

DELIVER-UPON-REQUEST SECURE ELECTRONIC MESSAGE SYSTEM

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to electronic message systems, and more specifically relates to an electronic message system and method allowing an intended recipient to determine whether or not to collect the full content of an electronic mail message from the source of the electronic message before it is delivered to the recipient's electronic mailbox.

Definition

The foregoing and other objects of the present invention, the various features thereof, as well as the invention itself, may be more fully understood based on the following definition of terms:

<i>Term</i>	<i>Definition</i>
Electronic Message	A message (may contain text, images, audio, voice, video, or their combinations) processed on computer systems and delivered over communication networks.
Electronic Mail Message	An Electronic Message that is delivered and placed on computer systems waiting for access.
Electronic Interactive Message	An Electronic Message that is transmitted for interactive communication.
Host Computer	A computer system comprising hardware and software that its users access over communication networks.

Local Computer	A computer system comprising hardware and software that a user works on locally.
Communication Apparatus	An electronic apparatus capable of sending and receiving Electronic Messages as a Local Computer but with less computing power or storage capacity, preferably a mobile device that can be connected to communication networks.
Sender	A human user or a software agent that uses a Local Computer or Communication Apparatus to send an outgoing Electronic Mail Message or to initiate an interactive communication over communication networks.
Recipient	A human user or a software agent that uses a Local Computer or Communication Apparatus to access an incoming Electronic Mail Message or to respond to an interactive communication over communication networks.
Sending Party	A Sender, a Local Computer or Communication Apparatus that a Sender uses, or a Host Computer that administrates the Sender's account.
Receiving Party	A Recipient, a Local Computer or Communication Apparatus that a Recipient uses, or a Host Computer that administrates the Recipient's account.

Description of the Prior Art

Electronic Mail Systems are implemented for delivering Electronic Mail Messages as long as the Recipients' Electronic Mail Addresses are known. Any Sender can send any Electronic Mail Message, even if undesired, to any Recipient's Electronic Mailbox and consumes the Recipient's available resources.

Further more, in the prior art, the sending party only leaves some uncertified

information about the sending party in the Electronic Mail Message. If the sending party forges information, the true source of the Electronic Mail Message may not be revealed. As a result, SPAM and Electronic Mail Messages carrying computer viruses or malicious programs can widely spread without an easy way to be tracked down. One of the key factors of the problems is due to the send-and-walk-away manner for delivering Electronic Mail Messages.

SUMMARY OF THE INVENTION

To achieve these and other advantages and in order to overcome the disadvantages of the conventional method in accordance with the purpose of the invention as embodied and broadly described herein, the present invention provides an electronic message system and method allowing an intended recipient to determine whether or not to collect the full content of an electronic mail message from the source of the electronic message before it is delivered to the recipient's electronic mailbox.

The present invention allows an intended Recipient to view some basic information of an Electronic Mail Message and determine whether or not to receive the full content of the Electronic Mail Message before it is delivered to the Recipient's Electronic Mailbox. Therefore, the Recipient's resources won't be consumed by undesired Electronic Mail Messages.

With the present invention, if the Recipient determines to receive the full content of an Electronic Mail Message, the Electronic Mail Message will be collected

from the sending party. To deliver an Electronic Mail Message successfully, the Host Computer that originates the delivery of the Electronic Mail Message must be always reachable and await the response from the intended Recipient. In other words, the source of the Electronic Mail Message can be identified and the Sender's identity might be more traceable. This feature will eliminate the possibilities of hiding the origins of SPAM and Electronic Mail Messages carrying computer viruses and malicious programs. Spammers and hackers, who take the advantages of Electronic Mail Systems to spread commercial information or destructive effects, have to reveal their identities, or at least, their Host Computers' identities. And most likely, revealing the true identity would scare annoying or malicious convicts away, especially if they have to face penalties by laws.

Another advantage of the present invention is that the sending parties will be responsible for maintaining and delivering the full contents of Electronic Mail Messages that they initiate. And therefore, the receiving parties won't be burdened by unexpected workload.

Further more, the present invention restricts that only one single copy of each Electronic Mail Message will be collected by each Recipient one by one if there are multiple Recipients. As a result, Electronic Mail Messages that carry computer viruses and malicious programs cannot spread or be forwarded automatically.

With the present invention, because of the possibilities of reducing SPAM and malicious Electronic Messages, the traffic on communication networks may be improved as well.

