(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 January 2010 (28.01.2010)

PCT

(10) International Publication Number
WO 2010/011443 A1

(51) International Patent Classification:
H04L 12/58 (2006.01)

(21) International Application Number:
PCT/US2009/047588

(22) International Filing Date:
17 June 2009 (17.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/176,935 21 July 2008 (21.07.2008) US

(71) Applicant *(for all designated States except US)*: **RAYTHEON COMPANY** [US/US]; 870 Winter Street, Waltham, MA 02451-1449 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **RODRIGUEZ, Ricardo, J.** [US/US]; 4815 70th Street East, Palmetto, FL 34221-7321 (US). **VISARIA, Jay, J.** [US/US]; 5503 110th Avenue, Pinellas Park, FL 33782-2228 (US). **PIPPINS, Jerry, L., Jr.** [US/US]; 17615 White Tail Court, Parrish, FL 34219-5046 (US). **OBERAI, Tina, A.** [US/US]; 4141 Bayshore Boulevard, No. 1403, Tampa, FL 33611-1802 (US). **FARLEY, Thomas, D.** [US/US]; 2014 Butch Cassidy Trail, Wimauma, FL 33598-7803 (US). **STAHL, Noah, Z.** [US/US]; 1653 67th Lane North, St. Petersburg, FL 33710 (US).

(74) Agent: **WILLIAMS, Bradley, P.**; Baker Botts, L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

WO 2010/011443 A1

(54) **Title**: SECURE E-MAIL MESSAGING SYSTEM

(57) **Abstract**: According to one embodiment, a secure e-mail messaging system includes an e-mail relay server coupled to a secure client configured on a secure domain and an external client configured on an external domain. The e- mail relay server has a memory for storage of an actual address of the secure client, a first certificate associated with the actual address, an alias address associated with the actual address, and a second certificate associated with the alias address. The e- mail relay server receives an e-mail message that includes the alias address from the external client and decrypts the e-mail message according to the second certificate. The e-mail messaging server then replaces the alias address with the actual address to form a modified e-mail message, encrypts the modified e-mail message according to the first certificate, and transmits the modified e-mail message to the secure client.

SECURE E-MAIL MESSAGING SYSTEM

TECHNICAL FIELD OF THE DISCLOSURE

This disclosure generally relates to communication systems, and more particularly, to an e-mail messaging system and a method of operating the same.

BACKGROUND OF THE DISCLOSURE

Many network computing systems use a distributed architecture in which individual computers may be communicate with one another using various communication protocols, such as an Ethernet or token ring protocol. Computing systems configured in networks may provide particular advantages over those configured in traditional centralized computing architectures. For example, computing systems configured in networks may provide an efficient means of communication with one another. Organizations often use network computing systems that are configured in one or more domains to handle many of their organizational processes.

SUMMARY OF THE DISCLOSURE

According to one embodiment, a secure e-mail messaging system includes an e-mail relay server coupled to a secure client configured on a secure domain and an external client configured on an external domain. The e-mail relay server has a memory for storage of an actual address of the secure client, a first certificate associated with the actual address, an alias address associated with the actual address, and a second certificate associated with the alias address. The e-mail relay server receives an e-mail message that includes the alias address from the external client and decrypts the e-mail message according to the second certificate. The e-mail messaging server then replaces the alias address with the actual address to form a modified e-mail message, encrypts the modified e-mail message according to the first certificate, and transmits the modified e-mail message to the secure client.

Some embodiments of the disclosure may provide numerous technical advantages. For example, one embodiment of the secure e-mail messaging system provides enhanced security over other known e-mail messaging systems. Using the secure e-mail messaging system of the present disclosure, e-mail messages may be transmitted between domains while hiding sensitive information, such as the domain structure of either domain involved in the e-mail transaction.

