The invention is concerned with providing positive notifications of message receipt in a network comprising at least a sending device 1 (e.g. a sending MUA), a sending device 3 (e.g. a mail server or MTA of a sending device), a receiving exchange 5 (e.g. a mail server or MTA of a receiving device) and a receiving device 7. The server of the receiving device sends a notification of delivery of the message. Preferably, this notification includes a signed hash of the received email to provide a degree of non-repudiation. The signing may be carried out remotely from the receiving server. In some embodiments the sending and receiving devices must authenticate themselves to their respective exchanges using a sign-on procedure. The server 8 provides a DNS function, as is standard in the art. The method may also include certifying the exchanges and entering them into an exchange database 8, and the sending exchange and/or receiving exchange querying the exchange database to determine whether to communicate the message.
1

Reliable and rapid communication of messages

Background

This invention relates to the communication of electronic messages through electronic message exchanges, in which the sending device receives a notification of delivery of the electronic message to a receiving device.

Traditional message delivery systems, i.e. postal systems, are slow, sometimes unreliable and require expensive physical handling and transport of messages.

On the other hand, present electronic message communication systems, for example the widely used email system, are known to be unreliable, low in confidence and to be ‘polluted’ by large volumes of unsolicited messages. Very important in some industries is that the sender cannot force the recipient to confirm receipt of the message. Although the accepted standards for email do include this ‘proof of delivery’ capability, it is easily circumvented by recipients. Also, it is possible for the sender to record and timestamp the transmission of a message to another computer as evidence of delivery, but there are many steps that may be carried out in between the sender and receive which may prevent the message getting through – for example checking for electronic malware by an agent. The sender may not therefore have legally valid proof that the recipient received the message.

However, email has an advantage that a wide range of tools, for example ‘email clients’ or Mail User Agents (MUAs), are available to send and receive messages, and it is easy for organisations to develop software to automatically create, send, receive and process email-formatted messages for their particular needs. Email also has an advantage that it is easily expanded – the sender’s server can locate the recipient’s server using the Domain Name System, and the recipient’s server can then identify the recipient from the delivery address. The sender’s server does not have to know the recipient for the message transmission to be successful, allowing user numbers to grow easily over time without the burden of synchronising the user identities across the entire system.

There are emerging into the marketplace a number of secure document exchange systems which solve some of the above problems. However, they introduce new problems: they require specialist software and training, they are not convenient to use, and are not easily expanded because all recipients must be known to the sending server for the communication to be successful.

It is therefore an object of the present invention to provide a method of communicating electronic messages that allows the sender to prove the receipt of a message by a recipient, while using existing software and while allowing for an easily expandable communication network.

Statement of Invention

A first aspect of the invention is a communication method according to Claim 1, which is hereby included by reference.

Preferred and optional features of the invention are set out in the dependent Claims, which are hereby included by reference.
A second aspect of the invention includes computer program code implementing the invention according to the first aspect.

A third aspect of the invention includes computer hardware utilising computer program code according to the second aspect.

**Description of Preferred Embodiments**

The example embodiment of the invention will now be described with reference to the following Figures:

Figure 1, showing a communication system according to the invention.

Figure 1 shows a first personal computer (PC) (1) running any one of a number of different Mail User Agent (MUA) programs (together acting as the sending device) and communicating over an internet TCP/IP connection (2) to a first computer server (3) running some software adapted to perform parts of the method of this invention (together acting as the sending server). The first computer server communicates over an internet TCP/IP connection (4) to a second computer server (5) running some software adapted to perform parts of the method of this invention (together acting as the receiving server), which in turn communicates over an internet TCP/IP connection (6) with a second PC (7) running any one of a number of different MUA programs (together acting as the receiving device). Each computer server includes databases (not shown), and is able to communicate with a third computer server (8) providing a Domain Name System (DNS) function for one internet domain and a store of cryptographic keys (acting as the server database) and a cryptographic signing function via internet TCP/IP connections (9,10).