These and other objectives of the present invention will become obvious to those of ordinary skill in the art after reading the following detailed description of preferred embodiments.

It is to be understood that both the foregoing general description and the following detailed description are exemplary, and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings are included to provide a further understanding of the invention, and are incorporated in and constitute a part of this specification. The drawings illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention. In the drawings,

Figure 1 is a block diagram illustrating a deliver-upon-request secure electronic message system for delivering an Electronic Mail Message according to an embodiment of the present invention;

Figure 2 is a block diagram illustrating a deliver-upon-request secure electronic message system in which both Source Message Server and Destination Message Server are on one single Host Computer for delivering an electronic message according to an embodiment of the present invention;

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the description to refer to the same or like parts.

FIG. 1 shows an exemplary embodiment of the present invention for delivering an Electronic Mail Message. A Source Message Client **11**, which is a Local Computer or Communication Apparatus used by a Sender, transmits the Electronic Mail Message for delivery to an intended Electronic Mail Address. A Source Message Server **12**, which is a Host Computer administrating the Sender's account, receives the Electronic Mail Message from the Source Message Client **11** for delivery to the intended Electronic Mail Address. A Destination Message Server **14**, which is a Host Computer administrating an Electronic Mailbox associated with the intended Electronic Mail Address that a Recipient is entitled to, receives the Electronic Mail Message as the ultimate destination. A Destination Message Client **15**, which is a Local Computer or Communication Apparatus used by the Recipient, accesses incoming Electronic Mail Messages in the Electronic Mailbox.

The Source Message Client **11**, the Source Message Server **12**, the Destination Message Server **14**, and the Destination Message Client **15** are connected to communication networks.

Each of the Source Message Server **12** and the Destination Message Server **14**

is assigned with a unique name such as Domain Name that is registered with authoritative organizations and can be used for establishing a connection to. For a single Host Computer, which performs as a Source Message Server **12** for outgoing Electronic Mail Messages and as a Destination Message Server **14** for incoming Electronic Mail Messages, only one unique Domain Name is needed.

The Source Message Client **11**, the Source Message Server **12**, the Destination Message Server **14**, and the Destination Message Client **15** all have capabilities of generating Public-Secret Key Pairs, encrypting and decrypting Electronic Messages using Public Key Cryptography.

The Source Message Server **12** (or Destination Message Server **14**) generates an initial Public-Secret Key Pair when it is set up to provide services of cryptography, and regenerates a new Public-Secret Key Pair later whenever needed. The Source Message Server **12** (or Destination Message Server **14**) maintains a Public-Secret Key Set containing a Public-Secret Key Pair and a Key Generating Time, which is the Greenwich Time when the Public-Secret Key Pair is generated, of all versions. All the Secret Keys are kept private by the Source Message Server **12** (or Destination Message Server **14**). The Source Message Server **12** (or Destination Message Server **14**) provides its Public Key Set, which contains the Public Key and the Key Generating Time, to its account holders and other parties as described in the following paragraphs. Further more, the Source Message Server **12** (or Destination Message Server **14**) provides a mechanism, such as using File Transfer Protocol (ftp) for exchanging files

over the Internet, for the public to download its most updated Public Key Set. For a single Host Computer, which performs as a Source Message Server **12** for outgoing Electronic Mail Messages and as a Destination Message Server **14** for incoming Electronic Mail Messages, Public-Secret Key Pair only needs to be generated once rather than twice as a Source Message Server **12** and as a Destination Message Server **14** separately.

Typical steps of obtaining the Public Key Set of the Source Message Server **12** (or Destination Message Server **14**) by the Source Message Client **11** (or Destination Message Client **15**) for the first time are as follows:

1. Initially, when the Sender (or Recipient) uses the Source Message Client **11** (or Destination Message Client **15**) to set up a new account corresponding to an Electronic Mail Address with the Source Message Server **12** (or Destination Message Server **14**), the Source Message Server **12** (or Destination Message Server **14**) encrypts its most updated Public Key Set with the associated Secret Key.
2. The Source Message Server **12** (or Destination Message Server **14**) provides, as an Information Flow **22** (or Information Flow **26**), the encrypted Public Key Set to the Source Message Client **11** (or Destination Message Client **15**).
3. Upon receipt of the encrypted Public Key Set, the Source Message Client **11** (or Destination Message Client **15**) downloads, based on a mechanism

provided by the Source Message Server **12** (or Destination Message Server **14**) for the public, the most updated Public Key Set of the Source Message Server **12** (or Destination Message Server **14**).