Certificates may be used enhance the security of e-mail communications. These certificates, however, may include sensitive information about the domain structure that may form a breach of security. Certain embodiments of the secure e-mail messaging system hides certificates associated with clients configured on the secure domain from other clients configured on external domains to enhance the security of secure domain.

Some embodiments may benefit from some, none, or all of these advantages. Other technical advantages may be readily ascertained by one of ordinary skill in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of embodiments of the disclosure will be apparent from the detailed description taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram showing one embodiment of a secure e-mail messaging system according to the teachings of the present disclosure;

FIGURE 2 is a diagram showing several elements of one embodiment of an e-mail relay server that may be used with the secure e-mail messaging system of FIGURE 1; and

FIGURE 3 is a flowchart showing one embodiment of a series of actions that may be performed by the e-mail handler process of FIGURE 2 to transfer e-mail messages from the external domain to the secure domain of FIGURE 1.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

As described previously, organizations often use network computing systems to handle many of their organizational processes. Network computing systems used by organizations may be structured in domains for ease of administration by maintenance personnel. These network computing systems may also be coupled to publicly accessible networks, such as the Internet, to extend their processing capability to other organizations. For example, organizations may be coupled together through the Internet to provide various communication services between organizations, such as e-mail messaging services, voice services, and/or instant messaging services.

Organizations often use information that may be confidential in nature. Due to the generally insecure nature of commonly known network architectures, organizations seek to manage the nature and type of information that may be shared externally with others. The United States Department of Defense (DoD), for example, has issued a Director of Central Intelligence Directive 6/3 (DCID 6/3) entitled "Protecting Sensitive Compartmented Information Within Information Systems." The Director of Central Intelligence Directive 6/3 generally includes a set of guidelines including several ascending levels of protection that extend from a protection level 0 (PL0) to a protection level 5 (PL5).

The protection level 4 (PL4) protection level specifies that "The security support structure shall maintain separate execution domains (e.g., address spaces) for each executing process." This requirement has not heretofore been possible using known e-mail messaging mechanisms or protocols. That is, known e-mail messaging protocols utilize a header structure including a sender's address portion and a recipient address portion that may be generally unalterable following creation of the e-mail message. Access to the sender's address portion and/or recipient address portion may create a breach of security, a problem that may not be solved using known e-mail messaging systems.

FIGURE 1 shows one embodiment of a secure e-mail messaging system 10 that may provide a solution to this problem as well as other problems. Secure e-mail messaging system 10 includes an e-mail relay server 12 that couples a secure client 14 configured on a secure domain 16 through a domain gateway 18 with an external client 20 configured on an external domain 22. E-mail relay server 12 is also coupled to a guard node 24. According to the teachings of the present disclosure, e-mail relay server 12 separates secure domain 16 from external domain 22 by isolating the domain structure of secure domain 16 from external domain 22. That is, provisions are made for e-mail communication of secure client 14 with external client 20 without revealing the domain structure of secure domain 16.

Secure domain 16 may be any type of network computing system that maintains a secure environment from external domain 22. Secure domain 16 may include, for example, a network computing system of an organization, such as the Department of Defense (DoD) that handles confidential information as part of its organizational processes. External domain 22 may be any other computing system, such as a stand-alone computing system, a distributed computing system, or other network computing system, such as the Internet or an intranet of another organization. In one embodiment, secure domain 16 and external domain 22 are administered by a single organization that administers communication with differing levels of security. For example, the Department of Defense may implement secure domain 16 to have a "top secret" security level and external domain 22 to have a "secret" security level. In other embodiments, secure domain 16 and external domain 22 may form a portion of an organization, such as the Department of Defense, having multi-tiered levels of security in which various domains that are separated from one another according to various corresponding caveats or sub-security levels.

