Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2862557 C 2021/01/26

(11)(21) 2 862 557

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2013/02/19
(87) Date publication PCT/PCT Publication Date: 2013/08/29
(45) Date de délivrance/Issue Date: 2021/01/26
(85) Entrée phase nationale/National Entry: 2014/07/24
(86) N° demande PCT/PCT Application No.: ES 2013/070104
(87) N° publication PCT/PCT Publication No.: 2013/124511
(30) Priorité/Priority: 2012/02/21 (EP12382060.7)

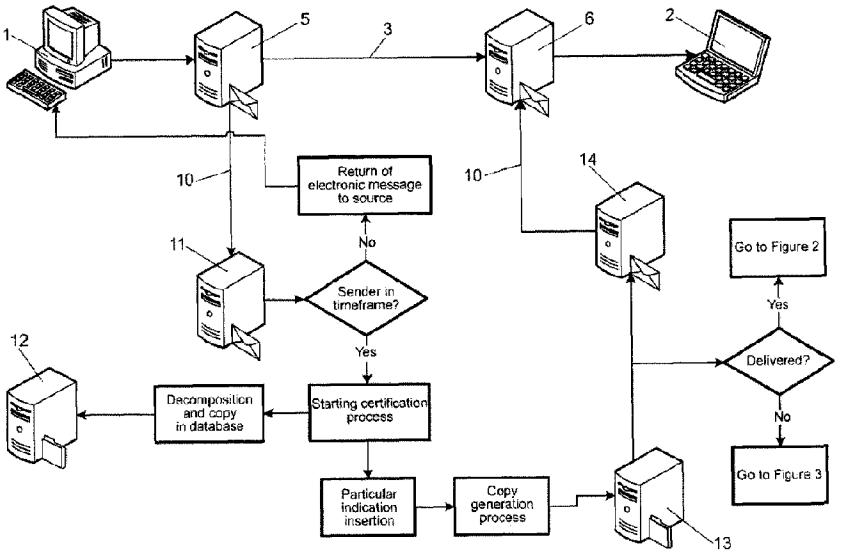
(51) Cl.Int./Int.Cl. *H04L 12/58* (2006.01),
G06Q 10/10 (2012.01)

(72) Inventeur/Inventor:
SAPENA SOLER, FRANCISCO, ES

(73) Propriétaire/Owner:
LLEIDANETWORKS SERVEIS TELEMATICS S.A., ES

(74) Agent: NORTON ROSE FULBRIGHT CANADA LLP/S.E.N.C.R.L., S.R.L.

(54) Titre : PROCEDE DE CERTIFICATION DE L'ENVOI D'UN COURRIER ELECTRONIQUE
(54) Title: METHOD FOR CERTIFYING THE SENDING OF ELECTRONIC MAIL



(57) Abrégé/Abstract:
The object of the invention is a method to receive and send electronic mail from a transmitting user to a recipient, generating proof of the operation transactions to submit the transmitting user a certificate as a trusted third party. To that end, it features the steps of reception in a mail server (11) of a copy of the first electronic message sent by the transmitting user (1) to the recipient (2), the later delivery of a copy of the first electronic message to the recipient (2) together with a particular indication, so that the recipient (2) receives (14) a second electronic message copy of the first electronic message from the mail server, which comprises that particular indication. Finally, the data processing unit (11) creates an electronic document with the transactional data of the delivered copy and signs it digitally creating a certificate (4) that is sent to the initial user (1).

ABSTRACT

The object of the invention is a method to receive and send electronic mail from a transmitting user to a recipient, generating proof of the operation transactions to submit the transmitting user a certificate as a trusted third party. To that end, it features the steps of reception in a mail server (11) of a copy of the first electronic message sent by the transmitting user (1) to the recipient (2), the later delivery of a copy of the first electronic message to the recipient (2) together with a particular indication, so that the recipient (2) receives (14) a second electronic message copy of the first electronic message from the mail server, which comprises that particular indication. Finally, the data processing unit (11) creates an electronic document with the transactional data of the delivered copy and signs it digitally creating a certificate (4) that is sent to the initial user (1).

METHOD FOR CERTIFYING THE SENDING OF ELECTRONIC MAIL

Description

OBJECT OF THE INVENTION

The object of the invention is a method so that a telecommunications operator can receive, forward and send electronic mail from a transmitting user to one or several recipients, generating proof of all the transactional operations to, finally, sign it digitally and submit a certificate to the transmitting user as the operator and trusted third party.

BACKGROUND OF THE INVENTION

It is known that, currently, electronic communications have become an essential and indispensable tool for any operation, both legal and illegal. Communications are used for all kinds of transactions, call and message generation, etc., from a source to a destination.

Telecommunications operators are the ones providing the infrastructures that manage, direct and store a large part of this traffic. These telecommunications operators are subjected to regulations, among others, for the use of the radio spectrum, which is limited, or for the use of telephone numbering resources, which are also finite.

Telecommunications operators, in addition, keep records of the transactions performed by users with the objective, among others, of pricing, registration of the numbers associated with them, billing references, as well as the record of any transactional data used in billing the user. These records are preserved for further verification of pricing and/or follow-up of the traffic on the part of the user.

