company may check the emails (4) in the mail box where the mails are usually much more important, and check the mails in the

junk mail box if time allows. In this way, the chance for the user to delete some important emails (4) when dismissing these junk mails in hasty would be greatly reduced. And the system illustrated in FIG. 4 comprises following C steps:

C1. when a sender in company A sends an email (4) to a recipient in company B, the email (4) is forwarded to the sending server (2-1) via a user terminal (3);

C2. the sending server (2-1) encrypts the email (4) with the private key for the digital certificate (5-3) of company A, then forwards the encrypted email to the receiving server (2-2);

C3. the receiving server (2-2) decrypts the received encrypted email with the public key for the digital certificate (5-3) of company A, then determines that the email is forwarded from the sending server (2-1) of company A if the decryption is successful, and then promptly stores the decrypted email (4) into the email box of the recipient in company B, where the recipient can check the email (4) via internet.



The further improvement in the invention is the introduction of charge mechanism of the sender paying to the recipient, namely the step B5 is added into the embodiment illustrated in FIG. 3. The sender has to pay a certain sum of money to the recipient for every email (4) he/she sends, and the exchange center (1) charges the money from the company at the sending server (2-1) on a monthly settlement basis, and deposits the money, from which a service charge has been deducted, into the bank account of the company at the recipient server (2-2). Then the company at the sending server (2-1) charges relevant money from the sender, while the company at the recipient server (2-2) returns relevant money to the recipient.

Firstly, the exchange center (1) registers the bank account number of respective email server (2) which also signs a contract with the exchange center (1) at the same time agreeing that the emails (4) are charged on quantity basis. The email server (2) has to pay a certain sum of money for each mail it sends to other email server (2) through the exchange center (1), that is, the sender's email server (2) i.e. the sending server (2-1) pays to the recipient's email server (2) i.e. the receiving server (2-2). The fee for sending and receiving emails (4) may be settled promptly, namely, the money for the fee is transferred promptly from the bank account of the sending server (2-1) to the bank account of the receiving server (2-2) at the time the email (4) is sent, or the fee for sending and receiving emails (4) may be settled regularly, such as daily, weekly, or monthly. The amount of money to be charged from and money to be collected by respective email server (2) are calculated during the settlement, and then the exchange center (1) pays or deposits the money with transfers between the bank accounts of the email servers via the payment gateway (7). The exchange center (1) takes out service charge either at certain rate or of fixed amount from the money charged for sending and receiving emails (4). Since the common personal email (4) communication and the email (4) communication in business between companies are usually mutual communications, that is to say, both the sender and recipient pay for each other, and the money paid and the money received would not be somewhat different, therefore, the user would usually not pay too much money.

Refer to FIG. 5. FIG. 5 is the diagram showing the steps for the embodiment of the invention's system where the charge mechanism is applied, and comprises following D steps:

D1. when a sender sends email (4) to a recipient, the email (4) is forwarded to the sending server (2-1) via a user terminal (3);

D2. the sending server (2-1) encrypts this email (4) with the private key for its own digital certificate (5-2), then forwards the encrypted email to the exchange center (1), and then records this count of debt into the sender's account book;

D3. the exchange center (1) decrypts the received encrypted email with the public key for the digital certificate (5-2) of the sending server (2-1), determines that the email is sent from the sending server (2-1) if the decryption is successful, records this count of debt for sending this email into the account book of the sending server (2-1), then encrypts the decrypted email (4) with the private key for the digital certificate (5-1) of the exchange center (1) and forwards the encrypted email to the receiving server (2-2), at last records the income for receiving this email into the account book of the receiving server (2-2);

D4. the receiving server (2-2) decrypts the received encrypted email with the public key for the digital certificate (5-1) of the exchange center (1), determines that the email is forwarded from the exchange center (1) if the decryption is successful, then stores the decrypted email (4) into the recipient's email box promptly for the recipient to check and records the income for receiving this mail into the recipient's account book;

D5. during the settlement, the exchange center (1), based on account book of the respective email server (2), calculates the money to be paid or the money to be received by the email servers (2) with the service charge deducted, then charges or deposits the money via transfer between the bank accounts of the email servers (2) through the payment gateway (7) and the bank account computer system (8), at last the respective email

servers (2) i.e. the sender server (2-1) and the receiving server (2-2) charge the money from or return the money to the accounts of their own users.