E-mail relay server 12 separates secure domain 16 from any external domain 22 as described above. In this respect, the term "separated" refers to the quality of hiding the domain structure of secure domain 16 from external domain 22 and/or isolating certificates issued within secure domain 16 from those issued to external domain 22. Use of the domain structure within the e-mail message may provide benefits for the organization if used internally. For example, administrators may diagnose faults in a relatively efficient manner using the domain structure information included in e-mail messages. This information, however, may compromise the security of secure domain 16 if allowed access by others outside of secure domain 16. Access to certificates issued within secure domain 16 by users from external domains 22 may also provide a breach of security. Certificates typically include information to verify the identity and address information of secure clients 14 configured on secure domain 16. Knowledge of this information may therefore be detrimental to the security of secure domain 16. Thus, e-mail relay server 12 separates secure domain 16 from external domain 22 by hiding the address of secure client 14 and any certificates associated with secure client 14.

Secure client 14 and external client 20 may include any suitable type of e-mail client that transmits or receives e-mail messages, such as Mozilla Thunderbird, Microsoft Mail, or Pegasus Mail. Secure client 14 transmits or receives e-mail messages to or from, respectively, another secure client configured on secure domain 16 or external client 20 configured on external domain 22. Domain gateway 18 may be provided to route e-mail messages between secure domain 16 and external domain 22. In one embodiment, domain gateway 18 includes an adjudicator device that regulates communication services of secure clients 14 in secure domain 16 to those in external domain 22. In another embodiment, domain gateway 18 configured as an adjudicator restricts information received by or transmitted from secure client 14 in a compartmented fashion according to a protection level 3 (PL3) protection level. For example, domain gateway 18 may restrict access by secure client 14 or external client 20 to published information according to a security level of the respective client. According to this example, domain gateway 18 may negotiate a login session with secure client 14 or external client 20, and subsequently allow access to information according to a security level of the login session.

Guard node 24 is executed on any suitable computer having a processor that executes instructions stored in a memory. Guard node 24 verifies e-mail messages processed by e-mail relay server 12. Upon receipt of e-mail messages, e-mail relay server 12 decrypts the e-mail messages and forwards the decrypted e-mail messages to guard node 24 for verification. Guard node 24 may verify e-mail messages according to one or more rules. Verification of e-mail messages may trap various malicious intruder attempts to gain illicit access to secure domain 16. For example, guard node 24 may compare sender or recipient addresses included in the e-mail messages and reject any that are suspicious. In one embodiment, guard node 24 searches the body portion of e-mail messages for suspicious or illicit content. For example, the body portion of e-mail messages may be searched, such as with a regular expression search, to determine if content is found that may be inconsistent with the security level of the sender or recipient. If malicious or illicit content is found, the message may be restricted from being forwarded to the recipient address.

FIGURE 2 is a diagram showing several elements of one embodiment of an e-mail relay server 12 that may be used with the secure e-mail messaging system 10 of FIGURE 1. E-mail relay server 12 may be implemented on any suitable computing system, such as a personal computer, a laptop computer, a workstation, or a network of multiple computers configured on a local area network (LAN). E-mail relay server 12 includes a simple mail transport protocol (SMTP) server 28, a memory 30, and a port 32 for communication with guard node 24. E-mail relay server 12 also executes an e-mail handler process 34 that executes instructions stored in memory 30. Operation of e-mail handler process 34 will be described in detail below.

Simple mail transport protocol server 28 is coupled to secure domain 16 and external domain 22 for relaying e-mail messages between one another. In one embodiment, e-mail relay server 12 includes multiple simple mail transport protocol servers 28 that are each individually coupled to secure domain 16 and external domain 22. In the particular embodiment shown, simple mail transport protocol server 28 communicates with secure domain 16 and external domain 22 using a simple mail transport protocol; however, any suitable e-mail messaging protocol may be used, such as a post office protocol (POP) or an Internet message access protocol (IMAP).