4. The Source Message Client **11** (or Destination Message Client **15**) decrypts the encrypted Public Key Set with the downloaded Public Key Set to authenticate the identity of Source Message Server **12** (or Destination Message Server **14**), and ensures that the Public Key Set obtained from the decryption is identical to the downloaded Public Key Set.
5. If the decryption succeeds and the two Public key Sets are identical, the Source Message Client **11** (or Destination Message Client **15**) will maintain the Public Key Set obtained from decryption.
6. If the decryption fails or the two Public Key Sets are not identical, the Sender (or Recipient) needs to contact the administrators of the Source Message Server **12** (or Destination Message Server **14**) for straightening things out.

The above steps (1) to (6) only need to be executed once for an account as a user rather than twice as a Sender and a Recipient separately.

If the Source Message Client **11** (or Destination Message Client **15**) already has a Public Key Set of the Source Message Server **12** (or Destination Message Server **14**), typical steps to update the Public Key Set are as follows:

1. Whenever the Source Message Client **11** (or Destination Message Client **15**) establishes a connection to the Source Message Server **12** (or Destination Message Server **14**), the Source Message Client **11** (or Destination Message Client **15**) provides, as an Information Flow **21** (or Information Flow **25**), the last received Key Generating Time of the Source Message Server **12** (or Destination Message Server **14**) to the Source Message Server **12** (or Destination Message Server **14**).
2. The Source Message Server **12** (or Destination Message Server **14**) identifies its Secret Key associated with the Key Generating Time, encrypts its most updated Public Key Set with the identified Secret Key.
3. The Source Message Server **12** (or Destination Message Server **14**) provides, as an Information Flow **22** (or Information Flow **26**), the encrypted Public Key Set to the Source Message Client **11** (or Destination Message Client **15**).
4. The Source Message Client **11** (or Destination Message Client **15**) decrypts the encrypted Public Key Set with the last received Public Key of the Source Message Server **12** (or Destination Message Server **14**) to authenticate the identity of the Source Message Server **12** (or Destination Message Server **14**) and to obtain the most updated Public Key Set of the Source Message Server **12** (or Destination Message Server **14**), then updates the maintained Public Key Set of the Source Message Server **12** (or

Destination Message Server **14**) if necessary.

Again, the above steps (1) to (4) only need to be executed once for an account as a user rather than twice as a Sender and a Recipient separately.

Each of the Source Message Server **12** and the Destination Message Server **14** maintains a Server Database that contains records of information of other Destination Message Servers or Source Message Servers such as Registered Domain Names, Public Keys, Key Generating Times, etc.

When a Destination Message Server **14** (or Source Message Server **12**), called “the initiating party” in the following description, establishes a connection to a Source Message Server **12** (or Destination Message Server **14**), called “the responding party” in the following description, using a Registered Domain Name of the responding party, if the initiating party does not have any Public Key Set of the responding party, the initiating party will request the responding party to provide its Public Key Set. Typical steps are as follows:

1. The initiating party will request the responding party to provide the Public Key Set of the responding party.
2. The responding party encrypts its most updated Public Key Set with the associated Secret Key, provides, as an Information Flow **32** (or Information Flow **31**), the encrypted Public Key Set and a mechanism of downloading its most updated Public Key Set to the initiating party.

3. The initiating party downloads the Public Key Set of the responding party.
4. The initiating party decrypts the encrypted Public Key Set with the downloaded Public Key, and ensures that the Public Key Set obtained from the decryption is identical to the downloaded Public Key Set. If the decryption succeeds and the two Public Key Sets are identical, the initiating party adds the Public Key Set from decryption to its Server Database.

In the above case of establishing a connection between the initiating party and the responding party, if the initiating party already has a Public Key Set of the responding party in its Server Database, the initiating party will update the Public Key Set of the responding party. Typical steps are as follows:

1. The initiating party provides, as an Information Flow **31** (or Information Flow **32**), the last received Key Generating Time of the responding party to the responding party.
2. The responding party identifies its Secret Key associated with the Key Generating Time, encrypts its most updated Public Key Set with the identified Secret Key, and provides, as an Information Flow **32** (or Information Flow **31**), the encrypted Public Key Set to the initiating party.
3. The initiating party decrypts the encrypted Public Key Set with the last received Public Key of the responding party to authenticate the identity of the responding party and to obtain the most updated Public Key Set of the responding party, and then updates the Public Key Set of the responding

party in its Server Database if necessary.

