Title: SECURE MULTI-IDENTITY MANAGEMENT METHODS FOR A CENTRALIZED MESSAGING SERVICE

Abstract: User message management and routing methods applied to a standard facility of delivery protocols and managed according to the identity used by the user by means of: I - Identification of the identity producing the message; II - Application of suitable headings to the message according to: a - identity of the user; b - regulations defined by the user; III - Routing of the message to geo-located output points where the message is input again into the standard delivery net. The system is a complement of the already existing security systems for messaging services and adds also the protection of the privacy of the user to the protection of the contents by uncoupling the identity used.
Secure multi-identity management methods for a centralized messaging service

The present invention relates to net security problems, and particularly those concerning the privacy of the actors of a messaging system, and relies on already existing technologies with the aid of privacy and identity protection systems able to hide associations between identity and subscription from the recipients of messages.

Index of acronyms
DNS – Domain Name Server: net service attending to the resolutions of the textual domain addresses in their numerical counterparts; moreover, it provides details of mail servers associated to textual domains;
IMAP or IMAPS – Internet Message Access Protocol: net service for the users to gain access to a database containing electronic-mail messages associated to that particular user;
SMTP or SMTPS – Simple Mail Transfer Protocol: net protocol to address and transmit e-mail messages;
HTTP/HTTPS – Hyper Text Transfer Protocol (Secure): net protocol allowing data to be transferred from a service unit to an applicant. The secure release provides additionally the encryption of the transit data.

State of art
Electronic-mail systems are based upon concepts which are similar to the traditional mail systems as far as the routing aspect is concerned. A subject is identified by an univocal address which is specified by him/her as sender upon sending a message. Such address allows the geographic delivery area of any mail message addressed to him/her to be identified.
The mail service of the sender adds suitable notes (headings) to the message indicating the transit of the same through the mail office concerned.
Such headings indicate the geographic position of the area where the subject has gone to hand over the message to the mail service. A sender may have several addresses, but if the latter are managed by the same mail facility, they can be traced back to the same geographic area.

Such a management by the traditional e-mail service providers causes actual privacy problems. Thus it is possible for the recipient of a message to identify the geographic area of origin of the same as well as the geographic area where the sender handed over the message to the mail service.

At the present state of art it is then impossible for the sender to indicate an address having a different geographic location from the local mail service as this difference can be easily detected by the recipient.

By way of example, a subject sending a message from Paris to London can use Rome as sender address, however, the British recipient will realize that the message was not sent by the Italian Postal Service from Rome but the French Postal Service from Paris. This scenario is valid both for the traditional mail systems and for the electronic mail systems.

Besides the sender address that can arbitrarily be written by the sender and the information relative to the service provider who is charged for the message to be delivered, e-mail systems also include the right address of the computer (or computer net) compiling and sending the message in the headings, thus causing considerable privacy problems. Technical solutions to such problems have been experimented with a limited success. Some e-mail service providers cancel the information relative to the right address of the computer (or computer net) from which the messages are sent.

This operation is little useful and can be easily detected by the recipients of the e-mail messages. Under these circumstances it is possible for the recipient to detect not
only that the e-mail provider is still the same but also the geographic coordinates of origin and destination are still the same apart of the presumed nationality of an e-mail address.

Subjects operating in international circles often need to communicate with third parties by holding a different office in different organizations with which they cooperate in different countries. To do this, they should originate information flows relative to any organization from the country of origin both to prevent interceptions and to show to third parties to stay physically in a determined location.

There is then the need for using a single e-mail client to communicate by the access to a single point with a single e-mail account through multi-identities (e-mail) the information of which at the input and the output of the system flows exclusively on communication lines relative to the countries of origin of the specific identity used and provided with headings which certify the presence of the sender in the same country.

The invention aims at providing an e-mail platform able to carry out:
- a geographic distribution of the message flow input/output points;
- geographic message routing mechanism based upon the preferences of the sender or the service provider (and not the traditional routing method based upon the recipient address);
- an use of geo-located multi-identities through a single account;
- a management of the geo-located e-mail headings according to the preferences of the user or the service provider.