Memory 30 stores an account 36 for each secure client 14 registered on secure domain 16. Account 36 may be generated due to registration of secure client 14 and prior to communication of secure client 14 with external client 20. Each account 36 includes an actual address 38 of secure client 14. Upon registration, a certificate 40 is generated to provide secure communication within secure domain 16. An alias address 42 is also generated and bound to actual address 38 such that, when an e-mail message is sent to or from secure domain 16, e-mail handler process 34 may associate actual address 38 with alias address 42. Certificate 40 may include identifiable information about secure client 14. Providing access to certificate 40 may create a breach of security whereby illicit users may obtain information about secure client 14. Thus, certificate 44 is generated to provide secure communication of alias address 42 with external client 20 while alleviating the need to subject certificate 40 to use outside of secure domain 16.

Port 32, which couples e-mail relay server 12 to guard node 24, may be any suitable type of communication port, such as an Ethernet port or other suitable data communication port. In one embodiment, port 32 includes a queue for temporary storage of e-mail messages between guard node 24 and e-mail handler process 34. In one embodiment, e-mail messages conveyed between e-mail handler process 34 and guard node 24 may be wrapped in an extensible markup language (XML) message to facilitate parsing of information by guard node 24. In another embodiment, e-mail messages or extensible markup language messages encapsulating the e-mail messages may be encrypted prior to being transmitted to or from port 32.

Modifications, additions, or omissions may be made to secure e-mail messaging system 10 without departing from the scope of the disclosure. The components of secure e-mail messaging system 10 may be integrated or separated. For example, the functions of guard node 24 may be integrated with e-mail handler process 34 on e-mail relay server 12. Additionally, operations of e-mail relay server 12 may be performed using any suitable logic comprising software, hardware, and/or other logic. As used in this document, "each" refers to each member of a set or each member of a subset of a set.

FIGURE 3 is a flowchart showing one embodiment of a series of actions that may be performed by e-mail handler process 34 to transfer e-mail messages from external domain 22 to secure domain 16. In act 100, the process is initiated.

In act 102, e-mail handler process 34 receives an e-mail message from external client 20 configured on external domain 22. The e-mail message has several fields, such as a sender's address, a recipient address, and a body portion that includes text, graphics, or other useful information intended for view by secure client 14. An alias address is provided to external client 20 rather than the actual e-mail address of secure client 14 in order to hide the domain structure from view outside of secure domain 16. Thus, the recipient address includes alias address 42 of secure client 14. The e-mail message may be encrypted using any suitable approach.

In act 104, e-mail handler process 34 decrypts the e-mail message according to certificate 44 associated with alias address 42. Certificate 44 is issued to external client 20 for encrypting e-mail message prior to transmission. In one embodiment, e-mail message is decrypted according to a certificate 44 that includes a public key associated with alias address 42 and a private key associated with external client 20. The public key may be used to ensure the privacy of the e-mail message while the private key verifies the signature of external client 20.

In act 106, e-mail handler process 34 verifies e-mail message according to one or more rules. The quantity and type of rules may include any rule that ensures particular procedures are followed to maintain security of secure domain 16. For example, a particular rule may check the e-mail message to ensure that the domain structure is not included in the recipient address of the e-mail message. As another example, e-mail handler process 34 may perform a general search of the body portion of the e-mail message for particular words or phrases that may be inappropriate for view outside of secure domain 16. If any of the rules are violated, other measures may be taken, such as deletion of the e-mail message, quarantining of the e-mail message, or alerting management personnel of the suspect e-mail message.

In one embodiment, elements of the e-mail message may be transmitted to guard node 24 for verifying the e-mail message according to the one or more rules. In this embodiment, e-mail handler process 34 wraps the e-mail message in an extensible markup language (XML) message and transmits the extensible markup language message to guard node 24. Certain embodiments in which rules are verified using a guard node 24 that is separate from e-mail relay server 12 may provide an advantage in that administration of the one or more rules may be simplified using a independently managed computing system.

In act 108, e-mail handler process 34 replaces the alias address 42 with the actual address 38 in the recipient address portion of the e-mail message.

