US010541956B2

(12) **United States Patent**
Sachtjen

(10) **Patent No.: US 10,541,956 B2**
(45) **Date of Patent: *Jan. 21, 2020**

(54) **AUTHENTICATING AND CONFIDENCE MARKING E-MAIL MESSAGES**

(71) Applicant: **Iconix, Inc.**, San Jose, CA (US)

(72) Inventor: **Scott A. Sachtjen**, San Jose, CA (US)

(73) Assignee: **Iconix, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/132,251**

(22) Filed: **Sep. 14, 2018**

(65) **Prior Publication Data**

US 2019/0149499 A1 May 16, 2019

Related U.S. Application Data

(63) Continuation of application No. 12/024,980, filed on Feb. 1, 2008, now Pat. No. 10,110,530.

(60) Provisional application No. 60/899,064, filed on Feb. 2, 2007.

(51) **Int. Cl.**

H04L 12/58	(2006.01)
H04L 29/06	(2006.01)
H04L 9/12	(2006.01)
H04L 12/24	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 51/12*** (2013.01); ***H04L 9/12*** (2013.01); ***H04L 29/0651*** (2013.01); ***H04L 41/026*** (2013.01); ***H04L 51/00*** (2013.01); ***H04L 63/10*** (2013.01); ***H04L 63/126*** (2013.01)

(58) **Field of Classification Search**

CPC H04L 51/12; H04L 41/026; H04L 9/12; H04L 63/10; H04L 29/061; H04L 51/00; H04L 63/126

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,986,037	B1	1/2006	Assmann	
7,072,944	B2	7/2006	Lalonde	
7,313,700	B2 *	12/2007	Delany	H04L 29/12066 709/217
7,398,315	B2	7/2008	Atkinson	
7,461,339	B2	12/2008	Liao	
7,475,118	B2	1/2009	Leiba	
7,552,176	B2	6/2009	Atkinson	
7,634,543	B1	12/2009	Van Zant	
7,689,659	B1	3/2010	Granoff	
7,801,961	B2	9/2010	Sachtjen	
8,064,891	B2 *	11/2011	Fernandez-Alonso	H04L 63/0236 370/400

(Continued)

OTHER PUBLICATIONS

Aug. 5, 2019 Office Action, U.S. Appl. No. 13/231,795, 18 pages.

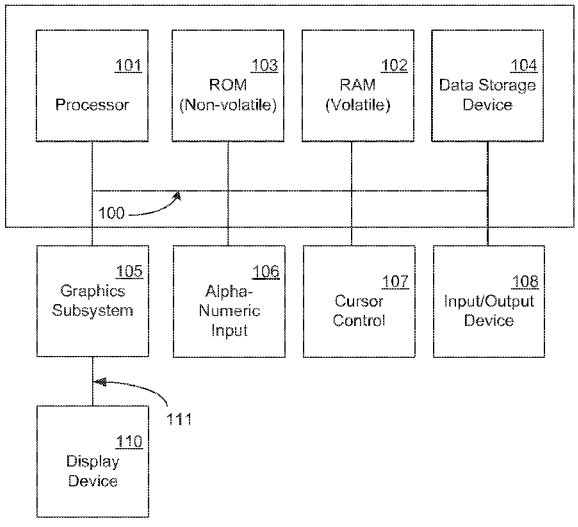
(Continued)

Primary Examiner — Saleh Najjar
Assistant Examiner — Feliciano S Mejia

(57) **ABSTRACT**

Methods and systems for authenticating and confidence marking e-mail messages are described. One embodiment describes a method of authenticating an e-mail message. This method involves extracting a plurality of e-mail headers associated with the e-mail message, and identifying a sending edge mail transfer agent (MTA). The method then calls for determining if the sending edge MTA is authorized to send the e-mail message.