It is still an object of the present invention to provide an e-mail platform able to carry out a centralized multi-identity management both of the routing headings and the routing according to the sender of the message, thus allowing the operation with a flexible uncoupling of the sending identity from the identity of the sending user.

At last an object of the present invention is to provide a platform using known means and technology within technology and protocol of
Internet to operate with a net facility of easy maintenance and prompt feasibility.

These and other objects which will be more readily apparent from the following description are accomplished by a multi-identity management method for centralized messaging services according to the principles set forth in the appended claims.

The e-mail platform consists of several servers that manage the several aspects of the system. From the operation point of view the several logic units are able to exchange with one another data regarding the state of the message and to forward the message to the following logic unit by mailing or to the final destination by delivery.

The net system is integrated and cooperate with the already existing security systems. Actually, such units allow the message to appear as originated by the server unit operating at a primary stage of interaction with the user and processing SMTP or SMTPS outputs, and each domain can be arranged to be outputted from any unit so that the origin of the e-mail message is masked and the user is uncoupled from the impersonated identity.

Actually, the main advantage is certainly to add to the protection of the contents also the protection of the privacy of the user by de-coupling him/her from the sending identity.

In order to better clarify the invention and without limiting its scope and fields of application, some specific embodiments will be described herebelow with reference to the sole figure in which a general block diagram of the apparatus of the invention is shown.

**Description of some preferred embodiments.**

The electronic mail is a largely widespread, studied communication standard which is the object of many technical embodiments solving already the problems of the protection of the contents and then an object of the present invention is to implement the identity. Every mail server allows two possible routing modes: the first one is the
forced routing to a fixed destination of the message, the second one instead is the resolution of the destination of the message by direct request of DNS server responsible for the domain of belonging of the e-mail. In the following description the implementation of the first routing method is referred to as “forwarding”, and the implementation of the second routing method is referred to as “delivery”.

The implementation consists of several servers managing the several aspects of the system and operating to ensure the confidentiality of the sensible data of the users. In particular, three categories of servers managing the several communication aspects are identified:

- storage servers: machines where user’s messages are stored;
- backend servers: machines responsible for protecting the confidentiality of the messages and implementing the geographic routing to the geographical servers;
- geographical servers: relay machines responsible for delivering the mail to the recipients simulating the local production of the message.

Such systems are supported on the user’s side by messaging applications responsible for managing the encryption of the contents in the user’s machine to guarantee the confidentiality of the contents since before the reception of the contents by the system. Actually, the whole system is divided in logic units able to exchange data regarding the state of the message with one another and to forward the message to the following logic unit by forwarding or to the final destination by delivery.

I - The messages sent by the users through mail client are delivered to unit 1 (server operating at a primary stage of interaction with the user) which re-addresses the SMTP or SMTPS connections to the logic unit 3 and any IMAP or IMAPS connections to logic unit 2 and controls the authentication of the user as well as checks that the defined identity to send the message is accessible by that particular user. In case the message is sent through web interface, the user gains access through HTTPS protocol to logic unit 1 which re-addresses the
connection to logic unit 2 (service server for user’s processing) which is responsible for providing to client web the interface for sending e-mails and all of the activities of authentication and validation performed in the same way as unit 1. After these initial tests the message is forwarded to unit 3 (service server for SMTP or SMTPS output processing) by SMTP or SMTPS protocol. A lot of units 1 managing the access of the users can coexist to ensure a greater separation among users. Unit 3 forwards the message to unit 9 (output filter service server) to be further processed. As unit 9 returns the message to unit 3 the server provides for identifying the sender and reading from unit 6 (service server for administrative processing) the routing information relative to the sender and according to this information forwards the message to that logic unit 7 (server operating at a primary stage of interaction with other outside management and delivery services and processing SMTP outputs) indicated among the available units as output point of the sender. Unit 7 is responsible for cancelling the routing headings inside the message as well as delivering to final destination.

After having been processed as disclosed above and if envisaged by the user’s preferences or those of the service provider or the administrator of the group of users, output messages can be:

- handed over to an outside post system for the delivery to final destination;
- handed over to an inside mail box of transitory storage provided, if necessary, at the moment; in this case a notice containing the information to gain access to such message mail will be sent to final destination.