In act 110, e-mail handler process 34 encrypts the modified e-mail message according to another certificate 40 associated with actual address 38. In one embodiment, certificate 40 includes a public key of actual address 38 and a private key of alias address 42. The public key of actual address 38 may be used to ensure privacy of the e-mail message while the private key of the alias address may be used to sign the message. That is, the private key may be used to verify the identity of secure client 14 such that the originator of the e-mail message was not spoofed by an illicit user.

In act 112, the encrypted e-mail message is transmitted to secure client 14 using the actual address 38.

The previously described process may be repeated with each e-mail message transmitted from an external client 20 to secure client 14. To transmit an e-mail message from secure client 14 to external client 20, the previously described process may be reversed. In act 114, the process ends.

Modifications, additions, or omissions may be made to the method without departing from the scope of the invention. The method may include more, fewer, or other acts. For example, the e-mail message may be encrypted prior to transmission or receipt from e-mail relay server 12 to guard node 24. In this manner, security of the e-mail message may be maintained throughout the transmission path of e-mail messages.

Although the present disclosure has been described with several embodiments, a myriad of changes, variations, alterations, transformations, and modifications may be suggested to one skilled in the art, and it is intended that the present disclosure encompass such changes, variations, alterations, transformation, and modifications as they fall within the scope of the appended claims.

What is claimed is:

1. A secure e-mail messaging system comprising:

an e-mail relay server coupled to a secure client configured on a secure domain and an external client configured on an external domain, the e-mail relay server having a memory for storage of an actual address of the secure client, a first certificate associated with the actual address, an alias address associated with the actual address, and a second certificate associated with the alias address, the e-mail relay server operable to:

receive an e-mail message comprising the alias address from the external client, the e-mail message being encrypted according to the second certificate;

decrypt the e-mail message according to the second certificate;

replace the alias address with the actual address to form a modified e-mail message;

encrypt the modified e-mail message according to the first certificate; and

transmit the modified e-mail message to the secure client.

2. The secure e-mail messaging system of Claim 1, wherein the e-mail relay server is further operable to:

receive another e-mail message comprising the actual address from the secure client, the e-mail message being encrypted according to the first certificate;

encrypt the another e-mail message according to the first certificate;

replace the actual address with the alias address to form another modified e-mail message;

encrypt the another modified e-mail message according to the second certificate; and

transmit the another modified e-mail message to the external client.

3. The secure e-mail messaging system of Claim 1, wherein the e-mail relay server is operable to decrypt the e-mail message according to the second certificate by decrypting the e-mail message according to a private key of the alias address and verify an external address of the external client according to a public key of the external client.

4. The secure e-mail messaging system of Claim 1, wherein the first domain comprises a secure network having a security level that differs from the security level of the second domain.

5. The secure e-mail messaging system of Claim 1, wherein the first certificate is isolated from the second domain and the second certificate is isolated from the first domain.

6. The secure e-mail messaging system of Claim 1, further comprising a guard node coupled to the e-mail relay server, the guard node operable to verify the e-mail message according to a plurality of rules.

7. The secure e-mail messaging system of Claim 6, wherein the guard node is operable to verify the first e-mail message by searching the body portion for instances of one of a plurality of key phrases or one of a plurality of keywords and if found, restrict the e-mail

relay server from transmitting the modified e-mail message.

8. The secure e-mail messaging system of Claim 1, wherein e-mail relay server is coupled to the secure client through a domain gateway, the domain gateway operable to compartment information transmitted from the secure domain to the external domain.

9. A secure e-mail messaging method comprising:

receiving an e-mail message comprising an alias address from an external client configured on an external domain, the alias address associated with an actual address of a secure client configured on a secure network, the e-mail message being encrypted according to a second certificate associated with the alias address;

decrypting the e-mail message according to the second certificate;

replacing the alias address with the actual address to form a modified e-mail message;

encrypting the modified e-mail message according to a first certificate associated with the actual address; and

transmitting the modified e-mail message to the secure client.