24 Claims, 7 Drawing Sheets



(56) **References Cited**

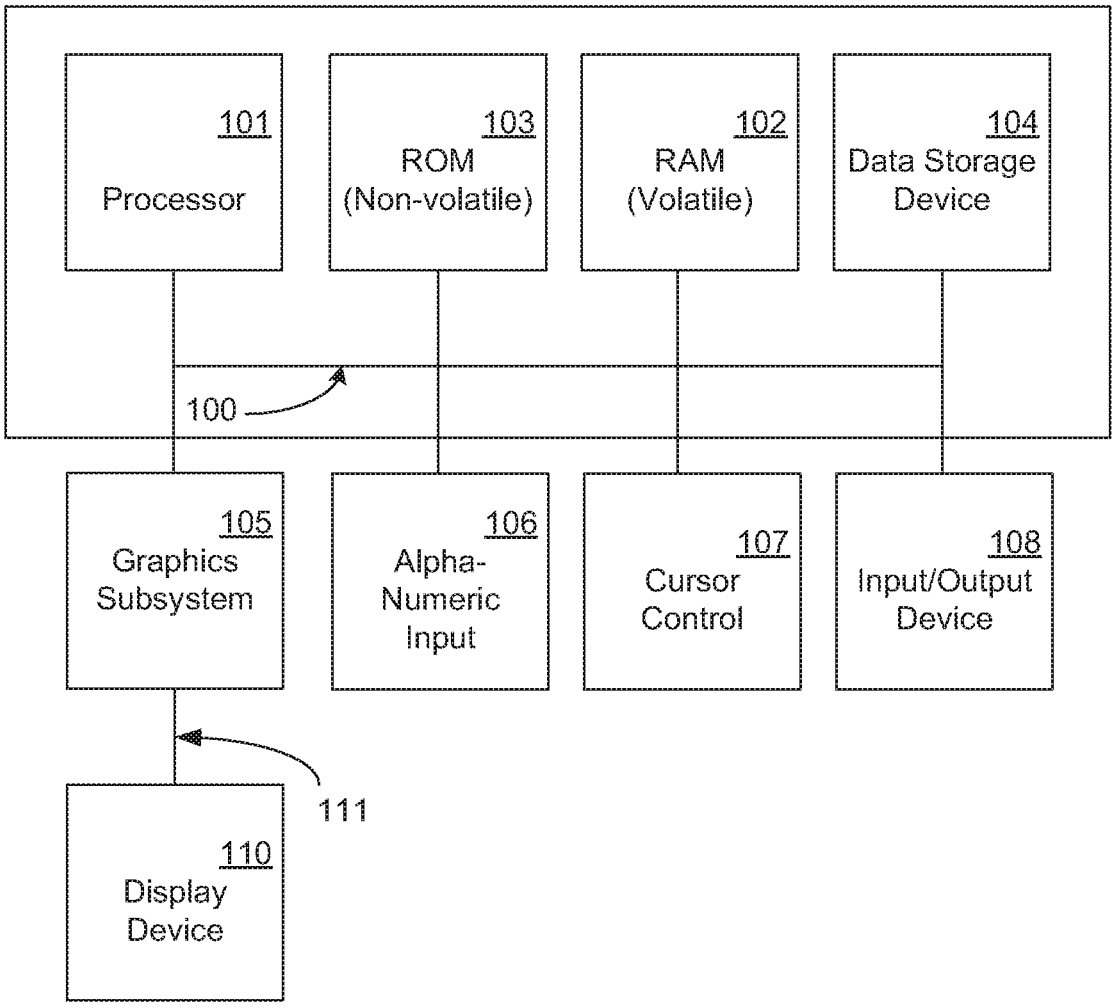
U.S. PATENT DOCUMENTS

8,090,940	B1	1/2012	Fenton	
8,156,654	B2 *	4/2012	Reed	B27B 17/02 30/371
8,200,979	B2 *	6/2012	Nadalin	G06F 21/6209 380/28
8,640,201	B2	1/2014	Kay	
8,984,640	B1 *	3/2015	Emigh	H04L 63/1441 726/25
10,110,530	B2	10/2018	Sachtjen	
10,277,397	B2	4/2019	Sachtjen	
2004/0260778	A1	12/2004	Banister	
2005/0081059	A1	4/2005	Bandini	
2006/0004896	A1	1/2006	Nelson	
2006/0168066	A1	1/2006	Helsper	
2006/0031319	A1	2/2006	Nelson	
2006/0085506	A1	4/2006	Meyers	
2006/0089970	A1	4/2006	Pearson	
2006/0224677	A1	10/2006	Ishikawa	
2006/0277597	A1	12/2006	Dreyman	
2007/0027992	A1	2/2007	Judge	
2007/0208941	A1	9/2007	Backer	
2008/0034212	A1	2/2008	Alfieri	
2008/0072294	A1	3/2008	Chatterjee	
2008/0141346	A1	6/2008	Kay	
2008/0320591	A1 *	12/2008	Fenton	H04L 51/12 726/22
2009/0094334	A1	4/2009	Eriksson	
2009/0094342	A1	4/2009	Lieba	
2014/0146727	A1	5/2014	Segev	

OTHER PUBLICATIONS

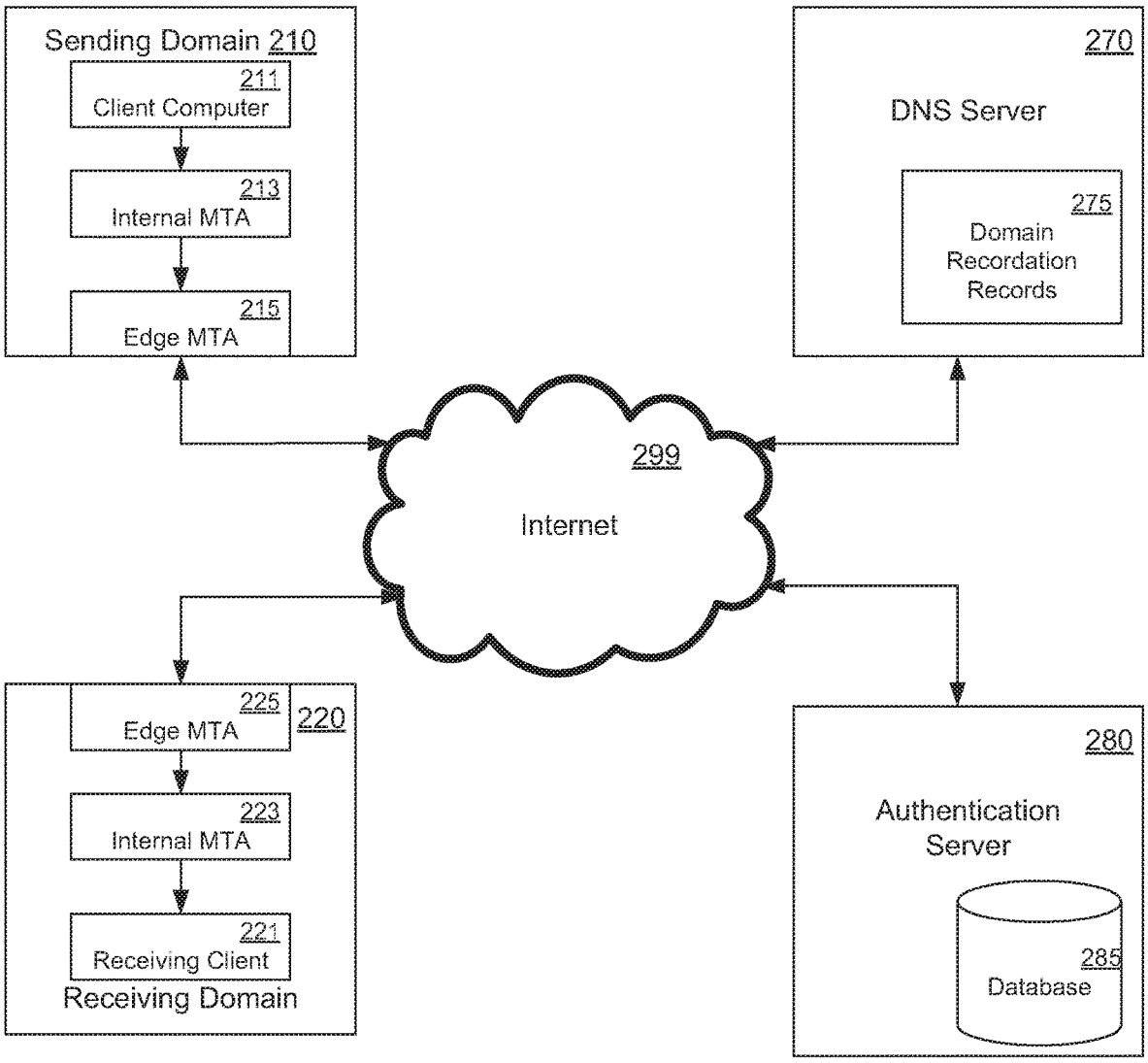
Dec. 6, 2018 BPAT decision, U.S. Appl. No. 14/977,505, 18 pages.
Jan. 12, 2018 Applicant Reply Brief, U.S. Appl. No. 14/977,505, 69 pages.
Nov. 14, 2017 Examiner Answer, U.S. Appl. No. 14/977,505, 33 pages.
Oct. 6, 2017 Applicant Appeal Brief, U.S. Appl. No. 14/977,505, 34 pages.
RFC 4406, "SenderID," Apr. 2006, 15 pages.
RFC 4407, "Purported Responsible Authority (PRA)," Apr. 2006, 6 pages.
RFC 4408, "Sender Policy Framework (SPF)," Apr. 2006, 38 pages.
RFC 4871, "Domain Keys Identified Mail (DKIM)," Apr. 2007, 71 pages.