Refer to FIG. 6. FIG. 6 is the diagram structurally showing the embodiment of the invention's system applying the charge mechanism, and illustrates the establishment of exchange centers (1) at different regions. For the sake of easy description, the Figure merely shows the exchange centers (1) at two regions X and Y, every exchange center (1) is in charge of exchanging emails (4), clearing settlements or the like for the local email servers (2). When an email (4) is forwarded from region X to region Y, it is forwarded to the recipient's email box at the receiving server (2-2) through the sender's sending server (2-1), the exchange center (1) at region X, and the exchange center (1) at region Y. At the time for settlement, the exchange centers (1) at the two regions clear the settlement based on the quantity of emails (4) received and sent then make transfers through the payment gateway (7) and the bank account computer system (8). Once the exchange centers (1) are established all over the world, all normal emails (4) would be forwarded to the recipient's email box through the exchange centers (1); in this manner, the user is immune to the junk mails once the user forwards emails (4) through the email servers (2) registered at the exchange centers (1). While the junk mails are usually sent in one-way to recipients from the email-spammer, thus it costs a great sum of money if the junk mails are sent through the exchange center (1), which would become an unbearable burden to the email-spammer; if the junk mails are sent through other servers, these mails are thus disposed by the recipient's email server (2) or stored into the recipient's junk mail box. Since those normal emails (4)

are already stored into the recipient's email box, fewer people would check the junk mail box, so that the email-spammer cannot convey the information within the junk mails to the recipients. As a result, few people will send junk mails from then on. Charging a fee to the email sender is the best way to prevent junk mails, and furthermore, the exchange center (1) can donate all the money, from which its cost has been deducted, collected from the email senders to the charity organizations. For example, the money may be donated to the charity voluntary organizations such as Doctors Without Borders and the ORBIS Sight Hospital to help those in need, which most email users surely will not object, moreover, it is also helpful to popularize the systems and methods of the invention.

The local governments may also tax the email senders through the exchange center (1), which would also increase the government's revenue. Since the objects to be taxed are only the email senders, it will neither lay burden to the citizens, nor bring effects on the local economy; therefore it is a good way to increase the government's revenue.

Refer to FIG. 7. FIG. 7 is the diagram showing the embodiment of the invention to which an email charge inquiry website (9) is added. This embodiment employs a mechanism of adding a self-defined donation into the fixed charge, and the self-defined donation charge is the donation level set by the email address owner, it is known from comparison between this embodiment and the one illustrated in FIG. 6 that an email charge inquiry website (9) is added there. Wherein, the email charge inquiry website (9) is for providing information related to the donation charge for the email addresses at the email servers (2) all over the world, and the self-defined donation charge for an email address can be found

through logging onto the email charge inquiry website thence inputting the email address to be inquired. The respective email server (2) classifies its email users into two groups; one group is common email users, to whom the emails can be successfully sent with a payment of the fixed charge, while the other group is the email users with self-defined donation charge, if a person wants to send emails (4) to the email boxes of this group, the person has to pay not only the fixed charge but also the donation charge defined by the recipient. The email server (2) also stores the information such as the email address of the email user with self-defined donation charge and the amount of money for the donation charge into the email charge inquiry website (9), and the email address owners can change the amount of money for the self-defined donation charge at will by sending email to the email charge inquiry website; the email user sends through the sending server (2-1) an email (4) to the email charge inquiry website (9), wherein the content in the email is the new amount of money for the self-defined donation charge, thus the amount of money for the self-defined donation charge is alternated in this way. If some email user wants to receive fewer emails (4), he/she may set a much higher amount of money for the self-defined donation charge, for example, if the chairman of the board of a company set 100 US dollars as the self-defined donation charge for his/her own email address, then only those who are willing to donate 100 US dollars can successfully send an email (4) to the email box of the chairman of the board. The embodiment illustrated in FIG. 7 comprises following E steps:

E1. before sending an email (4) to the recipient, the sender logs on the email charge inquiry website (9) and inputs the recipient's email address, then the sender can find out the amount of money for the

self-defined donation charge set by the recipient;

E2. if the sender accepts the amount of money for the self-defined donation charge, the sender forwards the email (4) to the sending server (2-1) via a user terminal (3);

E3. the sending server (2-1) encrypts the email (4) with the private key for its own digital certificate (5-2), then forwards the encrypted email (4) to the exchange center (1) and records this count of debt into the sender's account book;

E4. the exchange center (1) decrypts the received email (4) with the public key for the digital certificates (5-2) of the sending server (2-1), determines that the email is forwarded from the sending server (2-1) if the decryption is successful, promptly records this count of debt into the account book of the sending server (2-1), then encrypts this email (4) with the private key for its own digital certificate (5-1), and then records this count of income into the account book of the receiving server (2-2);

E5. the receiving server (2-2) decrypts the received encrypted email with the public key for the digital certificate (5-1) of the exchange center (1), determines that the email is forwarded from the exchange center (1) if the decryption is successful, then promptly records this count of income into the recipient's account book; besides, the receiving server (2-2) checks whether the recipient's email address is a common one or the one with self-define donation charge, if this recipient is a common email user, the receiving server (2-2) promptly stores the decrypted email (4) into the recipient's email box for the recipient to check thence skips to step E15, while if the recipient is an email user with self-defined donation charge, then the receiving server (2-2) temporarily stores the email (4) and comes to step E6;