In the above case of establishing a connection between the initiating party and the responding party, if the responding party does not have any Public Key Set of the initiating party in its Server Database, the responding party will establish a connection to the initiating party using the Registered Domain Name of the initiating party to obtain the Public Key Set of the initiating party. Typical steps are as follows:

1. The responding party will request the initiating party to provide the Registered Domain Name of the initiating party.
2. The initiating party provides, as an Information Flow **31** (or Information Flow **32**), its Registered Domain Name to the responding party.
3. Right after this connection is closed, the responding party will establish a connection to the initiating party using the given Registered Domain Name, then follow the steps as in the previous description to obtain the Public Key Set of the initiating party by reversing the roles of the initiating party and the responding party as the new initiating party does not have any Public Key Set of the new responding party.

In the above case of establishing a connection between the initiating party and the responding party, if the responding party already has a Public Key Set of the initiating party in its Server Database, the responding party will update the Public Key Set of the initiating party. Typical steps are as follows:

1. The responding party provides, as an Information Flow **32** (or Information Flow **31**), the last received Key Generating Time of the initiating party to the initiating party.
2. The initiating party identifies its Secret Key associated with the Key Generating Time, encrypts its most updated Public Key Set with the identified Secret Key, and provides, as an Information Flow **31** (or Information Flow **32**), the encrypted Public Key Set to the responding party.
3. The responding party decrypts the encrypted Public Key Set with the last received Public Key of the initiating party to authenticate the identity of the initiating party and to obtain the most updated Public Key Set of the initiating party, and then updates the Public Key Set of the initiating party in its Server Database if necessary.

Whenever a Recipient's (or Sender's) Destination Message Client **15** (or Source Message Client **11**) initially generates or regenerates a Public-Secret Key Pair, the Public-Secret Key Pair will be maintained on the Destination Message Client **15** (or Source Message Client **11**), the Public Key must be reported to and maintained on the Destination Message Server **14** (or Source Message Server **12**) that the Recipient (or Sender) has an account with. The Destination Message Server **14** (or Source Message Server **12**) maintains a Client Database that contains records of its user accounts' information such as Electronic Mail Addresses, Public Keys, Key Generating Times, etc.

Typical steps of generating and maintaining an initial user's Public-Secret Key Pair are as follows:

1. Initially, when a Recipient (or Sender) sets up an account with a Destination Message Server **14** (or Source Message Server **12**), the Recipient (or Sender) uses a Destination Message Client **15** (or Source Message Client **11**) to log on the Destination Message Server **14** (or Source Message Server **12**) using the Recipient's (or Sender's) user ID and password.
2. The Destination Message Server **14** (or Source Message Server **12**) provides its most updated Public Key Set to the Destination Message Client **15** (or Source Message Client **11**) as described in the previous paragraphs.
3. The Destination Message Client **15** (or Source Message Client **11**) generates an initial Public-Secret Key Pair, and maintains a Public-Secret Key Set containing the Public-Secret Key Pair and the Key Generating Time.
4. The Destination Message Client **15** (or Source Message Client **11**) keeps the Secret Key private.
5. The Destination Message Client **15** (or Source Message Client **11**) encrypts the Recipient's (or Sender's) password and a Public Key Set, which contains the Recipient's (or Sender's) Public Key and Key Generating Time, with the Public Key of the Destination Message Server **14** (or Source Message Server **12**).

6. The Destination Message Client **15** (or Source Message Client **11**) reports, as an Information Flow **25** (or Information Flow **21**), the encrypted password and Public Key Set to the Destination Message Server **14** (or Source Message Server **12**).
7. The Destination Message Server **14** (or Source Message Server **12**) decrypts the encrypted password and Public Key Set with the Secret Key of the Destination Message Server **14** (or Source Message Server **12**), and ensures that the password is legitimate.
8. If the decryption succeeds and the password is legitimate, the Destination Message Server **14** (or Source Message Server **12**) adds the Public Key Set associated with the Recipient's (or Sender's) account to its Client Database.
9. If the decryption fails or the password is not legitimate, the administrators of the Destination Message Server **14** (or Source Message Server **12**) need to straighten things out.