Occasionally, judicial authorities request the telecommunications operators the recorded data of electronic transactions that were carried out, since they consider them trusted third parties for the purpose of providing these data, as well as any data that could help to determine the physical or legal persons that have done the act in question.

However, the search for data requested to the telecommunications

operator is usually complicated by the fact that it is performed on records of high volume activity, normally designed for billing more than for the follow-up of data traceability. Therefore, the above mentioned search of the requested data may consume an enormous amount of resources for the telecommunications operator.

Once the data requested by the judicial authorities is located, the operator issues a certificate in which it explicitly states the transactional data requested, the frequency, destinations, as well as any information that was requested by the relevant judicial authority.

Also, there is among users this same need to have the capability of requesting this information to the communications operators in order to know and certify the transaction data itself, e.g. the transmitted data, the date, the receiving data or any other information useful to the user. This need could be motivated by the request from a third party to the user of the previously mentioned transactional data.

Various methods and systems are known in the current state of the art for the verification of transmission as well as of the integrity of the data contained in an electronic mail. These known methods normally provide proofs and contents of delivery and reception of electronic mails based on a technological solution that allows verifying the transmission.

However, the methods known in the current state of the art have the disadvantage that they implement algorithms and verifications that modify the contents of the message and they also require the comparison of the digital signature of the generated document to the digital signature stored in the server. These verifications are electronic and online, which may be a disadvantage for some third parties requesting this service.

To that end, in case a transmitting user wishes to certify an electronic mail message, the message passes through a second route that implies the delivery of the message to the recipient through the server of a certifying entity, instead of the traditional route for delivery to the recipient. However, this presents a disadvantage since the message is manipulated in this delivery through the certifying entity's server so that the message that is finally received by the

recipient is not really the original sent by the sender, but the one transformed by the certifying entity.

Besides the above mentioned, the methods known in the current state of the art file a unique cryptographic algorithm associated to each message, i.e., the digital signature. Later, in case the message needs to be verified, the digital signature of a generated document must be compared to the digital signature stored in the server of the certifying entity and, again, a comparison algorithm must be made between the cryptographic algorithm, which is the data generated and stored by the system known in the current state of the art, and the above comparison must be carried out using a comparison algorithm.

As a special case, in which proof of the delivery to the recipient is needed, there is the delivery of the invoices issued by a generating user to be able to show that, subsequently to the reception of the provision of services or products, a receiving user gets the invoice for those services, thus avoiding that the receiving users of a product or service claim non-receipt of the corresponding invoice to avoid or delay payment of the same.

The methods known in the current state of the art for official notification, such as the telegram, office fax or registered letter have several disadvantages such as the non-mechanization of the process, which results in an elevated time consumption as well as a high cost. For example US2007174402 describes a system and a method verifying delivery and integrity of electronic mails where a server transmits a message from a sender to a destination address. During transmission, the server and the destination address have a dialog constituting an attachment, via a particular one of SMTP and ESMTP protocols, concerning the message, the server and the destination address. The message passes through servers between the server and the destination address. This passage is included in the attachment. Verifiers are provided for the message and for the attachments. The verifiers may constitute encrypted hashes of the message and of the attachment. The sender receives the message, the attachments and the verifications from the server before authentication and transmits the message, the attachments and the verifiers to the server to obtain authentication by the server.;

The server operates on the message and the message verifier to authenticate the message and operates on the attachments and the attachments' verifier to verify the attachments. In US2008278740 is described a method, a system and, a computer program product for bulk communication of information to recipients via multiple delivery media are disclosed. The media include facsimile, email, surface mail, SMS messaging, and archiving (and is adapted for new media types in the future). A single interface is used to receive information for distribution including one or more template documents and data specific to each recipient. At least one document based on the received information is transmitted using a specified delivery for each recipient based on the recipients' delivery preferences. Escalating transmission of the document may occur using a different delivery media for any recipients for whom transmission by the specified delivery media fails.; The escalating step may depend upon status information from a carrier regarding delivery of the document to each recipient. In US5815555 is disclosed a method of certifying delivery of an E-mail transmission through a telephonic network. The method includes the steps of detecting a request for an E-mail certification from an originating computer to a destination computer by a controller of the telephonic network and storing a copy of the E-mail transmission in the controller. The method further includes the step of certifying delivery of the E-mail transmission by matching a copy of the E-mail transmission received by the destination computer with the stored copy. Finally US2004177048 unveils a method and apparatus for sorting, prioritizing, identifying, managing, and otherwise controlling (collectively, "controlling") a communication. A frank may be used to associate a value and a class with a communication. The communication may be associated with the frank through the method of selecting a frank associated with a value from among a plurality of frank types, each of the frank types having a pre-assigned value, associating the frank with the communication, and initiating transmission of the franked communication across a network. Value may include anything important of having meaning to the parties, including, for example, money, credit (or a promise to pay), frequent flier miles, and so forth. "Franking" a communication generally associates some indicia of value and/or a

service class with a communication.