E6. the receiving server (2-2) sends to the exchange center (1) a request for paying the self-defined donation charge, wherein the information content includes the email sender's email address, the recipient's email address, title, date and time of that email, etc.;

E7. after receiving the request for paying the self-defined donation charge, the exchange center (1) searches out the recipient's email address from the information content, then promptly checks the amount of money for the donation charged for the email address on the email inquiry charge website (9);

E8. the email inquiry charge website (9) searches out information about the amount of money for the donation charged for the email address from the records it keeps, then promptly forwards to the exchange center (1) the information about the amount of money for the donation;

E9. the exchange center (1) promptly stores temporarily the information about the amount of money for the donation charge, replies the sender with an email encrypted with the private key for its own digital certificate (5-1), wherein this email is to inform the sender the relevant donation charge and a donation reference code and to remind the sender to pay the relevant donation charge on-line via logging on the website of the exchange center (1) within a designated time limit (such as a week), said donation reference code is a number for distinguishing different emails (4) when receiving the donation;

E10. the sender's email server (2) decrypts the reply email with the public key for the digital key (5-1) of the exchange center (1), determines that the email (4) is sent from the exchange center (1) if the decryption is successful, and it is known from the content that this email is to ask the sender to pay the donation charge, thence this email is stored into the

sender's email box;

E11. when checking the email box, the sender reads the content of the reply email; if the sender agrees to make a donation, he/she may, within the designated time limit, log on the website of the exchange center (1), and input his/her own email address and payment reference code; the sender finds out on the website of the exchange center (1) the recipient's email address for the email (4) sent to the sending server (2-1) described in preceding step E2; after checking the information, the sender inputs the payment information, including information such as credit card number, valid date of the credit card or the debit card and password which is essential for on-line payment, on the payment webpage of the exchange center (1);

E12. the exchange center (1) forwards through the payment gateway (7) the payment information and the total amount of money to the bank account computer system (8) and requests for transfer of the money;

E13. the bank account computer system (8) checks validation of the payment information and account balance, etc., if all information is valid, then transfers the money from the user's account provided in the payment information to the bank account of the exchange center (1), and then informs the exchange center (1) that the transfer is successful;

E14. the exchange center (1) forwards to the receiving server (2-2) the received information about successful transfer for the payment, then the receiving server (2-2) stores the decrypted email (4), which has been temporarily stored at step E5, into the recipient's email box for the recipient to check;

E15. during the settlement, the exchange center (1), based on record of receiving and sending emails at fixed charge for the respective email

server (2), calculates the money to be paid or the money to be received by the email servers (2) with deduction of the service charge from the respective account, then charges or deposits the money with transfer between the bank accounts of the email servers (2) through the payment gateway (7) and the bank account computer system (8), at last the respective email servers (2) i.e. the sending server (2-1) and the receiving server (2-2) charge the money from or return the money to the accounts of their own users; as to the donation collected at step E13, the exchange center (1) donates all the money with the service charged deducted to the charity organizations.

In this embodiment, the exchange center (1) donates all money collected through the donations with service charge deducted to the local charity organizations; besides, the email charge inquiry website (9) would build a webpage about the rank list showing the amount of donation each email address collects, and people can, through logging on this webpage, find out the email address which collects the largest amount of donation, that is, the person to whom most people are willing to make a donation for sending him/her an email. The system and method described in this embodiment is not only able to prevent junk mails, but also able to reduce the amount of emails of less importance; once a much high amount for self-defined donation charge is set up, it is surely that the emails (4) received are of great importance. As a result, the invention prevents junk mails as well as makes charity, which is actually one move serving two ends.

Refer to FIG. 8. FIG. 8 illustrates the steps for a messaging system that does not have an exchange center. This system differs from aforesaid embodiments as follows. This system contains no exchange center (1) nor

an email charge inquiry website (9) but an email server i.e. the fee-charged email server (22); this system is suitable for the email users such as celebrities and the officials of multinational companies. With spamming of junk mails, most celebrities and the senior executives in the business organizations are afraid to make their email addresses known to the public, since their email boxes would be bombast with mails everyday once their email addresses are no longer in secrecy, wherein most of these mails are mainly junk mails, which would bring grave effects to their daily life because email (4) is an essential communication tool for them. Consequently, most of these people would like to keep their email addresses in secrecy or usually for internal use, which is thus not available for other people. Although these people are celebrities in the society, it is still difficult for ordinary people to send emails (4) to them. Thus a website for the fee-charged email server (22) is established, and every celebrity is assigned an email box and an email address which is open to the public. Those who want to send emails (4) to these celebrities firstly have to log onto the website of the fee-charged email server (22) and pay a certain amount of fee such as 1,000 dollars, so that they can send emails (4) to those celebrities, while all the money collected by the fee-charged email server (22) with the service charge deducted would be donated to the charity organization. Since the email sender sends the celebrity an email (4) by making a donation, the celebrity would usually read the content in the email (4) carefully and make a nice reply to the kindhearted donator, which is beneficial to both the celebrities and the society. The system illustrated in Fig. 8 comprises following F steps:

F1. before sending an email (4) to a celebrity, the sender firstly has to open an account at the website of the fee-charged email server (22) and

buy points at that website, then the sender inputs the value of points to be bought and the payment information such as his/her credit card number, for example, 1 dollar equals to 1 point, thus the sender has to pay 1, 000 for 1, 000 points;

F2. the fee-charged email server (22) forwards to the bank card center (88) the sender's payment information such as the credit card number and the amount of money to be transferred for the payment;

F3. after checking that the payment information and the account balance are valid, the bank card center (88) transfers money from the sender's credit card account to the account of the fee-charged email server (22), then informs the fee-charged email server (22) that the transfer is successful;

F4. the fee-charged email server (22) informs the sender his/her application for an account is accept, and the money for buying points has been charged from his/her credit card account;

F5. the sender searches the celebrity's email address from the website of the fee-charged email server (22) and checks the fee (i.e. point) for the authorization code needed for sending an email (4) to the celebrity, for example, the authorization code for sending an email to Bill Gates of the Microsoft costs 500 points, the sender has to buy the authorization code with the points he/she bought right now on the website;

F6. after checking that the sender's point account is valid, the fee-charged email server (22) deducts the fee (i.e. point) needed for the authorization code from the sender's account, then forwards the sender a random authorization code which is unique and one-off; the sender writes this authorization code into the title of the email (4) within the designated time limit (such as a week), then sends the email (4) to the selected

celebrity Bill Gates' email address at the fee-charged email server (22);

F7. within the designated time limit, the sender writes an email (4) entitled with the authorization code and sends it the selected celebrity Bill Gates' email address at the fee-charged email server (22); after receiving the email (4), the charged email server (22) compares the authorization code within the title of the email (4) with the authorization code issued in step F6, if the two codes are consistent, stores the email (4) into the email box of the selected celebrity Bill Gates, and then deletes records of this authorization code; if there is no authorization code corresponding to the recipient within the title of the email received by the fee-charged email server (22), the fee-charged email server (22) disposes this email and informs the sender by email the detailed information that the sender has to buy relevant authorization code so that the email (4) can be sent successfully;

F8. the celebrity Bill Gates logs on the fee-charged email server (22) to check the email (4);

F9. the fee-charged email server (22) forwards the email (4) sent from the sender to the celebrity Bill Gates to check.

The implementation of the invention would thoroughly solve the spamming of junk mails, and reduce loss in productivity due to junk mails. The invention is mainly characterized in that the email communication through all the email servers (2) and exchange centers (1) are authenticated with PKI digital certificate technology. Once the email server (2) is authorized, that means the emails (4) of all the users at this email server (2) would be authenticated, thus this approach would popularize the PKI digital certificate technology more effectively comparing with the traditional approach of authenticating the user

individually, since most users of the traditional approach do not understand thoroughly its installation and usage steps and even often make mistakes, thus they cannot make good use of the digital certificate. However, the method of the invention provides that the emails are authenticated by the email servers (2), and the users can send and receive emails (4) as usual without making any setup, thus the PKI digital certificate technology is applied effectively and is also suitable for most users. As to the requirement for digital signature and confidence, the sender can sign and encrypt the email (4), then send the email to the recipient through the system and method of the invention, and then the recipient decrypts this email and check the digital signature, which is safer and more trustable.

**Claims**

1. A method for exchanging authenticated messages, the method comprising:

encrypting a first message from at least one sender (3) at a first email server (2) to obtain a first encrypted message which is transmitted to an exchange centre (1);

authenticating the first encrypted message at the exchange centre and subsequently obtaining a second message by decrypting the first encrypted message;

encrypting the second message at the exchange centre to obtain a second encrypted message which is transmitted to a second email server (2); and

providing the second message to at least one receiver (3) when the second encrypted message is decrypted and authenticated at the second email server,

wherein the first message is encrypted using a private key of the first email server or the at least one sender and the first encrypted message is decrypted using a public key of the first email server or the at least one sender, the public key being associated with a digital certificate that identifies the first email server or the at least one sender; and

wherein the second message is encrypted using a private key of the exchange centre and the second encrypted message is decrypted using a public key of the exchange centre.

2. The method according to claim 1, further comprising storing the digital certificates at the exchange centre prior to exchanging the authentication messages for identifying at least one of the first email server and the at least one sender.