As a common practice, the user usually works on a single Local Computer or Communication Apparatus, which performs as a Source Message Client **11** for outgoing Electronic Messages and as a Destination Message Client **15** for incoming Electronic Mail Messages of a user's account, to communicate with a single Host Computer, which performs as a Source Message Server **12** for outgoing Electronic Mail Messages and as a Destination Message Server **14** for incoming Electronic Mail Messages of its user accounts. Therefore, the above steps (1) to (9) only need to be

executed once for an account as a user rather than twice as a Sender and a Recipient separately.

Typical steps of regenerating and maintaining the user's Public-Secret Key Pair are as follows:

1. Whenever the Destination Message Client **15** (or Source Message Client **11**) regenerates the Recipient's (or Sender's) Public-Secret Key Pair associated with the Recipient's (or Sender's) account, the Destination Message Client **15** (or Source Message Client **11**) will maintain the new Public-Secret Key Set as the most updated version while keeping all old Public-Secret Key Sets.
2. The Destination Message Client **15** (or Source Message Client **11**) keeps all Secret Keys private.
3. The Destination Message Client **15** (or Source Message Client **11**) encrypts the Recipient's (or Sender's) new Public Key Set with the Recipient's (or Sender's) last Secret Key.
4. The Destination Message Client **15** (or Source Message Client **11**) reports, as an Information Flow **25** (or Information Flow **21**), the encrypted new Public Key Set to the Destination Message Server **14** (or Source Message Server **12**).
5. The Destination Message Server **14** (or Source Message Server **12**) decrypts

the encrypted new Public Key Set with the Recipient's (or Sender's) latest Public Key to authenticate the Recipient's (or Sender's) identity and obtain the Recipient's (or Sender's) new Public Key Set.

6. If the decryption succeeds, the Destination Message Server **14** (or Source Message Server **12**) updates the Public Key Set associated with the Recipient's (or Sender's) account in its Client Database.
7. If the decryption fails, the administrators of the Destination Message Server **14** (or Source Message Server **12**) need to straighten things out.

Again, usually the above steps (1) to (7) only need to be executed once as a user rather than twice as a Recipient and a Sender separately.

Based on the above description, the Source Message Server **12** and the Destination Message Server **14** maintain its account holder's Public Key Set; the user's Source Message Client **11** and Destination Message Client **15** maintain the Public Key Set of the Source Message Server **12** and the Destination Message Server **14** that administrate the user's account; and the Source Message Server **12** and the Destination Message Server **14** maintain each other's Public Key Set as long as a connection has been made; the maintained Public Key Sets are needed for delivering an Electronic Mail Message securely. Typical steps of delivering an Electronic Mail Message from a Sender to an intended Recipient are as follows:

1. The Sender uses a Source Message Client **11** to compose an Electronic Mail Message for delivery to an Electronic Mail Address that the Recipient is

entitled to, and specify an expiration condition of the Electronic Mail Message such as “after delivery to all Recipients”, on a fixed date, or a combination of both, etc.

2. The Source Message Client **11** establishes a connection to a Source Message Server **12** that the Sender has an account with, receives (an Information Flow **22**) and updates the Public Key Set of the Source Message Server **12** as described in the previous paragraphs.
3. The Source Message Client **11** transmits (an Information Flow **21**) the Electronic Mail Message to the Source Message Server **12**.
4. Upon receipt of the Electronic Mail Message, the Source Message Server **12** keeps it in an outgoing Electronic Mailbox specifically assigned to the Sender's account.
5. The Source Message Server **12** creates an Intend-To-Deliver which is an Electronic Mail Message containing the Sender's name, the Sender's Electronic Mail Address, a subject, a sending date, some identification codes of the Electronic Mail Message, the Registered Domain Name of the Source Message Server **12**, and the Public Key Set of the Source Message Server **12**, the Public Key Set associated with the Sender's account, etc.
6. The Source Message Server **12** sends (an Information Flow **23**) the Intend-To-Deliver to the Electronic Mail Address. Typical process is to deliver the Intend-To-Deliver, as Simple Mail Transfer Protocol (SMTP) does for an

Electronic Mail Message in the prior art, in a transport service environment that provides an inter-process communication environment covering the communication networks. In the inter-process communication environment, the Intend-To-Deliver is transported via some Intermediate Message Transporters, which receive an Electronic Mail Message from a Host Computer and transports the received Electronic Mail Message to another Host Computer for delivery to the Electronic Mail Address, until arriving a Destination Message Server **14**, which administrates an Electronic Mailbox associated with the Electronic Mail Address, as the ultimate destination.