In use, the first and second computer servers are first tested to ensure that they comply with a specification describing their operation (which is to be described below). Testing includes examining the computer software code and observing the operation of the computer servers in a test environment. If the servers pass the tests, the identity of each server is stored on the third computer server (8). For example a certified server may have its TCP/IP address added to the DNS database and associated with a subdomain (for example s1.privatenetwork.net and s2.privatenetwork.net) and/or a public key, corresponding to a private cryptographic key known only to the certified server, is stored in the third computer server.

Usernames and passwords (acting as the credentials) are posted by letter to the owners of the first and second PCs, who configure the PCs with the credentials. The usernames and passwords are also stored in the first and second servers respectively, as are public and private key pairs for each owner.

To transmit a message, the first PC contacts the first server using an encrypted variant of, for example, the common SMTP protocol, and authenticates with the username and password it was provided with. The first server checks the username and password are stored in its database and accepts a message containing a recipient address from the first PC if they are. The message may comprise attachments such as documents and images. The first server then sets the sender header of the message to the username (acting as the individual portion) followed by “@” (acting as the exotic character) and followed by “s1.privatenetwork.net” (acting as the server portion):

Smith.LLP@s1.privatedomain.net

It then communicates the part of the recipient address coming after an “@” (acting as the server portion) in a ‘DNS lookup’ to some DNS server (e.g. the third server) to obtain the TCP/IP address of the second server. (If the server portion of the recipient header cannot be found, the first server places
a failure message into a delivery queue for the first PC.) The first server now computes an SHA-2 hash (acting as the cryptographic hash) of the message to concatenate with the first message to form a second message, signing the hash with the private key associated with the sender. The first server then obtains from the third server the public key corresponding to the second server and initiates an encrypted conversation with the second server using, for example, the common SMTP protocol.

The second server verifies the certification of the first server by performing a ‘Reverse DNS lookup’ of the first server’s TCP/IP address on for example the third server, and/or by checking the first server’s knowledge of its own private key, the corresponding public key of which is communicated to the second server by the third server. The second message is then transmitted to the second server, and the first server deletes the first and second messages.

The second server examines the part of the recipient address coming before the “@” (acting as the individual portion) and determines whether the recipient is known to the second server. If it is not known, the second server communicates a failure notification to the first PC (now acting as the notification receiving device) by transmitting it to the first server. If the recipient is known, the second server holds the message in a queue for the second PC. After some time, for example after 24 hours or 48 hours or longer when there is a holiday or weekend, the second server will transmit a notification message for the first PC to the first server to inform the owner of the first PC that the message was not delivered.

However, at some time after receiving the second message, the second PC contacts the second server using an encrypted variant of, for example, the common POP or IMAP protocols, supplies a username and password which the second server checks against its records, and receives the message (acting as the third message) from the second server. On completing the transmission, the second server creates a notification message comprising the message received from the first server, a delivery notice describing the date and/or time it delivered the message, and a cryptographic hash of the other parts of the message. The delivery notice may include the IP address or some other identifying information about the first PC, second PC, first server or second server, and dates or times associated with the communication of any preceding messages. The second server transmits the hash to the third server or another server which cryptographically signs the hash using a private key and returns it to the second server. The second server then sends the notification message to the first PC using the reverse of the method just described – the first PC again acts as the notification receiving device. The second server also deletes the second and third messages and the notification message.

The first PC then checks the authenticity of the cryptographic hash included in the notification message and informs its owner or user that the notification message has been received and that the hash is valid. It may then also tag the original message or link it to the notification message to indicate that the message was delivered.

**Advantageous Features**

Several optional features could be included in the communication system just described.

The first PC could provide personal and organisational parts of the individual portion of the recipient address, or for its own sender address. For example, the recipient address could be:

\[\text{Lloyd\_Smith}\text{Smith.LLP@s1.privatedomain.net}\]

The second server could provide the message to a second PC that supplies credentials matching only the organisational and server portions of the address (in this case Smith.LLP@s1.privatedomain.net). The second PC could then pass the third message to a final recipient, for example a third PC known to
it by examining and interpreting the personal part \({\{\text{Lloyd\_Smith}\}}\), which has been delineated by the “{“ and “}” characters, acting as exotic characters. The personal part might also include a code recognised by the sender or recipient or both:

636225/2241A\{\text{Lloyd\_Smith}\}Smith.LLP@s1.privatedomain.net

It may be possible that the server portion is not a valid internet domain, for example it might be a private domain such as “s1.r4s”.