DESCRIPTION OF THE INVENTION

The invention object of this application provides a solution to the previously explained disadvantages through a simple certification method that includes transmission data, the transmitted data, the transmitting operator, the destination operator and the final transmission status' data. The system requires a user being a client of the system since users may send the electronic mail in a normal way using the usual route while the system will carry out the certification method automatically. The system has access to a database where the transmitting users' information files are located with the certification capacity and the number of certifications they have available, as well as their operational capacity, then the system authorizes the certification system to let electronic mails in and begin the certification process. The user may use any device allowing navigation through the Internet., a personal computer, a tablet, a Smartphone since once the user is considered to be a client with available certifications, the system will carry out the certification method. According to what was previously explained, the object of the invention is a method so that a telecommunications operator can certify delivery of an electronic mail based on the verification of the transmission and the data it contains.

The method for delivery certification of an electronic mail from a transmitting user to a recipient object of the invention is characterized in that it comprises the following steps that are carried out in a certification system of the delivery of electronic mail which comprises at least one mail server and a data processing unit that are interconnected:

- reception in the mail server of a copy of a first electronic mail sent from the transmitting user to the recipient, i.e., the certification system does not receive the original electronic mail sent by the transmitting user, but a copy of it, while the original electronic mail is sent via the traditional route from the transmitting user to the recipient;
- delivery of the copy of the first electronic mail to the recipient together with a particular indication, so that the recipient receives a second

electronic mail copy of the first electronic mail from the mail server which comprises the particular indication, therefore the recipient receives both electronic mails;

- reception in the mail server of the notification data relative to the delivery to the recipient of the copy of the delivered electronic mail;
- creation at the data processing unit of an electronic document comprising at least the transmitting user's data, the date of issuance, the contents of the attached data and notification data regarding the delivery of the copy of the electronic mail sent;
- application at the data processing unit of a digital signature algorithm to the electronic document for the creation of a certificate;
- delivery of the certificate to the transmitting user through the mail server.

According to the above mentioned, the method object of the invention has the advantage that it does not modify the contents of the electronic mail received by the recipient, and also, it does not generate any algorithm for digital signature comparison, being therefore a method that, in the first place, is simpler than those known in the current state of the art and also it doesn't perform any modification on the electronic mail received by the recipient, but the recipient receives a second message which is the one going through the certifying entity's route, i.e., through the certification system's route.

DESCRIPTION OF THE DRAWINGS

To complement the description being made and in order to help better understand the features of the invention, according to a preferred embodiment thereof, a set of drawings is attached as an integral part of said description, wherein the following is shown as way of illustration but not limited to:

Figure 1.- Shows a flow diagram of a preferred embodiment of the method object of this invention.

Figure 2.- Shows a flow diagram of a preferred embodiment of the creation of a digital certificate.

Figure 3.- Shows a flow diagram of a preferred embodiment of the method

in case the copy of the electronic mail may not be delivered to the recipient.

Figure 4.- Shows a flow diagram of a preferred embodiment of the authentication method of the transmitting user.

PREFERRED EMBODIMENT OF THE INVENTION

Figure 1 shows a preferred embodiment of the electronic mail certification method object of the invention, which comprises the delivery of an electronic mail from a transmitting user (1) to a recipient (2).

The transmitting user (1), which is a client of the certifying entity, sends the electronic mail he/she whishes to certify to the destination electronic address, i.e., to the recipient (2) through an initial route (3) which is the conventional route for the delivery of electronic mails, and also sends a copy to the certifying entity, i.e. through a second route (10) different from the first route (3) in which an incoming mail server (11) receives the aforementioned copy. In the preferred embodiment being shown, the data processing unit (11) that manages the certification process coincides with the incoming mail server (11).

Therefore, the transmitting user (1) uses their usual electronic mail provider, delivering the electronic mail to the recipient or recipients (2). To that end, an initial mail server (5) will send a copy of the electronic mail to each of the destination addresses specified by the transmitting user (1) and a destination mail server (6) collects the electronic mail so that the recipient (2) is finally able to read it, with this electronic mail not suffering any manipulation by the certifying entity or the certifying system.

Additionally, the method may comprise the step of storing a copy of the electronic mail in a database (12) or even the processing unit (11) can previously decompose the copy of the electronic mail in the different objects that make it up: origin, destination(s), attached files, classification of the attached files and finally the numbering of all the objects with their assignation to the transmitting user (1).

As a preferred embodiment of the attached files, these may constitute an invoice, in this case wishing to certify that the invoice has been delivered to its recipient (2).

Once all its parts are decomposed, indexed and classified, the copy of the electronic mail is sent inserting a particular indication, which may be to include the following text in the electronic mail: CERTIFIED ELECTRONIC MAIL or even more specifically CERTIFIED INVOICE, if certification is desired for the contents of an invoice included in the attached data. Later, a new copy is made in a second database (13) and it is sent to the certification system's outgoing mail server (14). The outgoing mail server (14) will deliver it to the destination server (6) where it will be available for the recipient (2).

Therefore, the recipient (2) receives two electronic mails. One is the original electronic mail from the transmitting user (1) which uses his/her own servers (5, 6), therefore, through an initial route (3), and the other one is an electronic mail that is re-sent by the certifying entity's certification system through a second route (10) with the particular certification indication, e.g., CERTIFIED ELECTRONIC MAIL or CERTIFIED INVOICE.