7. Upon receipt of the Intend-To-Deliver, the Destination Message Server **14** encrypts the Recipient's Public Key Set with the Secret Key of the Destination Message Server **14**.
8. The Destination Message Server **14** establishes a connection to the Source Message Server **12** using the Registered Domain Name of the Source Message Server **12**, provides (an Information Flow **31**) the encrypted Recipient's Public Key Set and the Registered Domain Name of the Destination Message Server **14** to the Source Message Server **12**. The Destination Message Server **14** and the Source Message Server **12** also updates each other's Public Key Set as described in the previous paragraphs.
9. After receiving the encrypted Recipient's Public Key Set and updating the Public Key Set of the Destination Message Server **14**, the Source Message

Server **12** will decrypt the encrypted Recipient's Public Key Set with the Public Key of the Destination Message Server **14** to obtain and keep the Recipient's Public Key Set.

10. After providing the encrypted Recipient's Public Key Set to the Source Message Server **12**, the Destination Message Server **14** will append the Key Generating Time of the Recipient's Public Key Set to the Intend-To-Deliver, and deposit the Intend-To-Deliver in an incoming Electronic Mailbox for the Recipient to access.
11. The Recipient uses a Destination Message Client **15** to establish a connection to the Destination Message Server **14**, receive (an Information Flow **26**) and update the Public Key Set of the Destination Message Server **14** as described in the previous paragraphs, access (an Information Flow **26**) the Recipient's incoming Electronic Mailbox for any incoming Electronic Mail Messages including the Intend-To-Deliver.
12. If the Recipient determines to receive the Electronic Mail Message corresponding to the Intend-To-Deliver, the Recipient uses the Destination Message Client **15** to identify the Recipient's Secret Key associated the appended Key Generating Time in the Intend-To-Deliver.
13. The Destination Message Client **15** creates authentication information, which is a series of data codes encrypted with the identified Secret Key.
14. The Destination Message Client **15** creates a Request-For-Mail-Content

which is an Electronic Message containing the identification codes of the Electronic Mail Message, the Recipient's Electronic Mail Address, and the authentication information.

15. The Destination Message Client **15** establishes a connection to the Source Message Server **12** using the Registered Domain Name of the Source Message Server **12**, and provides (an Information Flow **27**) the Request-For-Mail-Content to the Source Message Server **12**.
16. Upon receipt of the Request-For-Mail-Content, the Source Message Server **12** identifies the Recipient's Public Key using the identification codes of the Electronic Mail Message and the Recipient's Electronic Mail Address, decrypts the authentication information with the identified Public Key to authenticate the Recipient's identity.
17. If the Recipient's identity is authenticated successfully, the Source Message Server **12** provides (an Information Flow **28**) the Electronic Mail Message to the Destination Message Client **15**, and records a delivery status such as “delivered to xxx” associated with the Electronic Mail Message.
18. If there are multiple Recipients, the above steps (7) to (17) should be executed for each Recipient separately.
19. Based on the expiration condition of the Electronic Mail Message, the Source Message Server **12** deletes the Electronic Mail Message from the Sender's outgoing Electronic Mailbox.

When the Destination Message Client **15** sends a Request-For-Mail-Content, even if the Sender didn't encrypt the Electronic Mail Message, the Recipient may instruct (an Information Flow **27**) the Source Message Server **12** to do so. Typical steps are as follows:

1. When the Destination Message Client **15** sends a Request-For-Mail-Content to the Source Message Server **12**, the Destination Message Client **15** adds an instruction of encrypting the Electronic Mail Message to the Request-For-Mail-Content.
2. After receiving the Request-For-Mail-Content and authenticating the Recipient's identity as in the above description, based on the instruction of encryption, the Source Message Server **12** randomly chooses a Session Key of Private Key Cryptography, encrypts the Electronic Mail Message with the chosen Session Key using Private Key Cryptography, and then encrypts the Session Key with the Recipient's Public Key using Public Key Cryptography.
3. The Source Message Server **12** provides (an Information Flow **28**) the encrypted Electronic Mail Message and the encrypted Session Key to the Destination Message Client **15**.
4. After receiving the encrypted Electronic Mail Message and the encrypted Session Key, the Destination Message Client **15** decrypts the encrypted Session Key with the Recipient's Secret Key to obtain the Session Key, and

then decrypts the encrypted Electronic Mail Message with the Session Key to obtain the Electronic Mail Message in an understandable format.