3. The method according to claim 1, further comprising:

recording a first value into a profile of the first email server when the first encrypted message is successfully authenticated and a second value into a profile of the second email server when the second encrypted message is transmitted to the second email server,

wherein subsequently, a sum corresponding to the first value is deducted from an account associated with the first email server and a sum corresponding to the second value is credited into an account associated with the second email server,

wherein each of the accounts associated with the first and second email servers comprises a financial component.

4. The method according to claim 3, further comprising:

logging onto a website prior to transmitting the first message to the first email server to determine a third value, wherein the third value is predefined by the at least one receiver; and

deducting a sum corresponding to the third value from an account of the at least one sender within a predetermined time period after the second encrypted message has been authenticated at the second email server.

5. A system for exchanging authenticated messages between first and second email servers via an exchange centre, the system comprising:

the first email server (2) for receiving a message from at least one sender (3) and encrypting the message before transmitting to the exchange centre;

the exchange centre (1) for decrypting and authenticating the encrypted message from the first email server before transmitting a re-encrypted message to the second email server; and

the second email server (2) for authenticating the encrypted message from the exchange centre before providing a decrypted message to at least one receiver (3),

wherein the exchange centre stores digital certificates containing a public key of at least one of the first email server and the at least one sender, and provides a private key for re-encrypting the message.

6. The system according to claim 5, wherein the second email server stores a digital certificate containing a public key of the exchange centre.

7. The system according to claim 5, further comprising:

a payment gateway (7) coupled to the exchange centre and arranged to one of credit to and deduct from accounts of the first and second email servers respectively sums equivalent to recorded financial parameters,

wherein the financial parameters are recorded and stored at the exchange centre when the message is received from the first email server.

8. The system according to claim 7, further comprising:

a web server (9) for hosting a website operable by the at least one sender, wherein the website provides at least one financial parameter required by the at least one sender for transmitting the message to the at least one receiver.

9. The system according to claim 8, wherein the at least one financial parameter is modifiable by transmitting a message comprising a replacement parameter to the web server.

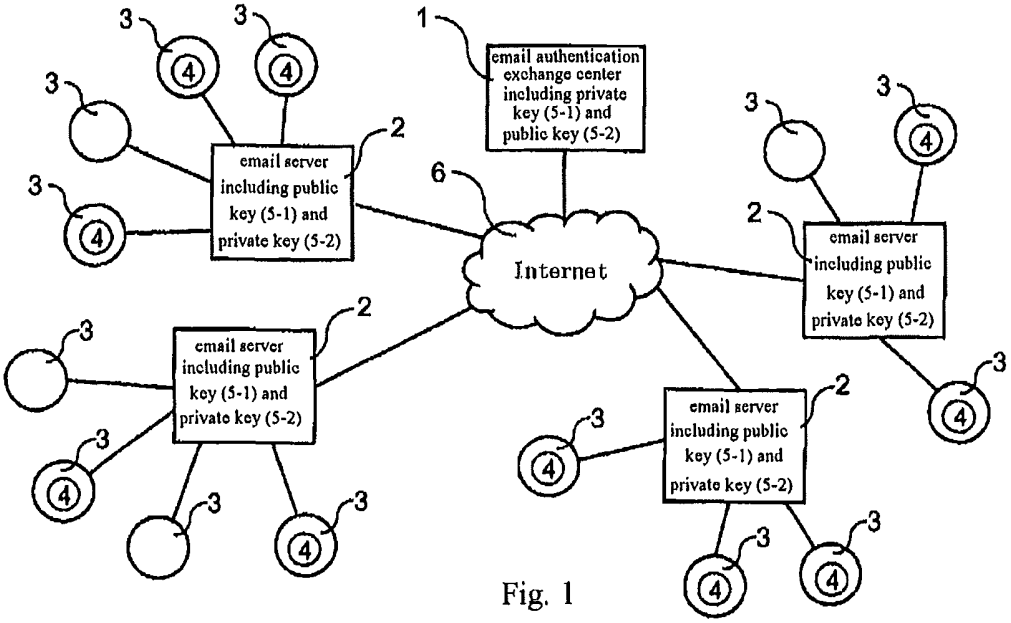
email authentication exchange center including private key (5-1) and public key (5-2)
email server including public key (5-1) and private key (5-2)
Internet
email server including public key (5-1) and private key (5-2)
email server including public key (5-1) and private key (5-2)
email server including public key (5-1) and private key (5-2)
1
2
3
4
6