* cited by examiner



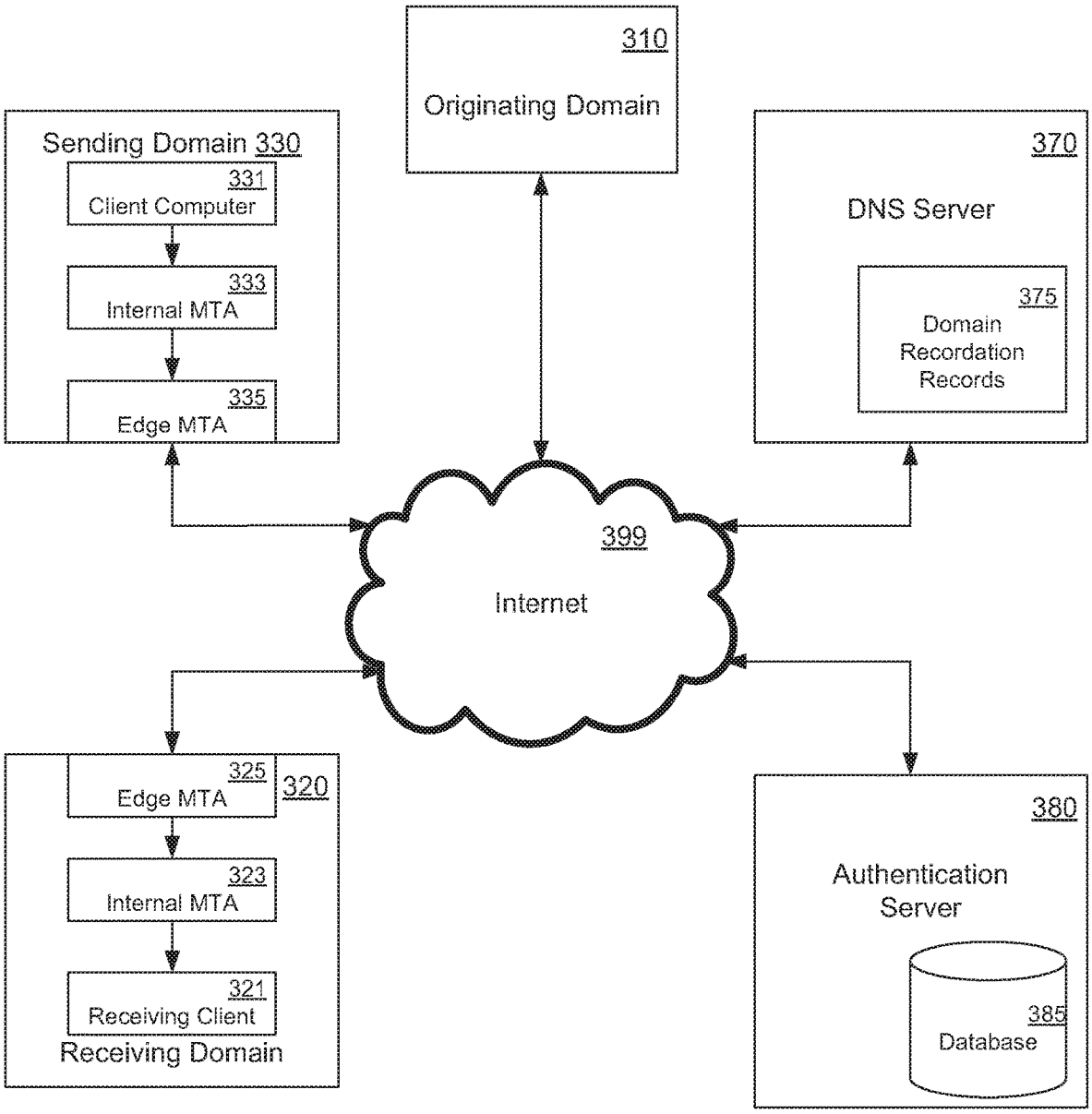
System 112

FIG. 1



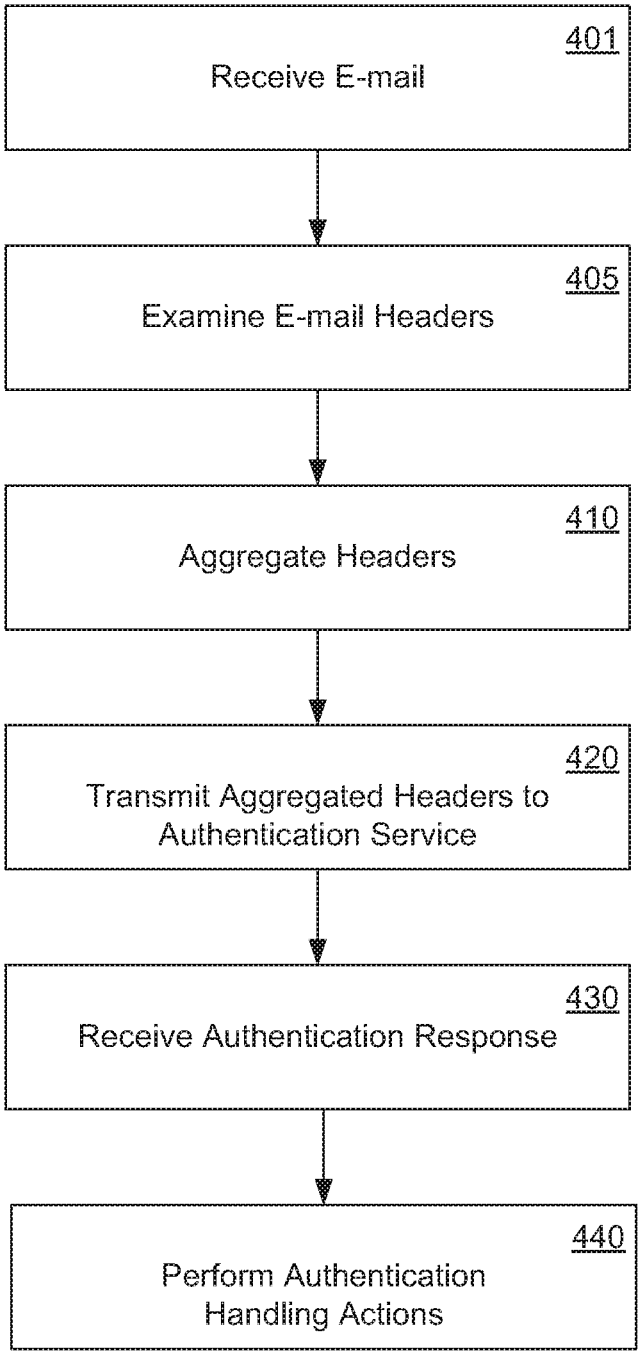
Network 200

FIG. 2



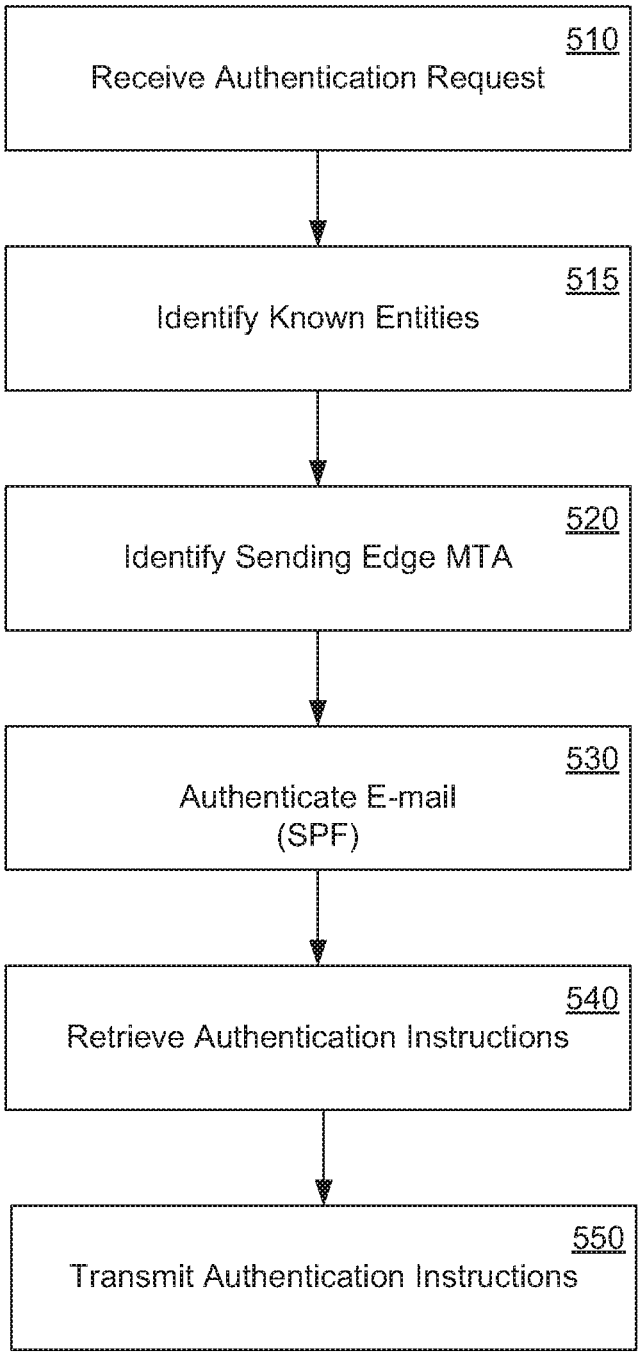
Network 300

FIG. 3



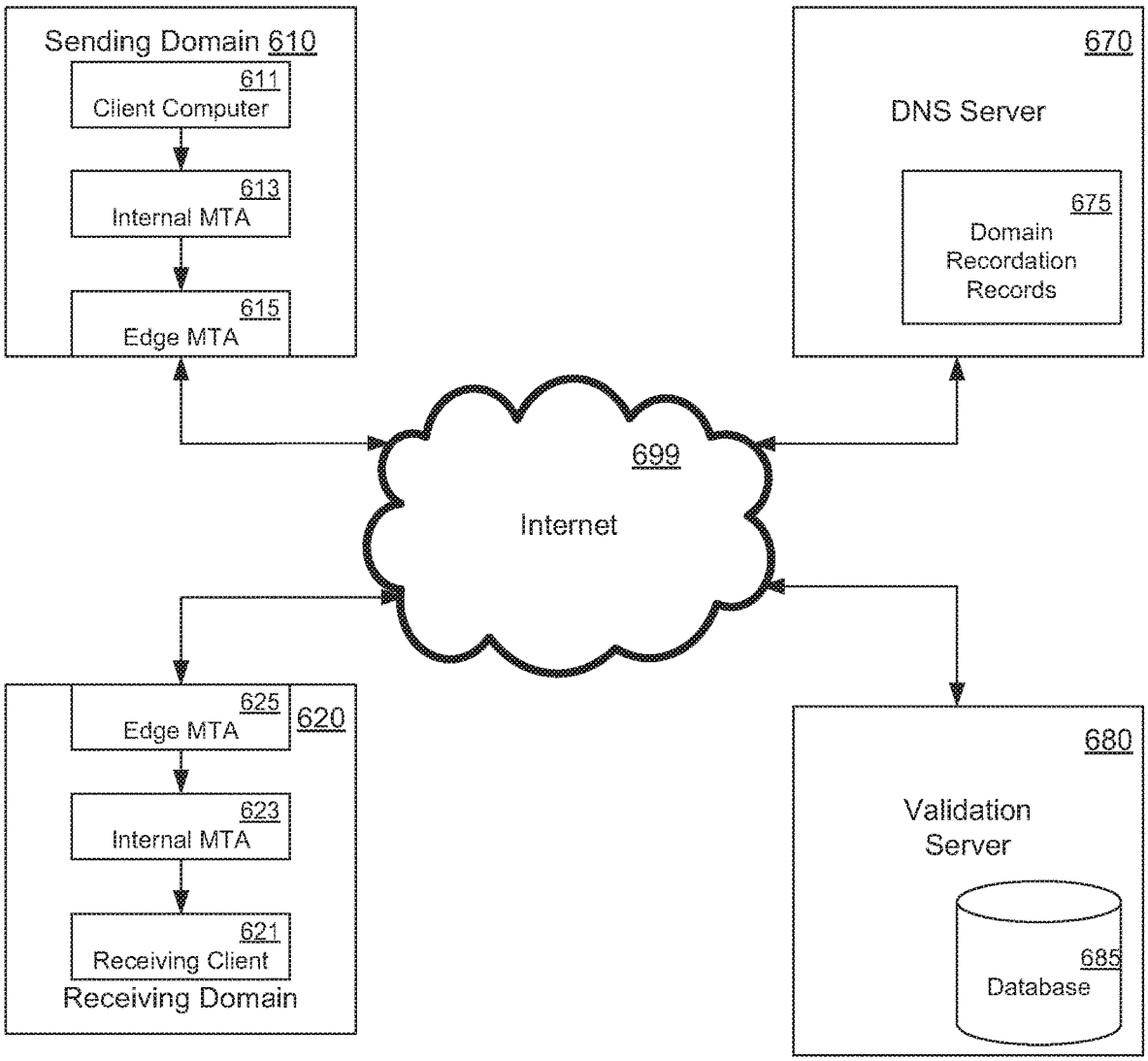
Flowchart 400

FIG. 4



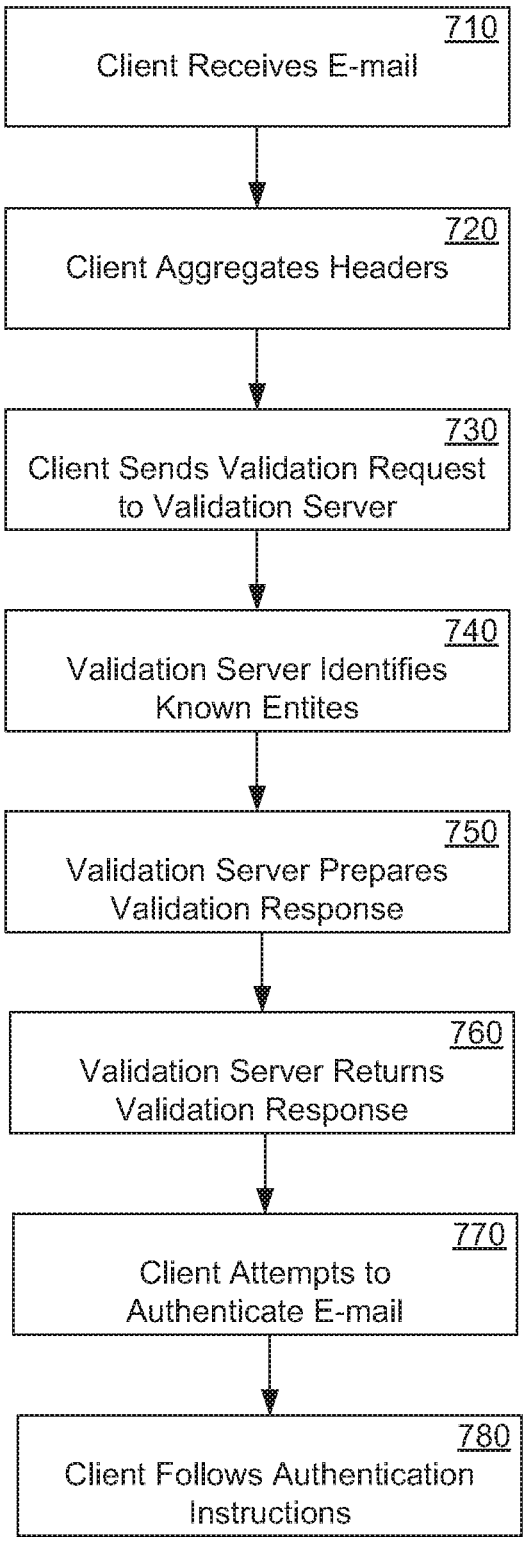
Flowchart 500

FIG. 5



Network 600

FIG. 6



Flowchart 700

FIG. 7

AUTHENTICATING AND CONFIDENCE MARKING E-MAIL MESSAGES

This application is a continuation of U.S. patent application Ser. No. 12/024,980, filed on Feb. 1, 2008 on behalf of first-named inventor Scott A. Sachtjen for "Authenticating And Confidence Marking E-Mail Messages" (issued on Oct. 23, 2018 as U.S. Pat. No. 10,110,530), which in turn claims the benefit of U.S. Provisional Application No. 60/899,064, filed on Feb. 2, 2007 on behalf of first-named inventor Scott A. Sachtjen for "A Method And System For Authentication And Confidence Marking Of Third-Party E-Mail Messages;" each of these prior applications is incorporated herein in its entirety.

BACKGROUND

Field of the Invention

Embodiments of the present invention relate to authenticating e-mail messages.

Related Art

One major concern in the field of electronic commerce is the need to identify and verify communications between parties. For example, when a customer is engaged in an e-commerce transaction with their bank, it is important to both the customer and the bank that the customer be able to identify and trust e-mail received from the bank. This concern is further complicated by third-party transactions, where a third party sends a message on behalf of someone else, such as where an online payment entity sends an e-mail to a customer on behalf of a seller.

A number of technologies, such as SPF (sender policy framework; RFC 4408) and Sender ID (RFC 4406), have been developed to help verify e-mail exchanged between servers or MTAs (mail transfer agents). Generally, these technologies are used to help ensure that the identifying information included in an e-mail's headers correlates with the sending MTA. However, these technologies do not address the problem of legitimate yet fraudulent senders; for example, an e-mail sent from YourOnlineBank.com (with the number "0") may comply with all of the necessary standards, but a user receiving that e-mail may easily confuse it for a legitimate e-mail from YourOnlineBank.com (with the letter "O").