For convenience, the Recipient may provide a list of Electronic Mail Addresses to the Destination Message Server **14** and authorize the Destination Message Server **14** to automatically collect all Electronic Mail Messages sent from the listed Electronic Mail Addresses. Typical steps are as follows:

1. Initially, the Recipient uses the Destination Message Client **15** to provide (an Information Flow **25**) a list of Electronic Mail Addresses to the Destination Message Server **14**.
2. Upon receipt of an Intend-To-Deliver for the Recipient, the Destination Message Server **14** checks the Sender's Electronic Mail Address against the list of Electronic Mail Addresses. If the Sender's Electronic Mail Address is covered by the list of Electronic Mail Addresses, the Destination Message Server **14** will provide (an Information Flow **31**) the Public Key Set of the Destination Message Server **14**, instead of the Recipient's Public Key Set, to the Source Message Server **12**.
3. Then, the Destination Message Server **14** sends (an Information Flow **31**) a Request-For-Mail-Content containing authentication information, which is created using the Secret Key of the Destination Message Server **14**, to the Source Message Server **12**.
4. The Source Message Server **12** decrypts the authentication information with

the Public Key of the Destination Message Server **14** and responds (an Information Flow **32** or **23**) with the Electronic Mail Message to the Destination Message Server **14**.

5. After receiving the Electronic Mail Message, the Destination Message Server **14** deposits it into the Recipient's incoming Electronic Mailbox waiting for the Recipient to access.

Based on the above description, it is obvious that there are many advantages of the present invention, and some of the major advantages are:

1. The intended Recipient can avoid receiving an undesired Electronic Mail Message by not sending a Request-For-Mail-Content.
2. The Recipient does not need to open the Intend-To-Deliver but viewing the basic information in a list format. Other information in the Intend-To-Deliver will be automatically processed by the system that is more capable of obviating the pitfalls embedded in the Electronic Mail Message.
3. The Electronic Mail Message will be collected from a Host Computer that is authenticated and is assigned with a unique Domain Name registered with authoritative organizations. Therefore, the source of the Electronic Mail Message can be identified and tracked down if necessary.

FIG. 2 shows a special case of FIG. 1, in which Source And Destination

Message Server **326** is a single Host Computer that performs the functions of a Sender's Source Message Server and a Recipient's Destination Message Server for delivering an Electronic Mail Message. In this case, the execution steps are as same as those explained in the description of FIG.1 with the exception that the processes between the Source Message Server and the Destination Message Server are carried out internally or omitted. The Source Message Server and the Destination Message Server do not need to authenticate the other party's identity. Both the Sender and the Recipient can obtain the other party's Public Key Set easily via the Source And Destination Message Server **326**.

The present invention provides a system and method for delivering Electronic Mail Message in a deliver-upon-request manner. While the above description contains many specifications, these should not be construed as limitations on the scope of the invention, but rather as an exemplification of preferred embodiments thereof. Many other variations are possible.

It will be apparent to those skilled in the art that various modifications and variations can be made to the present invention without departing from the scope or spirit of the invention. In view of the foregoing, it is intended that the present invention cover modifications and variations of this invention provided they fall within the scope of the invention and its equivalent.

CLAIMS

What is claimed is:

1. A method of delivering an electronic mail message from a sending party to a receiving party, comprising:

sending an intend-to-deliver containing some basic information of the electronic mail message by the sending party to the receiving party;

providing a public key of public key cryptography by the receiving party to the sending party upon receipt of the intend-to-deliver;

responding to the intend-to-deliver with a request-for-mail-content containing authentication information, which is a series of data codes encrypted with a secret key associated with the public key, and instructions of delivery by the receiving party to the sending party if the receiving party determines to do so;

decrypting the authentication information with a public key, which is a member selected from the group consisting of the public key provided by the receiving party and a source that the sending party considers to be trustworthy, by the sending party upon receipt of the authentication information; and

responding to the request-for-mail-content with the electronic mail message by the sending party to the receiving party if and only if the decryption of the authentication information succeeds.