If the copy of the electronic mail had a correct electronic mail address and was able to be delivered to the server (6) it continues the certification process, whose preferred embodiment is shown in figure 2. In case it was unable to be delivered or the address did not exist, the certification process continues according to the preferred embodiment included in figure 3.

Once the copy of the electronic mail has been delivered to the server (6) the outgoing mail server (14) receives the notification data relative to the delivery to the transmission of the electronic mail copy and sends it to the processing unit (11) which manages the certification process.

Once the delivery directions, steps, incidences or any information that may be useful for the certification process have been received, the processing unit (11) creates, in the preferred embodiment shown in figure 2, an electronic document in, for example, a PDF format which includes the transmitting user's (1) data, date of issuance, contents, attached files if any, and finally the date and time of delivery of the electronic mail copy.

Once the electronic document has been created, it is digitally signed through a digital signature algorithm for the creation of a certificate (4).

In addition, a digital sum of all the previous contents may be done, i.e., of the electronic document and the digital signature, and it is sent to a trusted timestamping (20) in order to obtain an electronic document with two electronic signatures from two companies in order to provide the certificate (4) itself with greater legal reinforcement.

Once the final file or certificate (4) is available, it is sent to the transmitting user (1) first withdrawing the cost from their credit account and is then delivered to the outgoing mail server (14). This server (14) sends an electronic mail to the transmitting user (1) including the certificate (4).

Figure 3 shows a preferred embodiment of a flow chart in which the copy of the electronic mail may not be delivered to the recipient (2). If the electronic mail cannot be delivered, either because the recipient (2) does not exist, or because the domain is inoperative, it is attempted again during a period of for example 24 hours.

If it is finally able to be delivered, it continues the process according to what was previously explained, but if it can not be delivered, the outgoing mail server (14) of the certifying entity's certification system receives the data from the transactions made, which are sent to the processing unit (11).

Once the delivery indications, the steps, the incidences and any information that might be useful to the certification process are received, the processing unit (11) creates, in the preferred embodiment shown in figure 3, an electronic document in, for example, a PDF format including the transmitting user's (1) data, the date of transmission, the contents, the attached files if any and finally the time and date of the delivery attempt of the copy of the electronic mail.

Once this electronic document has been created, it is signed digitally through a digital signature algorithm, creating a certificate (4).

In addition, a digital sum of all the previous contents may be done, i.e., of the electronic document and the digital signature, and it is sent to a trusted timestamping (20) in order to obtain an electronic document with two electronic signatures from two entities in order to provide the certificate (4) itself with

greater legal reinforcement.

Once the final file or certificate (4) is available, it is sent to the transmitting user (1) first withdrawing the cost from their credit account and is then delivered to the outgoing mail server (14). This server (14) sends an electronic mail to the transmitting user (1) including the certificate (4).

Figure 4 shows a preferred embodiment of the previous step in which the transmitting user (1) initiates the connection with the certifying entity's processing unit (11).

This transmitting user (1) may enter with different access systems, e.g., a personal computer, a tablet, a Smartphone or any device allowing navigation through the Internet.

In the preferred embodiment shown, the transmitting users (1) access a web control access system. This system has access to a database where the transmitting users' (1) information files are located with the certification capacity and the number of certifications they have available, as well as their operational capacity.

The transmitting user (1) enters his/her user name and password, if it is not correct, he/she gets redirected to a system help with an explanation on how to sign up, and reentry into the authentication system.

If the user is correctly authenticated, he/she may access a menu where, the characteristics regarding how the certificate (4) to be issued must be made and from which addresses the certification of electronic mails is allowed, can be specified. Once these parameters have been defined, the transmitting user (1) may request a certification processing timeframe and adjust its schedule. In other words, from a specific moment it authorizes the certification system to let electronic mails in and begin the certification process.

Finally, if when the process is initiated, the transmitting user (1) is in the delivery timeframe for the mail to be certified, it will begin the processes. Otherwise, the mail is returned indicating that it is outside the timeframe or that it is an unknown transmitting user (1).

As an alternative, the user may otherwise request a witness or encrypted

token to carry out certification requests without the need to open a window via the Web.

CLAIMS

What is claimed is:

1. Method for the certification of electronic mail delivery from a transmitting user (1) to a recipient (2), the method comprising carrying out in a certification system for electronic mail delivery which is implemented by a telecom operator, being the transmitting user (1) a client of said certification system for electronic mail delivery , said certification system for electronic mail delivery comprising at least a data processing unit (11) operative at least as an incoming mail server (11) and an outgoing mail server (14) which are interconnected, the following steps:

- sending an electronic mail from the transmitting user (1) to at least one destination electronic address of the recipient (2) through an initial route (3) by means of an initial mail server (5) and a destination mail server (6),
- sending, from the transmitting user (1), a copy of the electronic mail sent in the previous step to the certification system for electronic mail delivery through a second route (10),
- receiving said copy of the electronic mail at the incoming mail server (11) of the certification system,
- inserting a particular indication in said copy of the electronic mail by means of the processing unit (11) wherein the particular indication comprises the sentence CERTIFIED INVOICE,
- sending through the outgoing mail server (14) a second electronic mail which comprises the copy of the electronic mail with the particular indication,
- delivering to the destination mail server (6) the second electronic mail which comprises the copy of the electronic mail with the particular indication,
- delivering to the recipient (2):
  - the electronic mail through the initial route (3) ,

- the copy of the electronic mail through the second route (10), wherein said copy of the electronic mail comprises the particular indication,
- receiving in the incoming mail server (11) data relative to the delivery of the second electronic mail from the outgoing mail server (14),
- generating at the processing unit (11) an electronic document comprising data related to the preceding steps,
- applying a digital signature to the electronic document of the previous step for the creation of an electronic certificate (4),
- sending from the outgoing mail server (14) the electronic document to a third party to carry out a second digital signature, and
- delivering the electronic certificate (4) to the transmitting user (1) from the processing unit (11).

2. Method for the certification of electronic mail delivery, according to claim 1, characterized in that it further comprises the step of storing, in a database (12) , the copy of the electronic mail .

3. Method for the certification of electronic mail delivery, according to claim 2, characterized in that before storing it in the database (12), the processing unit (11) performs a decomposition of the copy of the first electronic mail in at least: origin, destination, attachments.

4. Method for the certification of electronic mail delivery, according to claim 3, characterized in that, additionally, the processing unit (11) numbers all of the elements in which the copy of the first electronic mail is decomposed and assigns them to the transmitting user (1).

5. Method for the certification of electronic mail delivery, according to any one of claims 1 to 4, characterized in that the processing unit (11) withdraws an

amount from the transmitting user's (1) account.

6. Method for the certification of electronic mail delivery, according to any one of claims 1 to 5, characterized in that it comprises the initial step of authentication of the transmitting user (1) in the certification system.