10. The secure e-mail messaging method of Claim 9, further comprising receiving another e-mail message comprising the actual address from the secure client, the e-mail message being encrypted according to the first certificate, encrypting the another e-mail message

according to the first certificate, replacing the actual address with the alias address to form another modified e-mail message, encrypting the another modified e-mail message according to the second certificate, and transmitting the another modified e-mail message to the external client.

11. The secure e-mail messaging method of Claim 9, wherein decrypting the e-mail message according to the second certificate further comprises decrypting the e-mail message according to a private key of the alias address and verifying an external address of the external client according to a public key of the external client.

12. The secure e-mail messaging method of Claim 9, wherein receiving the e-mail message from the external client configured on the external domain comprises receiving the e-mail message from the external client configured on the external domain having a security level that differs from the security level of the secure domain.

13. The secure e-mail messaging method of Claim 9, wherein encrypting the modified e-mail message according to the first certificate comprises encrypting the modified e-mail message according to the first certificate that is isolated from the external domain.

14. The secure e-mail messaging method of Claim 9, further comprising verifying the e-mail message according to a plurality of rules.

15. The secure e-mail messaging method of Claim 14, wherein verifying the e-mail message according to a plurality of rules comprises searching the body portion for instances of one of a plurality of key phrases or one of a plurality of keywords and if found, restricting the e-mail relay server from transmitting the modified e-mail message.

16. The secure e-mail messaging method of Claim 9, further comprising compartmenting information that is transmitted from the secure domain to the external domain.

17. Code embodied on a computer-readable medium, when executed on a computer processor, operable to perform at least the following:

receive an e-mail message comprising an alias address from an external client configured on an external domain, the alias address associated with an actual address of a secure client configured on a secure network, the e-mail message being encrypted according to a second certificate associated with the alias address;

decrypt the e-mail message according to the second certificate;

replace the alias address with the actual address to form a modified e-mail message;

encrypt the modified e-mail message according to a first certificate associated with the actual address; and

transmit the modified e-mail message to the secure client.

18. The code of Claim 17, further operable to receive another e-mail message comprising the actual

address from the secure client, the e-mail message being encrypted according to the first certificate, encrypt the another e-mail message according to the first certificate, replace the actual address with the alias address to form another modified e-mail message, encrypt the another modified e-mail message according to the second certificate, and transmit the another modified e-mail message to the external client.

19. The code of Claim 17, further operable to decrypt the e-mail message according to the second certificate by decrypting the e-mail message according to a private key of the alias address and verifying an external address of the external client according to a public key of the external client.

20. The code of Claim 17, further operable to receive the e-mail message from the external client configured on the external domain that has a security level that differs from the security level of the secure domain.

21. The code of Claim 17, further operable to encrypt the modified e-mail message according to the first certificate that is isolated from the external domain.

22. The code of Claim 17, further operable to verify the e-mail message according to a plurality of rules.

23. The code of Claim 22, further operable to verify

the e-mail message by searching the body portion for instances of one of a plurality of key phrases or one of a plurality of keywords and if found, restricting the e-mail relay server from transmitting the modified e-mail message.

24. The code of Claim 17, further operable to compartment information that is transmitted from the secure domain to the external domain.