The existing standards are set up to help prevent e-mail with forged header information from reaching the end user. However, the current standards do not protect the user from fraudulent e-mail with correct, but misleading, header information. Further, the current standards do not provide the user with any indicator of an e-mail which is authentic and trustworthy, as the current standards do not test for authenticity or trustworthiness.

SUMMARY

Methods and systems for authenticating and confidence marking e-mail messages are described. One embodiment describes a method of authenticating an e-mail message. This method involves extracting a plurality of e-mail headers associated with the e-mail message, and identifying a sending edge mail transfer agent (MTA). The method then calls for determining if the sending edge MTA is authorized to send the e-mail message.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention:

FIG. **1** is a block diagram of an exemplary computer system upon which embodiments of the present invention may be implemented.

FIG. **2** is a block diagram of an exemplary networking environment, according to one embodiment.

FIG. **3** is a block diagram of an exemplary networking environment, according to one embodiment.

FIG. **4** is a flowchart of a method of e-mail authentication, according to one embodiment.

FIG. **5** is a flowchart of a method of e-mail authentication, according one embodiment.

FIG. **6** is a block diagram of an exemplary networking environment, according to one embodiment.

FIG. **7** is a flowchart of a method of the new authentication, according to one embodiment.

DETAILED DESCRIPTION

Reference will now be made in detail to several embodiments of the invention. While the invention will be described in conjunction with the alternative embodiment (s), it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternative, modifications, and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims.

Furthermore, in the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the claimed subject matter. However, it will be recognized by one skilled in the art that embodiments may be practiced without these specific details or with equivalents thereof. In other instances, well-known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects and features of the subject matter.