Fig. 1

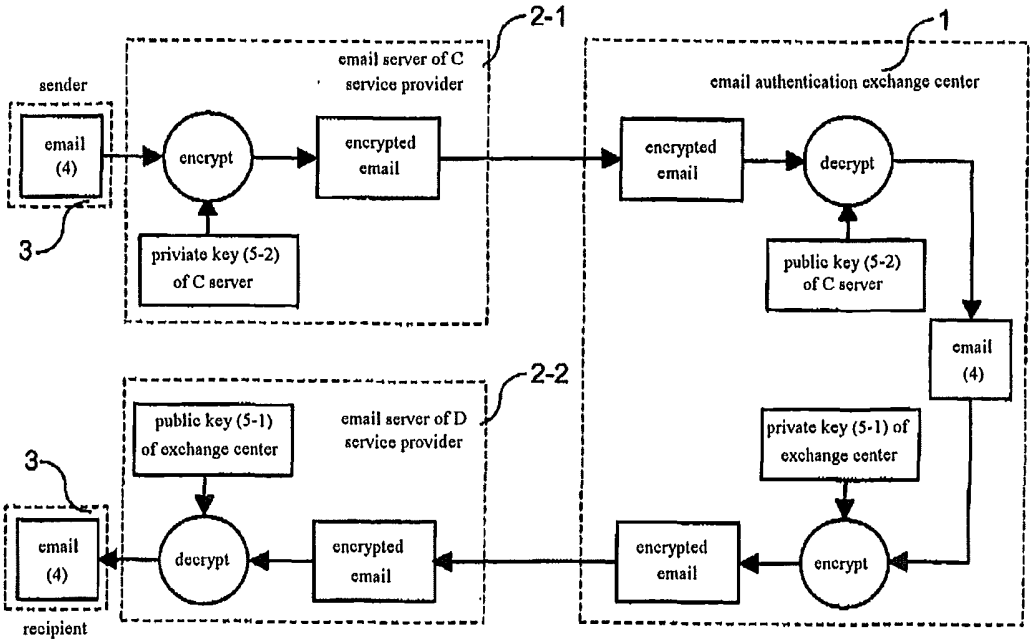
sender
email (4)
encrypt
encrypted email
priviate key (5-2) of C server
email server of C service provider
2-1
email authentication exchange center
1
encrypted email
decrypt
public key (5-2) of C server
email (4)
private key (5-1) of exchange center
encrypt
encrypted email
email server of D service provider
2-2
public key (5-1) of exchange center
decrypt
encrypted email
email (4)
recipient
3

Fig. 2

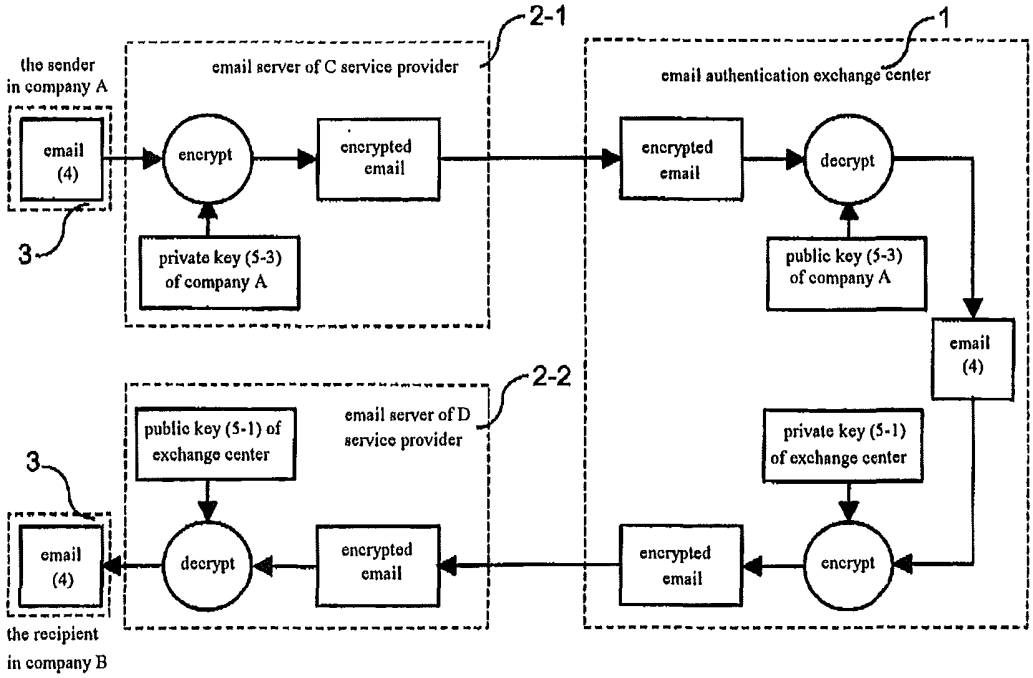
2-1
1
the sender
in company A
email server of C service provider
email authentication exchange center
email
(4)
encrypt
encrypted
email
encrypted
email
decrypt
3
private key (5-3)
of company A
public key (5-3)
of company A
email
(4)
2-2
public key (5-1) of
exchange center
email server of D
service provider
private key (5-1)
of exchange center
3
email
(4)
decrypt
encrypted
email
encrypted
email
encrypt
the recipient
in company B