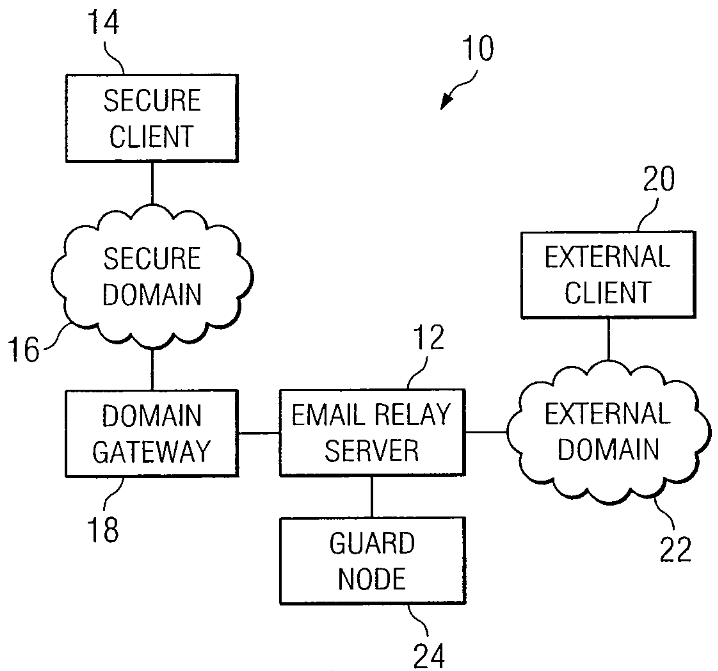
14
10
SECURE CLIENT
SECURE DOMAIN
16
20
EXTERNAL CLIENT
12
DOMAIN GATEWAY
EMAIL RELAY SERVER
EXTERNAL DOMAIN
18
GUARD NODE
22
24

FIG. 1

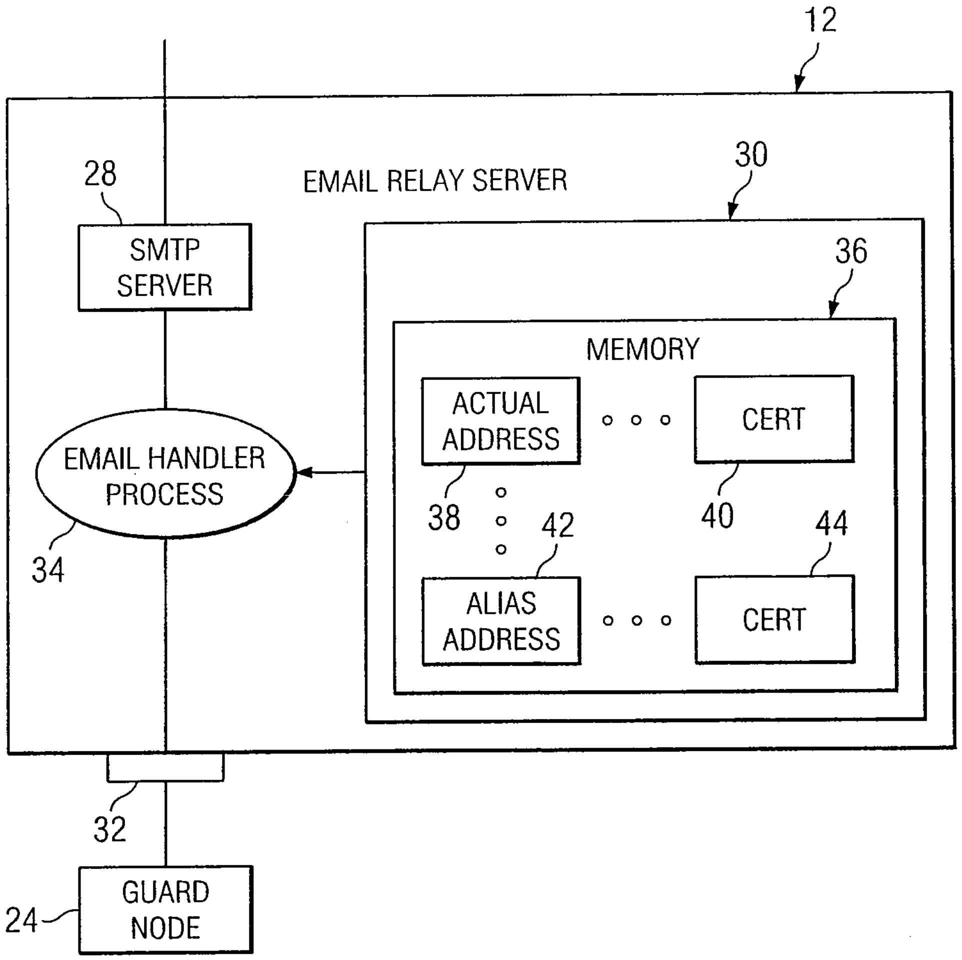
12
28
EMAIL RELAY SERVER
30
SMTP SERVER
36
MEMORY
ACTUAL ADDRESS
CERT
EMAIL HANDLER PROCESS
38
42
40
44
34
ALIAS ADDRESS
CERT
32
24
GUARD NODE