Portions of the detailed description that follows are presented and discussed in terms of a method. Although steps and sequencing thereof are disclosed in figures herein (e.g., FIG. **3**) describing the operations of this method, such steps and sequencing are exemplary. Embodiments are well suited to performing various other steps or variations of the steps recited in the flowchart of the figure herein, and in a sequence other than that depicted and described herein.

Some portions of the detailed description are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer-executed step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout, discussions utilizing terms such as "accessing," "writing," "including," "storing," "transmitting," "traversing," "associating," "identifying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Computing devices typically include at least some form of computer readable media. Computer readable media can be any available media that can be accessed by a computing device. By way of example, and not limitation, computer readable medium may comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile discs (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computing device. Communication media typically embodies computer readable instructions, data structures, program modules, or other data in a modulated data signals such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared, and other wireless media. Combinations of any of the above should also be included within the scope of computer readable media.

Some embodiments may be described in the general context of computer-executable instructions, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments.

Although embodiments described herein may make reference to a CPU and a GPU as discrete components of a computer system, those skilled in the art will recognize that a CPU and a GPU can be integrated into a single device, and a CPU and GPU may share various resources such as instruction logic, buffers, functional units and so on; or separate resources may be provided for graphics and general-purpose operations. Accordingly, any or all of the circuits and/or functionality described herein as being associated with GPU could also be implemented in and performed by a suitably configured CPU.

Further, while embodiments described herein may make reference to a GPU, it is to be understood that the circuits and/or functionality described herein could also be implemented in other types of processors, such as general-purpose or other special-purpose coprocessors, or within a CPU.