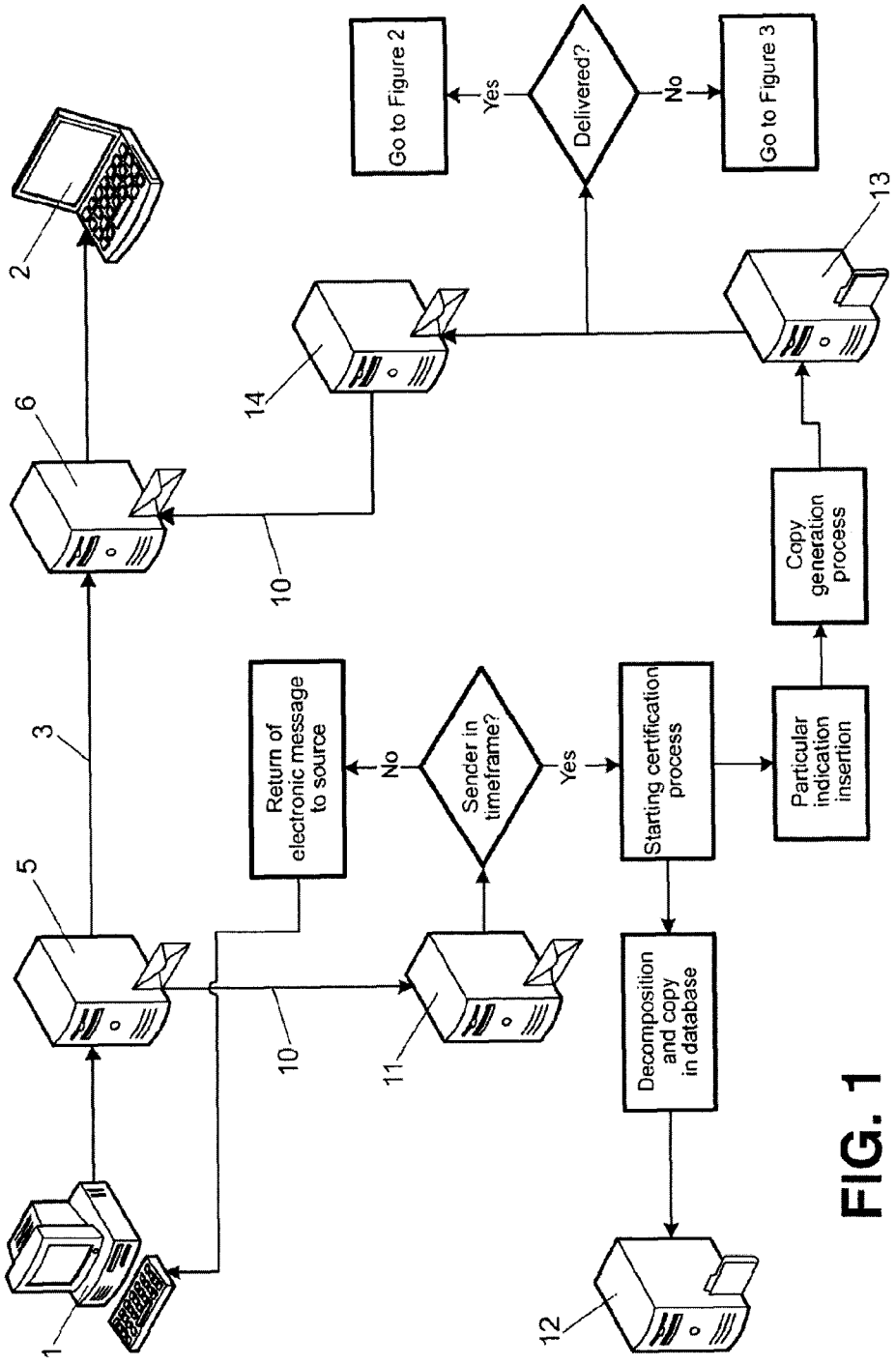

Go to Figure 2
Yes
Delivered?
No
Go to Figure 3
2
13
14
6
10
Copy generation process
3
Return of electronic message to source
No
Sender in timeframe?
Yes
Starting certification process
Particular indication insertion
5
10
11
Decomposition and copy in database
1
12

FIG. 1

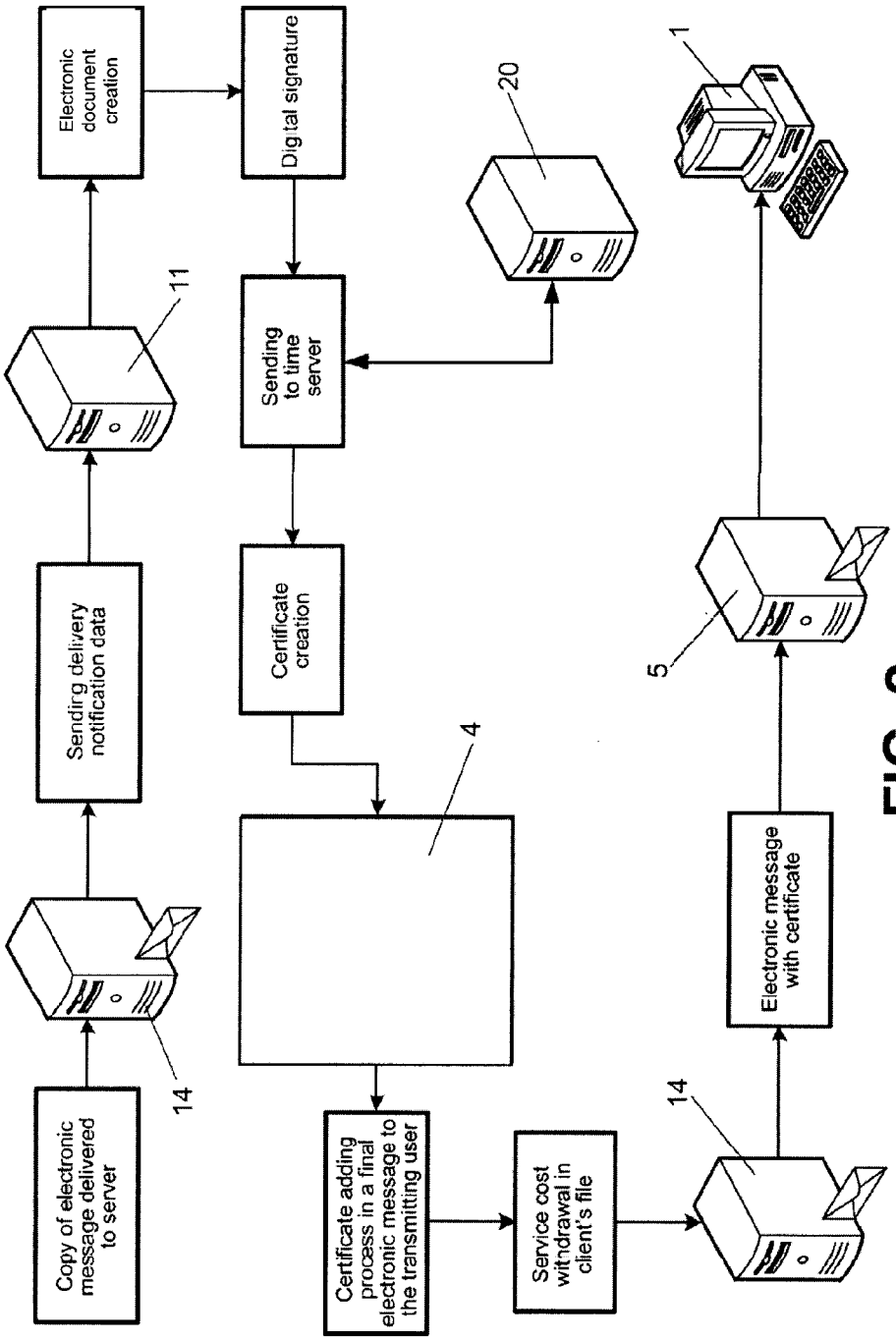

Electronic document creation
Digital signature
20
1
11
Sending to time server
Sending delivery notification data
Certificate creation
5
4
14
Electronic message with certificate
Copy of electronic message delivered to server
Certificate adding process in a final electronic message to the transmitting user
Service cost withdrawal in client's file
14