636225/2241A\{\text{Lloyd\_Smith}\}Smith.LLP@s1.r4s

It is also possible that the first PC has received the message it transmitted to the first server from another PC, and it may modify the sender address by adding codes, names etc. to the message.
Claims

1. A method of communication in which a sending exchange is contacted by and receives a first electronic message comprising a recipient address from a sending device, the sending exchange then communicates a second electronic message to a receiving exchange associated with the recipient address, and the receiving exchange communicates a third electronic message to a receiving device associated with the recipient address, characterised in that the receiving exchange afterward communicates a notification message to a notification receiving device, notifying the notification receiving device of the successful communication of the third message to the receiving device.

2. The method of any preceding Claim wherein the second, third and notification messages comprise at least some of the content of one of the first, second or third messages.

3. The method of any preceding Claim wherein the notification message includes the date or time of the successful communication of the third message to the receiving device.

4. The method of any preceding Claim wherein the exchanges delete any messages they communicated after successful communication.

5. The method of any preceding Claim further including the step of forming a cryptographic hash of one of the first, second or third messages, creating a signed cryptographic hash by signing the cryptographic hash with a private key, and attaching the signed cryptographic hash to any of the messages.

6. The method of Claim 5 further including the steps of one of the exchanges communicating the cryptographic hash to a remote signing exchange for signing, and communicating the signed cryptographic hash back to the exchange that communicated the cryptographic hash, and including the signed cryptographic hash into a later message communicated by the exchange.

7. The method of any preceding Claim wherein each communication step utilises an encrypted communication channel.

8. The method of any preceding Claim wherein at least the second and third messages comprise a sender address associated with the sending device.

9. The method of Claim 8 wherein the sending exchange sets the sender address of the second message to match an entry in the sender database corresponding to the credentials supplied by the sending device.

10. The method of any preceding Claim wherein the sender address or recipient address comprises an individual portion and a exchange portion.

11. The method of any preceding Claim wherein the sending exchange comprises a sender database and the method includes the step of refusing the first message when the sending device does not supply credentials matching an entry in the sender database.

12. The method of any preceding Claim wherein the receiving exchange comprises a recipient database and communicates messages only to receiving devices that supply credentials matching an entry in the recipient database.
13. The method of any preceding Claim wherein the receiving exchange comprises a recipient database and the method includes the step of refusing the second message when the recipient address doesn’t match an entry in the recipient database.

14. The method of any preceding Claim further including the step of performing a certifying test wherein the operation of an exchange is tested against a specification, and entering the exchange into an exchange database if it achieves the specification.

15. The method of Claim 14 wherein the certifying step comprises inspecting the operating code of the exchange.

16. The method of any of Claims 14 to 15 wherein the certifying step comprises a process of automated communication with the exchange and automated analysis of the observable behaviour of the exchange.

17. The method of any of Claims 14 to 16 wherein the certifying step is repeated regularly.

18. The method of any of Claims 14 to 17 wherein the exchange is removed from the exchange database if it does not achieve the specification.

19. The method of any of Claims 14 to 18 wherein the sending exchange checks the exchange portion of the recipient address matches an entry in the exchange database and refuses the first message if it does not.

20. The method of any of Claims 14 to 19 wherein the receiving exchange checks that the sending exchange is in the exchange database and refuses the message if it is not.

21. The method of Claim 20 further including the step of identifying the sending exchange from the exchange portion of the sender address or the IP address of the sending exchange or a cryptographic certificate communicated by the sending exchange.

22. The method of any of Claims 14 to 21 wherein the exchange database comprises a Domain Name System (DNS) server and wherein a plurality of sending exchanges or receiving exchanges are recorded as subdomains of one internet domain.

23. The method of any of Claims 14 to 22 wherein the exchange database comprises a database of cryptographic keys for identifying sending exchanges and receiving exchanges.

24. The method of any preceding Claim wherein the second message comprises a cryptographic hash of the first message signed with a key associated with the sending device.