If an encryption is preferred, then the mail kept locally will be encrypted by a suitable method: sender and recipient may agree a password for each message or the recipient may select a password or a permanently valid cryptographic key which will be used for all future messages received by him/her.
These numerous units are the only elements of the actual facility seen by the outside mail systems upon sending the e-mail, each identity and each user being arranged to leave any such numerous units so that the origin of the message is masked and the user is uncoupled from the impersonated identity.

II – Messages directed to mail boxes managed by the present system are delivered from the servers of the sender systems to logic unit 8 (server operating at a primary stage of interaction with the system managing global e-mail and processing SMTP or SMTPS inputs). DNS server which is responsible for indicating to outside mail systems to address the e-mail to a particular unit 8 among those available according to the sites to which the domain is desired to belong is arranged for each domain managed by the system. These units are similar to units 7 and serve to keep the consistency among output and input points of the electronic mail and upon receiving the message forward it to unit 4 (input filter service server). Unit 4 controls that the input message has valid recipients inside the service and forwards the message to unit 10 (input filter service server). After the message is returned from unit 10 to unit 4 it is further forwarded to unit 5 (storage service server for IMAP or IMAPS access to e-mail) to be stored and made available for the users.

III – Users who want to gain access to their own mail system perform IMAP or IMAPS access through webmail or IMAP or IMAPS client by the connection to logic unit 1 which re-addresses the connections to logic unit 2 which gains access to logic unit 5 through IMAP or IMAPS proxy. According to this embodiment users cooperate with the identity to which they gain access as sub-files inside the files of their IMAP or IMAPS account which are combined hierarchically by domain.

Units 9, 10 include mail service filters responsible for managing on the base of user preferences the production of routing headings to be added to output mail messages according to the identity specified
upon sending and including information regarding the desired apparent origin of the message as well as information regarding the intermediate servers which processed the message. Input filter (unit 10) further provides advanced functions forming the core of the added value of the service and including among others:
- any encryption of the input message by a suitable cryptographic key belonging to the recipient,
- sending notice e-mail regarding the receipt of the e-mail,
- forwarding the message as annexed to another address based both on the sender and the recipient.

These functionality can be controlled by the users or the provider or an administrator of groups of users through a suitable available interface, for example, but not limited thereto, with HTTPS service from logic unit 1 allowing their interaction and the partial control of the operations performed by the filter. The interface allows the following settings:
- number of notices for each identity and their recipients,
- number of re-addressing for each identity and their recipients,
- advanced functionality of forwarding messages again which allows an identity to send the mail message to an address chosen by the user provided that the sender belongs to a defined address list,
- content protection functionality which prevents the user from sending e-mail the content of which is not encrypted,
- advanced functionality of content protection which encrypts automatically the not encrypted messages of the user by a local transitory deposit system if the cryptographic key of the recipient is not available.

With respect to the traditional mail system a complete privacy protection is accomplished as only the geo-located servers are connected to the message destinations and the routing information able to relate the real message delivery point to the virtual delivery point of said system is concealed.
Claims

1. A method of managing and routing user’s messages transmitted to a standard delivery protocol facility and managed on the base of the identity used by the user, characterized by the following steps:
   i – identifying the identity that generates a message,
   ii – establishing message headings based on:
      a – identity of the user, and/or
      b – regulations defined by the user,
   iii – routing the message to geo-located output points where the message is re-introduced into the standard delivery net.

2. The multi-identity management method for centralized messaging services according to claim 1, characterized by the following steps:
   i – delivering the messages sent by the users through mail client to a server (1) operating at a primary stage of interaction with the user who re-addresses SMTP or SMTPS connections to unit logic (3) and IMAP or IMAPS connections to logic unit (2), manages the authentication of the user and controls that the identity defined for sending the message is accessible by that particular user;
   ii – after the initial test, forwarding the message to service server (3) for processing SMTP or SMTPS outputs by SMTP or SMTPS protocol;
   iii – transmitting the message to be subjected to further processing from service server (3) processing SMTP or SMTPS outputs to service server (9) operating as output filter;
   iv – after server (9) transmits back the message to service server (3) for processing SMTP or SMTPS outputs, identifying the sender by means of server (3) which also reads from administrative processing service server (6) routing information relative to sender and on the base of this information forwards the message to server (7) operating
at a primary stage of interaction with the other outside management and delivery services;

v – processing SMTP outputs by server (7) operating at a primary stage of interaction with the other outside management and delivery services and being available as output point of the sender, and further cancelling inside routing headings of the message and the delivery to final destination.

3. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that in case the message is sent through web interface the user gains access through HTTPS protocol to service server (2) for user’s processing which is responsible for providing to client web the interface for sending e-mails and all of the activities of authentication and validation performed in the same way as unit (1) operating at the primary stage of interaction with the user.

4. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that it operates with a lot of servers (1) activated at the primary stage of interaction with the user and managing the access of the users to ensure an optimised separation among users.

5. The multi-identity management method for centralized messaging services according to any preceding claim, characterized by the following steps:

i – delivering the messages directed to mail boxes by the servers of the sender systems to server (8) operating at a primary stage of interaction with the system managing global e-mail and processing SMTP or SMTPS inputs, and arranging for each managed domain the DNS server which is responsible for indicating to outside mail systems to address the e-mail to a particular server (8) among those
available according to the sites to which the domain is desired to belong;
ii - keeping the consistency among output and input points of the electronic mail by server (8) and, upon receiving the message, forwarding it to server (4) acting as input filter controlling that the input message has valid recipients inside the service and then forwarding the message to service server (10) acting as input filter;
ili - after the message is returned from server (10) to server (4) acting as input filter, forwarding such message to service server (5) for the storage and the IMAP or IMAPS access to e-mail so that the message is stored and made available for the users.

6. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that users who want to gain access to their own mail system perform IMAP or IMAPS access through webmail or IMAP or IMAPS client by the connection to server (1) operating at a primary stage of interaction with the user which re-addresses the connections to user's processing service server (2) which in turn gains access to storage server (5) through IMAP or IMAPS proxy.

7. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that users cooperates with the identity to which they gain access as sub-files inside the files of their IMAP or IMAPS account which are combined hierarchically by domain.

8. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that service server (9) acting as output filter and service server (10) acting as input filter include mail service filters responsible for managing on the base of user's or provider's preferences the production of routing
headings to be added to output mail messages according to the identity specified upon sending and including information regarding the desired apparent origin of the message as well as information regarding the intermediate servers which processed the message.

9. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that server (10) acting as input filter performs the function of forwarding the message as annexed to another address based both on the sender and the recipient.

10. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that the setting of the number of notices for each identity and their recipients is performed.

11. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that there is provided the functionality of forwarding messages again which allows an identity to send the mail message to an address chosen by the user provided that the sender belongs to a defined address list.

12. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that there is provided a content protection functionality which prevents the user from sending e-mail the content of which is not encrypted.

13. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that there is provided an advanced functionality of content protection which encrypts automatically the not encrypted messages of the user by a local transitory deposit system if the cryptographic key of the
recipient is not available and sends a notice to the recipient.

14. A data communication facility for the multi-identity management of centralized messaging services according to any preceding claim, characterized by:
- server (1) operating at a primary stage of interaction with the user,
- service server (2) for the user's processing;
- service server (3) for SMTP or SMTPS output processing;
- service server (4) for SMTP or SMTPS input processing;
- server (5) for storing IMAP or IMAPS;
- service server (6) for administrative processing;
- server (7) operating at a primary stage of interaction with the user and processing SMTP or SMTPS outputs;
- server (8) operating at a primary stage of interaction with the user and processing SMTP or SMTPS inputs;
- service server (9) acting as output filter;
- service server (10) acting as input filter.

15. The multi-identity management method for centralized messaging services according to claim 13, characterized in that sender and recipient may agree a password for each message, and the thereby encrypted message is deposited in a transitory deposit system and a notice of a new message is sent to the recipient.

16. The multi-identity management method for centralized messaging services according to claim 15, wherein the recipient apart from the knowledge of the sender may select a cryptographic key or password with prolonged validity in time by which the messages in the transitory deposit are encrypted.

17. The multi-identity management method for centralized messaging services according to any preceding claim, wherein SMTPS protocol
is used instead of SMTP protocol.

18. The multi-identity management method for centralized messaging services according to any preceding claim, characterized in that IMAPS protocol is used instead of IMAP protocol.