Basic Computing System

Referring now to FIG. **1**, a block diagram of an exemplary computer system **112** is shown. It is appreciated that computer system **112** described herein illustrates an exemplary configuration of an operational platform upon which embodiments may be implemented to advantage. Nevertheless, other computer systems with differing configurations can also be used in place of computer system **112** within the scope of the present invention. That is, computer system **112** can include elements other than those described in conjunction with FIG. **1**. Moreover, embodiments may be practiced on any system which can be configured to enable it, not just computer systems like computer system **112**. It is understood that embodiments can be practiced on many different types of computer system **112**. System **112** can be implemented as, for example, a desktop computer system or server computer system having a powerful general-purpose CPU coupled to a dedicated graphics rendering GPU. In such an embodiment, components can be included that add peripheral buses, specialized audio/video components, IO devices, and the like. Similarly, system **112** can be implemented as a handheld device (e.g., cellphone, etc.) or a set-top video game console device such as, for example, the Xbox®, available from Microsoft Corporation of Redmond, Wash., or the PlayStation3®, available from Sony Computer Entertainment Corporation of Tokyo, Japan. System **112** can also be implemented as a "system on a chip", where the electronics (e.g., the components **101**, **103**, **105**, **106**, and the like) of a computing device are wholly contained within a single integrated circuit die. Examples include a hand-held instrument with a display, a car navigation system, a portable entertainment system, and the like.

Computer system **112** comprises an address/data bus **100** for communicating information, a central processor **101** coupled with bus **100** for processing information and instructions; a volatile memory unit **102** (e.g., random access memory [RAM], static RAM, dynamic RAM, etc.) coupled with bus **100** for storing information and instructions for central processor **101**; and a non-volatile memory unit **103** (e.g., read only memory [ROM], programmable ROM, flash memory, etc.) coupled with bus **100** for storing static information and instructions for processor **101**. Moreover, computer system **112** also comprises a data storage device **104** (e.g., hard disk drive) for storing information and instructions.

Computer system **112** also comprises an optional graphics subsystem **105**, an optional alphanumeric input device **106**, an optional cursor control or directing device **107**, and signal communication interface (input/output device) **108**. Optional alphanumeric input device **106** can communicate information and command selections to central processor **101**. Optional cursor control or directing device **107** is coupled to bus **100** for communicating user input information and command selections to central processor **101**. Signal communication interface (input/output device) **108**, which is also coupled to bus **100**, can be a serial port. Communication interface **108** may also include wireless communication mechanisms. Using communication interface **108**, computer system **112** can be communicatively coupled to other computer systems over a communication network such as the Internet or an intranet (e.g., a local area network), or can receive data (e.g., a digital television signal). Computer system **112** may also comprise graphics subsystem **105** for presenting information to the computer

user, e.g., by displaying information on an attached display device **110**, connected by a video cable **111**. In some embodiments, graphics subsystem **105** is incorporated into central processor **101**. In other embodiments, graphics subsystem **105** is a separate, discrete component. In other embodiments, graphics subsystem **105** is incorporated into another component. In other embodiments, graphics subsystem **105** is included in system **112** in other ways.

First- and Third-Party E-Mail Authentication

In the description that follows, several types of e-mail messages are discussed. First party e-mails are e-mails sent directly from one party to another; for example, in electronic commerce, an online bank may send electronic statements directly to its customers. Typically, the headers of the first party e-mail are in agreement. e.g., both the "From:" and "Sender:" header is reflect the same party.

By contrast, third-party e-mails are e-mails sent by one party on behalf of another party; for example, a bank customer may set up an electronic bill payment. When the funds are transferred to the intended recipient, the bank sends an e-mail to the recipient, on behalf of the customer, indicating the transaction. By its very nature, a third-party e-mail will often include competing or contradictory header information. The e-mail will typically be marked "From:" one party, e.g., the bank customer, while the "Sender:" indicator will reflect another party, e.g., the bank.

In the following embodiments, an approach is described for authenticating e-mail. In several of these embodiments, header information is extracted from a received e-mail message. This header information is transmitted to an authentication service, which attempts to determine whether the e-mail was sent by, and/or on behalf of, a trustworthy sender. If the service verifies the e-mail, the e-mail can be displayed to the user in a specified manner, such as with the inclusion of some confidence mark or icon, so that the user knows that the e-mail was sent by, or on behalf of, a trustworthy entity.

One of the advantages of such embodiments is that the recipient of the e-mail is presented with an indication of the trustworthiness of the e-mail in a manner in which they are accustomed. Rather than requiring the user to read and understand e-mail headers, most of which are commonly hidden from the user by default, the user can be presented with a visual indicator, such as an icon or company logo. This visual indicator can provide both confidence in the trustworthiness of the e-mail and an indication of the source of the e-mail, such as in the case where a company logo is displayed. In the following description, the term "confidence icon" is utilized to reference this idea of a visual indication of trustworthiness. However, it is understood that, in different embodiments, such a visual indicator can take many forms, including, but not limited to, icons, logos, other graphical indicators, or textual indicators.

Another advantage of the embodiments described herein is that certain senders may be "prequalified" or "vetted" by the authentication service. For example, an online payment facilitating company may often send third-party e-mails, e.g., payment receipts on behalf of a purchaser to a seller. If that online payment facilitating company is known to the authentication service, e.g., by inclusion in a database of trustworthy senders, their e-mail can be verified as trustworthy, which benefits both the payment facilitator and their clients.

Exemplary Networking Environments

With reference now to FIG. **2**, an exemplary networking environment **200** is depicted, in accordance with one embodiment. While network **200** is depicted as incorporating specific, enumerated features and elements, it is understood that embodiments are well suited to applications involving additional, fewer, or different features, elements, or arrangements.

Network **200**, as depicted in FIG. **2**, is representative of the transactions which may occur during transmission and authentication of a first party e-mail, in one embodiment. For example, a user within the sending domain **210** uses client computer **211** to send an e-mail. The e-mail may pass through one or more internal MTAs (mail transfer agents) **213** within the sending domain **210**, before it reaches edge MTA **215**. The e-mail leaves sending domain **210** at edge MTA **215**, and passes through Internet **299** before reaching receiving domain **220**. The e-mail enters receiving domain **220** via edge MTA **225**, and may pass through one or more internal MTAs **223**, before reaching receiving client **221**.

In some embodiments, once the e-mail is received, software on receiving client **221** attempts to authenticate the e-mail. Portions of the e-mail, e.g., selected portions of the e-mail headers, are passed to authentication service **280**, which includes authentication database **285**. In several such embodiments, authentication service **280** accesses DNS server **270** while attempting to authenticate the e-mail, and retrieves domain recordation records **275**. One such embodiment is explored in greater detail below.

With reference now to FIG. **3**, an exemplary networking environment **300** is depicted, in accordance with one embodiment. While network **300** is depicted as incorporating specific, enumerated features and elements, it is understood that embodiments are well suited to applications involving additional, fewer, or different features, elements, or arrangements.