25. The method of any preceding Claim wherein the individual portion of an address itself comprises a personal portion and an organisational portion, and the step of matching the individual portion against the recipient database includes the step of ignoring the personal portion.

26. The method of any of Claims 10 to 25 wherein portions of an address are delineated by at least one exotic character.

27. The method of any preceding Claim further including the step of communicating a further message to the notification receiving device if the communication of the second or third messages does not occur within a certain defined time of any of the previous communication steps.
28. The method of any preceding Claim further comprising the step of the receiving device contacting the receiving exchange before the communication of the third message to the receiving device.

29. The method of any preceding Claim where any of the sending or receiving exchanges or sending or receiving devices communicate using a standard internet protocol.

30. The method of any preceding Claim wherein the receiving device is a widely available Mail User Agent, and the messages are email messages.

31. The method of any preceding Claim wherein the receiving device notifies the receiving exchange when the third message has been read, and the receiving exchange notifies the notification receiving device.

32. The method of Claims 11 to 30 wherein the step of refusing the message includes the step of sending a notification message to the notification receiving device.

33. The method of Claims 11 to 32 wherein the step of refusing the message includes the step of refusing the communication of at least part of the message.

34. The method of any preceding Claim further including the step of the sending exchange recording that a payment is due from the operator of the sending device.

35. The method of any preceding Claim further including the step of the receiving exchange recording that a payment is due from the operator of the sending exchange.

36. The method of any preceding Claim further including the step of the receiving exchange recording that a payment is due to the operator of the receiving device.

37. The method of any preceding Claim further including the step of checking the identity of the operator of the sending device or the receiving device, prior to entering the credentials required of the sending device or the receiving device into the sender database or the receiver database respectively.

38. The method of any preceding Claim wherein the step of checking the identity of a device owner includes sending a postal letter to the device owner, the postal letter comprising at least part of the credentials.

39. The method of any preceding Claim wherein the functions of the sending exchange and the receiving exchange are performed within one physical device.

40. The method of any preceding Claim wherein the functions of the sending device and the notification receiving device are performed within one physical device.
Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

<table>
<thead>
<tr>
<th>Category</th>
<th>Relevant to claims</th>
<th>Identity of document and passage or figure of particular relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>1-5, 7, 8, 10, 22, 27 and 29 at least</td>
<td>WO02/011025 A2 (RPOST) See whole document but note in particular Figs. 1, 2B, 2C, line 22 of p14 to line 7 of p15, lines 14-19 of p21, p25 and lines 3-12 of p34.</td>
</tr>
<tr>
<td>X</td>
<td>1-3, 5 and 7 at least.</td>
<td>US2009/006851 A1 (FREEMAN) See Figs. 1 and 5E-G, and para 23.</td>
</tr>
<tr>
<td>X</td>
<td>1, 2, 5 and 7 at least.</td>
<td>US5812669 A (JENKINS) See Abstract and Figs. 1 and 3.</td>
</tr>
<tr>
<td>X</td>
<td>1, 2, 5 and 12 at least</td>
<td>US2009/144382 A1 (BENNINGHOFF) See Figs. 1-6.</td>
</tr>
<tr>
<td>X</td>
<td>1, 2, 5 and 6 at least</td>
<td>WO2007/071040 A1 (KRYPTIVA) See Figs. 1 and 5, and Para 110.</td>
</tr>
</tbody>
</table>

Categories:

- X Document indicating lack of novelty or inventive step
- Y Document indicating lack of inventive step if combined with one or more other documents of same category.
- & Member of the same patent family

- A Document indicating technological background and/or state of the art.
- P Document published on or after the declared priority date but before the filing date of this invention.
- E Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC:

Worldwide search of patent documents classified in the following areas of the IPC
H04L

The following online and other databases have been used in the preparation of this search report
Online: WPI, EPODOC

**International Classification:**

<table>
<thead>
<tr>
<th>Subclass</th>
<th>Subgroup</th>
<th>Valid From</th>
</tr>
</thead>
<tbody>
<tr>
<td>H04L</td>
<td>0012/58</td>
<td>01/01/2006</td>
</tr>
<tr>
<td>H04L</td>
<td>0009/32</td>
<td>01/01/2006</td>
</tr>
</tbody>
</table>