Fig. 3

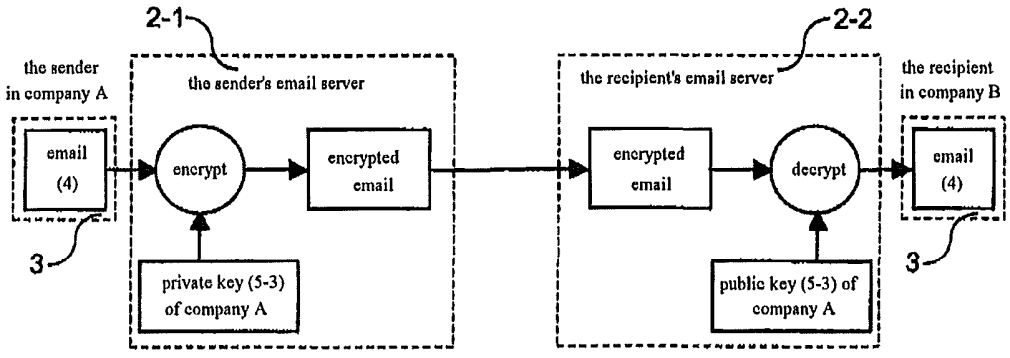
2-1
2-2
the sender
in company A
the sender's email server
the recipient's email server
the recipient
in company B
email
(4)
encrypt
encrypted
email
encrypted
email
decrypt
email
(4)
3
private key (5-3)
of company A
public key (5-3) of
company A
3

Fig. 4

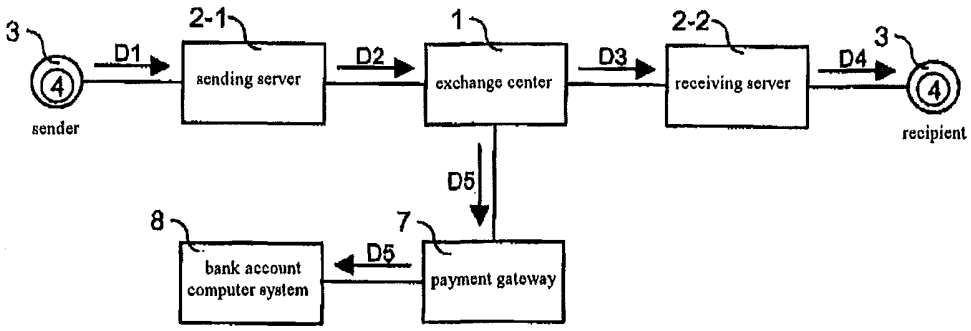
3
D1
2-1
sending server
D2
1
exchange center
D3
2-2
receiving server
D4
3
sender
recipient
D5
8
bank account computer system
D5
7
payment gateway

Fig. 5

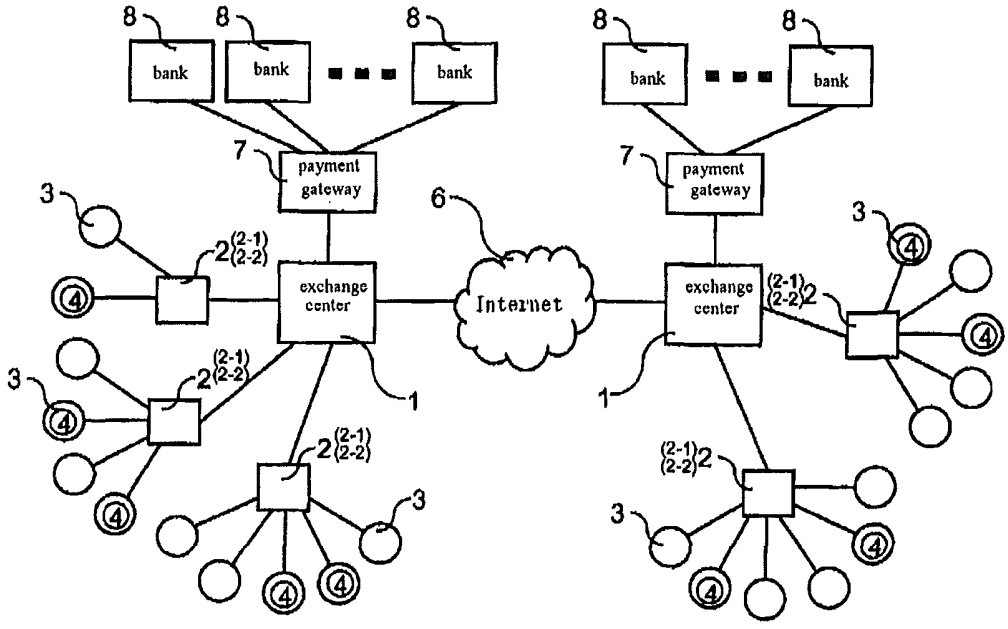
8
bank
payment gateway
7
3
2 (2-1) (2-2)
exchange center
6
Internet
1
4