Network **300**, as depicted in FIG. **3**, is representative of the transactions which may occur during transmission and authentication of a third-party e-mail, in one embodiment. For example, a user within originating domain **310** may engage in some e-commerce transaction with a user within receiving domain **320**. As a result of this transaction, a third-party sender within sending domain **330** may use client computer **331** to send an e-mail. The e-mail may pass through one or more internal MTAs **333** within the sending domain **330**, before it reaches edge MTA **335**. The e-mail leaves sending domain **330** at edge MTA **335**, and passes through Internet **399** before reaching receiving domain **320**. The e-mail enters receiving domain **320** via edge MTA **325**, and may pass through one or more internal MTAs **323** before reaching receiving client **321**.

In some embodiments, once the e-mail is received, software on receiving client **321** attempts to authenticate the e-mail. Portions of the e-mail, e.g., selected portions of the e-mail headers, are passed to authentication service **380**, which includes authentication database **385**. In several such embodiments, authentication service **380** accesses DNS server **370** while attempting to authenticate the e-mail, and retrieves domain recordation records **375**. One such embodiment is explored in greater detail below.

E-Mail Authentication: Client Behavior

In some embodiments, specialized software executing on the receiving client is utilized to perform e-mail authentication. In some embodiments, the software may modify or otherwise "plug in" to an existing e-mail client. In other embodiments, a specialized e-mail client may be utilized. In some embodiments, some or all portions of the e-mail client and/or client authentication software may reside and/or execute on a remote system. It is understood that embodiments of the invention are well suited to applications involving distributing some or all of the computational tasks

ascribed to either the client or the authentication server across local or network accessible computer systems. Further, is understood that embodiments of the invention are well suited to applications wherein some or all of the functionality ascribed to either the client or the authentication server may be consolidated.

With reference now to FIG. **4**, a flowchart **400** of a method of e-mail authentication is depicted, in accordance with one embodiment. Although specific steps are disclosed in flowchart **400**, such steps are exemplary. That is, embodiments of the present invention are well suited to performing various other (additional) steps or variations of the steps recited in flowchart **400**. It is appreciated that the steps in flowchart **400** may be performed in an order different than presented, and that not all of the steps in flowchart **400** may be performed.

With reference to step **401**, an e-mail is received. As is well known in the art, as e-mails are passed between MTAs, additional headers may be added. For example, each MTA may add a separate "Received:" to each e-mail that passes through the MTA. These "Received:" headers indicate each MTA involved in passing the message between the originator and the receiver. This header information is included in the received e-mail, although it may be hidden from the user.

For example, with reference to FIG. **3**, receiving client **321** receives an e-mail from a third-party sender using client computer **331**. Each MTA between client computer **331** and receiving client **321** adds an additional "Received:" header to the e-mail, including internal MTA **331**, edge MTA **335**, edge MTA **325**, and internal MTA **323**.

With reference now to step **405**, in some embodiments, a portion of the e-mail headers are examined. In such an embodiment, the e-mail client may attempt to determine if the originator of the e-mail appears on the list of known senders, e.g., by examining the "Sender:" or "Reply-to:" headers. This approach allows the e-mail client to selectively screen e-mail before attempting authentication, e.g., by restricting authentication to c-mails which appear to be from entities which are of particular interest, such as banks or online payment facilitators, and excluding other e-mails. For example, the client will attempt to authenticate emails from "YourOnlineBank.com", while excluding those from "Your0nlineBank.com". This approach may also allow the e-mail client to selectively exclude e-mail from attempted authentication, e.g., by allowing a user to prevent authentication attempts on e-mail where trustworthiness is less of a concern, such as e-mail from a family member. In some embodiments, this step is omitted.

For example, the e-mail program for receiving client **321** may examine the headers in the e-mail from the third-party sender. If, for example, sending domain **330** appears in a list of senders to authenticate, the e-mail program will attempt to authenticate the e-mail.

With reference now to step **410**, information contained in the e-mail headers is aggregated. In different embodiments, different headers are used by the authentication service. In this step, those headers that are of interest can be extracted from the e-mail, and prepared for transmission to the authentication service. Further, in some embodiments, redundant or duplicative headers can be excluded during this aggregation process.

For example, the e-mail client for receiving client **321** may extract the "Received:" headers, the "From:" header, and the "Sender:" header from the e-mail received from the third-party sender. These headers are encapsulated and prepared for transmission to authentication service **380**.

With reference now to step **420**, the aggregated e-mail headers are transmitted to the authentication server.

For example, the e-mail program transmits the aggregated headers from receiving client **321** to authentication server **380**.

With reference now to step **430**, an authentication response is received from the authentication service. In different embodiments, different actions may be specified by the authentication service. For example, the authentication response may include instructions for the e-mail program to retrieve a confidence icon relating to the sender of the e-mail, e.g., from a specified Internet location, and display it as part of the "From:" field for that e-mail. Alternatively, the e-mail program may be instructed to display a confidence icon indicating that the e-mail has been authenticated by the authentication service. If the authentication service was unable to authenticate the e-mail, the e-mail program may be instructed to display a different icon, or no icon at all. Additionally, the authentication response may include additional information, such as display directives, display signs, instructions regarding the location of additional information about the sender, instructions regarding the location of additional information about a third-party, authentication failure conditions, or authentication status.

For example, authentication server **380** instructs the e-mail program for receiving client **321** to retrieve a confidence icon, e.g., the company logo, corresponding to the identity of the third-party sender. This confidence icon is to be displayed in the "From:" field, when the e-mail is being viewed by a user.

With reference now to step **440**, the receiving client performs the actions specified by the authentication service. In different embodiments, different actions may be performed. For example, if the authentication response indicates that a confidence icon is to be retrieved and displayed, the receiving client would retrieve the icon, e.g., from a local cache of icons, or from a specified network location, and display it as instructed by the authentication response.

For example, the e-mail program for receiving client **321** obtains the confidence icon (company logo) corresponding to the identity of the third-party sender from a location specified by authentication server **380**, and displays the confidence icon as instructed.

E-Mail Authentication: Authentication Service

In some embodiments, an authentication service is utilized to provide authentication for e-mail. The components and configuration of such an authentication service may vary, across different embodiments. In some embodiments, the authentication service is configured to receive authentication requests from client software, attempt to authenticate the e-mail messages described in his authentication requests, and transmit authentication responses to client software.

With reference now to FIG. **5**, a flowchart **500** of a method of e-mail authentication is depicted, in accordance with one embodiment. Although specific steps are disclosed in flowchart **500**, such steps are exemplary. That is, embodiments of the present invention are well suited to performing various other (additional) steps or variations of the steps recited in flowchart **500**. It is appreciated that the steps in flowchart **500** may be performed in an order different than presented, and that not all of the steps in flowchart **500** may be performed.

With reference now to step **510**, an authentication request is received. In some embodiments, as previously described, client software executing on a client computer may prepare an authentication request. These requests may include one or more e-mails to be authenticated, and may include some

portion of the headers corresponding to these e-mail messages. In different embodiments, different formats and protocols may be utilized for transmitting and receiving these authentication requests.

For example, authentication server **380** receives an authentication request from receiving client **321**, regarding an e-mail sent by client computer **301** within sending domain **330**. The authentication request includes the "Received:" headers from the e-mail, as well as the "From:" and "Sender:" headers.