FIG. 2

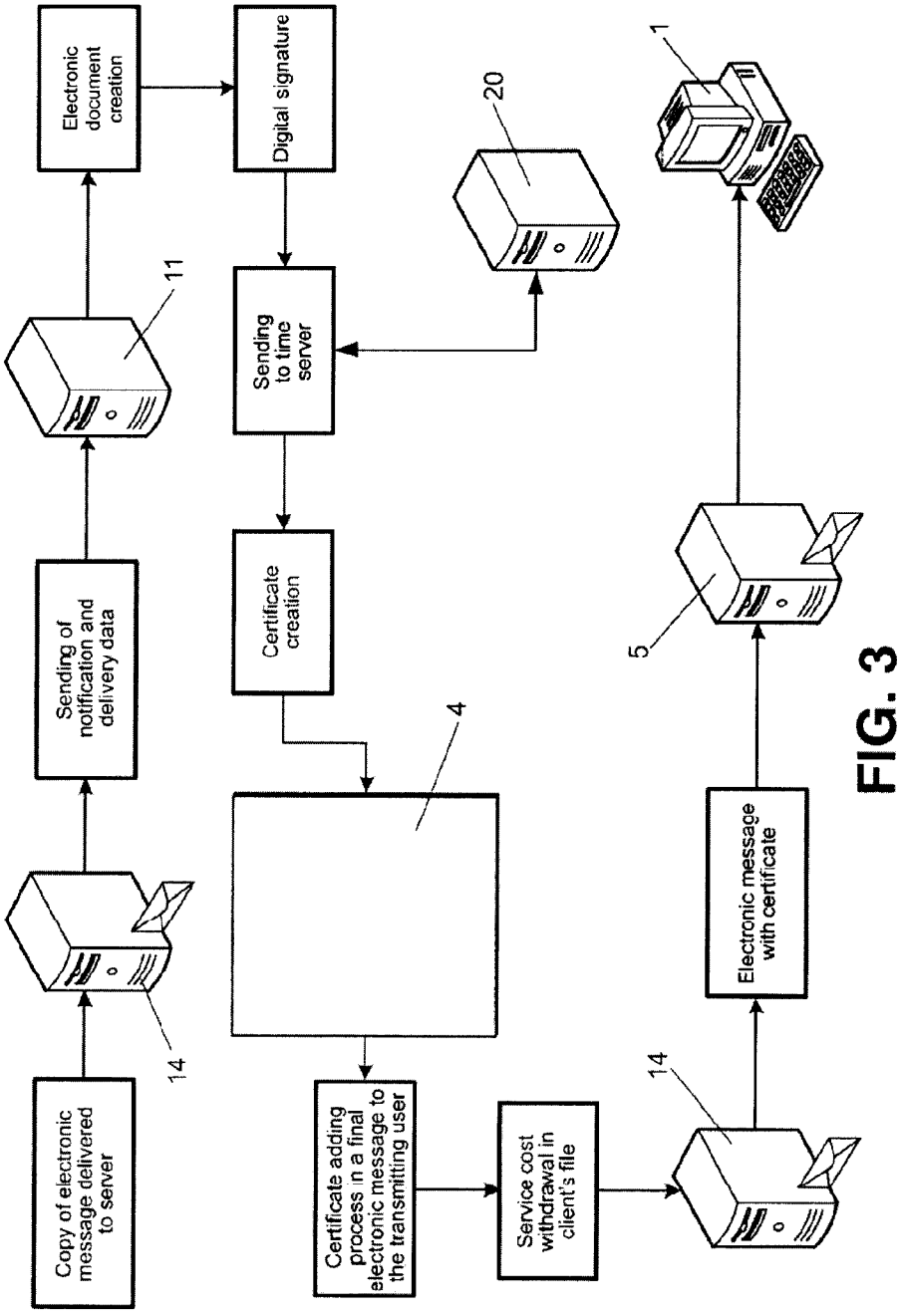

Electronic document creation
Digital signature
20
1
11
Sending to time server
Sending of notification and delivery data
Certificate creation
5
4
14
Electronic message with certificate
Copy of electronic message delivered to server
Certificate adding process in a final electronic message to the transmitting user
Service cost withdrawal in client's file
14