FIG. 2

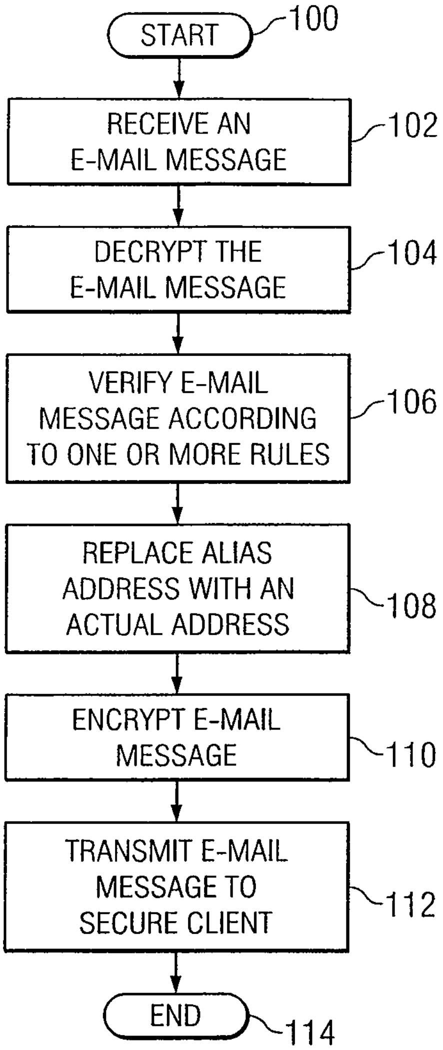
START
100
RECEIVE AN E-MAIL MESSAGE
102
DECRYPT THE E-MAIL MESSAGE
104
VERIFY E-MAIL MESSAGE ACCORDING TO ONE OR MORE RULES
106
REPLACE ALIAS ADDRESS WITH AN ACTUAL ADDRESS
108
ENCRYPT E-MAIL MESSAGE
110
TRANSMIT E-MAIL MESSAGE TO SECURE CLIENT
112
END
114

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/047588

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 328 351 B2 (YOKOTA TOMOFUMI [JP] ET AL) 5 February 2008 (2008-02-05)	1-7, 9-15, 17-23
Y	column 2, line 28 - line 43 column 3, line 29 - column 4, line 3 column 5, line 27 - line 56 column 5, line 57 - column 6, line 15 -----	8,16,24
Y	WO 2005/096543 A1 (COLLA GREGORY ALAN [AU]; JONES NEVILLE ROBERT [AU]) 13 October 2005 (2005-10-13) page 11, line 8 - line 22 -----	8,16,24
A	EP 1 635 524 A1 (ALADDIN KNOWLEDGE SYSTEMS LTD [IL]) 15 March 2006 (2006-03-15) paragraphs [0011] - [0015] -----	6-7, 14-15, 22-23

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 15 October 2009	Date of mailing of the international search report 23/10/2009
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Frey, Richard

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/047588

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
US 7328351	B2	05-02-2008	JP	3896886	B2	22-03-2007
			JP	2003298658	A	17-10-2003
			US	2003217261	A1	20-11-2003
WO 2005096543	A1	13-10-2005	US	2007288746	A1	13-12-2007
EP 1635524	A1	15-03-2006	US	2006075048	A1	06-04-2006