Fig. 6

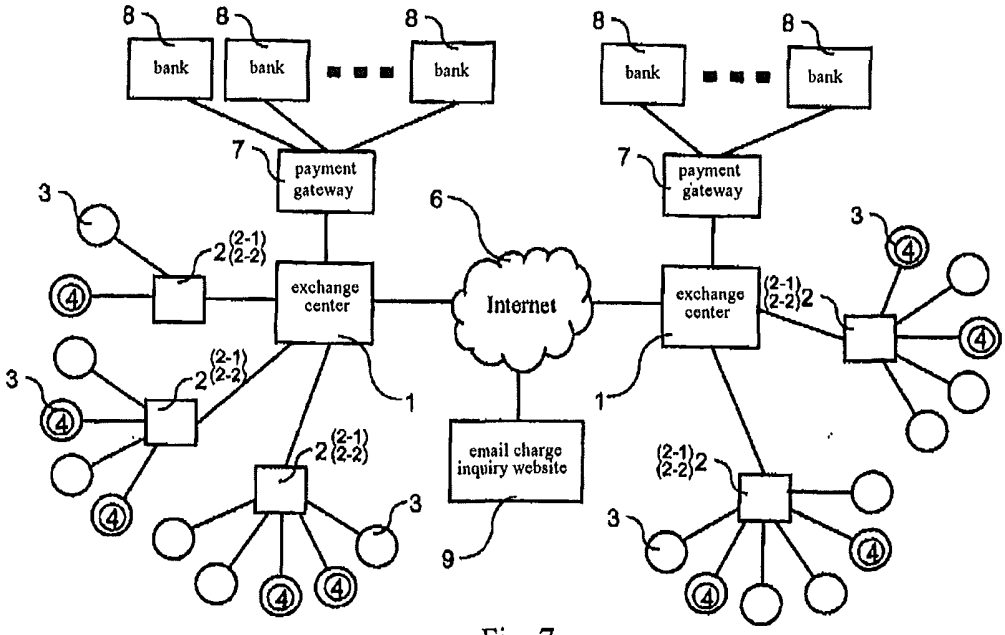
8
bank
bank
bank
bank
bank
7
payment gateway
payment gateway
6
Internet
3
2 (2-1) (2-2)
exchange center
exchange center
1
email charge inquiry website
9
4

Fig. 7

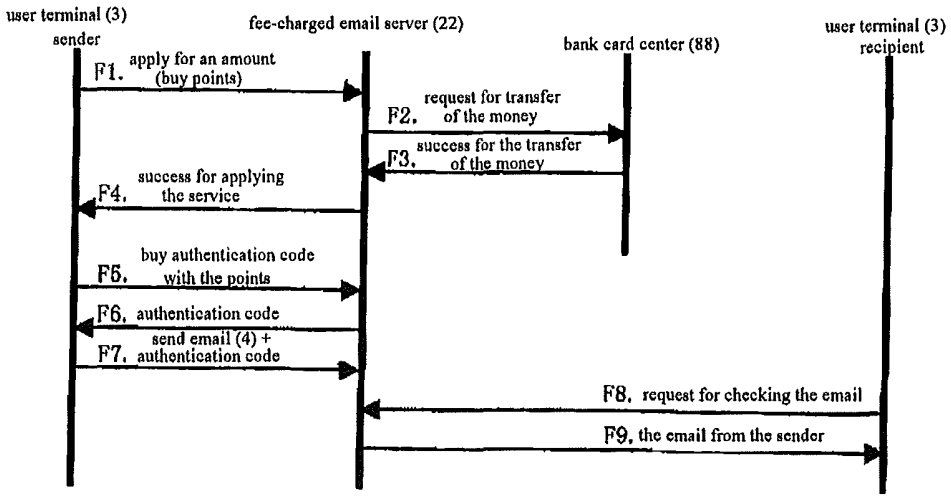
user terminal (3)
sender
fee-charged email server (22)
bank card center (88)
user terminal (3)
recipient
F1. apply for an amount (buy points)
F2. request for transfer of the money
F3. success for the transfer of the money
F4. success for applying the service
F5. buy authentication code with the points
F6. authentication code
F7. send email (4) + authentication code
F8. request for checking the email
F9. the email from the sender

Fig. 8