FIG. 3

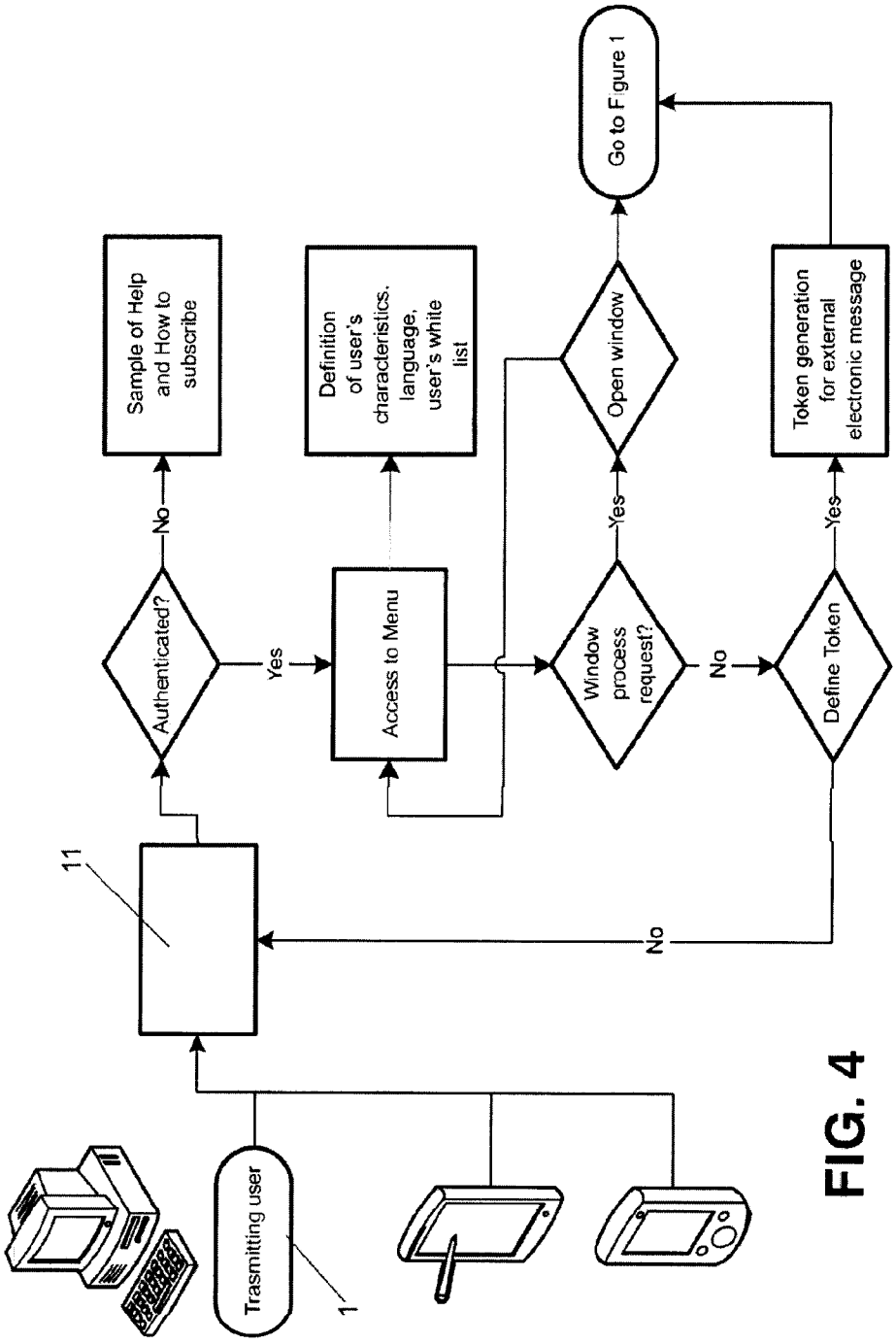
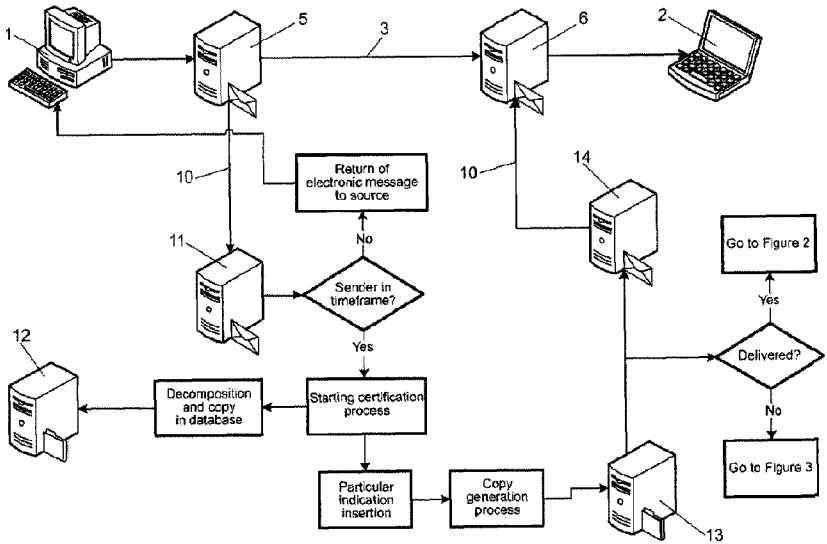

Trasmitting user
1
11
Authenticated?
No
Yes
Sample of Help and How to subscribe
Access to Menu
Definition of user's characteristics, language, user's white list
Window process request?
Yes
No
Open window
Go to Figure 1
Define Token
Yes
No
Token generation for external electronic message

FIG. 4


1
5
3
6
2
10
Return of electronic message to source
No
11
Sender in timeframe?
Yes
12
Decomposition and copy in database
Starting certification process
Particuler indication insertion
Copy generation process
10
14
13
Delivered?
Yes
No
Go to Figure 2
Go to Figure 3