With reference now to step **515**, the authentication server determines if a known entity is involved. For example, in some embodiments, the authentication server maintains a list or database of known, trustworthy entities. If these entities are purportedly involved in an authentication request, e.g., a known entity appears in the "Sender." or the "From:" headers, the authentication server will attempt to authenticate the e-mail. In some embodiments, the authentication server attempt to match a specific user, e.g., "knownuser@trustworthy.com". In other embodiments, the authentication server attempts to match the domains involved, e.g., "trustworthy.com". In some embodiments, the authentication server attempts to match first a specific user, and attempt to match the domains if no specific user match is found. Moreover, in some embodiments, the authentication server may not perform authentication if no match is found.

For example, authentication server **380** attempts to match the "From:" and "Sender:" headers from the authentication request to a list of known entities maintained in database **385**. If either originating domain **310** or sending domain **330** (or both) appears in database **385**, authentication server **380** attempt to authenticate the e-mail.

With reference now to step **520**, the sender's edge MTA is identified. As previously discussed, each MTA that an e-mail passes through adds an additional "Received:" header to the e-mail. By examining these headers, the edge transactions can be identified, e.g., those transactions where the e-mail was passed from an MTA for one domain to an MTA for a second domain. Identifying these edge transitions allows the authentication service to determine whether the sending edge MTAs are permitted to send e-mail on behalf of a trustworthy entity.

For example, authentication server **380** examines the headers included in the authentication request, in order to identify the sender's edge MTA. Here, authentication server **380** identifies edge MTA **335**.

With reference now to step **530**, the authentication service attempts to authenticate the e-mail. In some embodiments, the authentication server performs an SPF (sender policy framework) check to attempt to authenticate the e-mail. The DNS records corresponding to the involved domains are retrieved, and compared to the edge MTA previously identified. In the case of first party e-mail, if the edge MTA is identified as being allowed to send e-mail on behalf of the entity identified by the e-mail headers, e.g., in the "Sender:" or "From:" headers, the e-mail is authenticated. In the case of third-party e-mail, if the edge MTA is identified as being allowed to send e-mail on behalf of either entity identified in the "Sender:" or "From:" headers, the e-mail is authenticated. If, however, the edge MTA is not identified in the corresponding DNS records as permitted to send e-mail on behalf of a trustworthy entity, the authentication attempt may fail.

It is understood that in other environments, other authentication techniques may be utilized. For example, a "Sender ID" check may be performed; similarly, domainkeys identified mail may be authenticated in a manner similar to that described herein.

For example, authentication server **380** retrieves DNS records **375** from DNS server **370** corresponding to both originating domain **310** and sending domain **330**. If DNS records **375** indicate that edge MTA **335** is permitted to send e-mail on behalf of originating domain **310** or sending domain **330**, the e-mail is authenticated.

With reference now to step **540**, the authentication service retrieves authentication instructions. In different embodiments, different authentication results may result in different authentication instructions. For example, if an e-mail is identified as coming from a trustworthy sender, different authentication instructions may be used and if the e-mail is identified as being on behalf of a trustworthy third party. Further, different trustworthy entities may have different desired authentication instructions, e.g., in terms of which confidence icons to utilize, where to retrieve confidence icons, how to display them, or the like. Similarly, if authentication is unsuccessful, different authentication instructions may be sent to the client.

For example, authentication server **380** retrieves authentication instructions corresponding to sending domain **330** from database **385**.

With reference to step **550**, the authentication server transmits authentication instructions in response to the authentication request. The retrieved authentication instructions are transmitted to the requesting client, instructing the client on how to proceed. As noted previously, formats and protocols utilized in receiving and transmitting authentication instructions may vary, across different embodiment.

For example, authentication server **380** transmits authentication instructions to receiving client **321**, regarding how to handle the e-mail received from client computer **331**.

Remote Validation and Client-Based Authentication

As discussed previously, in different embodiments, in different portions of the authentication functionality may be performed by different computing entities. In one embodiment, for example, a remote validation server is used for identifying known entities and forwarding validation responses, while the receiving client is used to perform the actual authentication of an e-mail message.

With reference now to FIG. **6**, an exemplary networking environment **600** is depicted, in accordance with one embodiment. While network **600** is depicted as incorporating specific, enumerated features and elements, it is understood that embodiments are well suited to applications involving additional, fewer, or different features, elements, or arrangements.

Network **600**, as depicted in FIG. **6**, is representative of the transactions which may occur during transmission and authentication of a first party e-mail, in one embodiment. For example, a user within the sending domain **610** uses client computer **611** to send an e-mail. The e-mail may pass through one or more internal MTAs (mail transfer agents) **613** within the sending domain **610**, before it reaches edge MTA **615**. The e-mail leaves sending domain **610** at edge MTA **615**, and passes through Internet **699** before reaching receiving domain **620**. The e-mail enters receiving domain **620** via edge MTA **625**, and may pass through one or more internal MTAs **623**, before reaching receiving client **621**.

In this embodiment, once the e-mail is received, software on receiving client **621** attempts to authenticate the e-mail. Portions of the e-mail, e.g., selected portions of the e-mail headers, are passed to validation service **680**, which includes validation database **685**. Validation service **680** returns vali-

dation responses to receiving client **621**. Receiving client **621** then attempts to authenticate the e-mail message, e.g., by accessing DNS server **670** and retrieving domain recordation records **675**. Depending upon the success of the authentication attempt, receiving client **621** may perform portions of the authentication instructions provided by validation service **680**.

With reference now to FIG. **7**, a flowchart **700** of a method of authenticating an e-mail message is depicted, in accordance with one embodiment. Although specific steps are disclosed in flowchart **700**, such steps are exemplary. That is, embodiments of the present invention are well suited to performing various other (additional) steps or variations of the steps recited in flowchart **700**. It is appreciated that the steps in flowchart **700** may be performed in an order different than presented, and that not all of the steps in flowchart **700** may be performed.

With reference now to step **710**, a client receives an e-mail message. In different embodiments, different client software may be utilized on the receiving computer to handle e-mail authentication. In some embodiments, for example, e-mail authentication may be performed by a "helper" application, which coordinates with a separate e-mail program. In other embodiments, e-mail authentication may be included as part of an e-mail program.

For example, with reference to FIG. **6**, receiving client **621** receives an e-mail from client computer **611**.

With reference now to step **720**, the client aggregates headers from the e-mail message. In some embodiments, the client may extract several different headers from an e-mail message, such as the "From:" or "Sender:" headers. Moreover, in some embodiments, the client may process multiple e-mail messages simultaneously. During this step, the client may take action to reduce redundancy or repetition of headers.

Continuing the preceding example, receiving client **621** extracts the "From:" and "Sender:" headers from the e-mail message received from client computer **611**.

With reference now to step **730**, the client transmits a validation request to a validation server. In this embodiment, the validation server provides remote validation of known entities, as well as providing authentication instructions for successful or failed tense to authenticate the e-mail, but does not attempt to authenticate the e-mail. As such, the validation request will include the aggregated headers produced during step **720**, but is unlikely to include the "Received:" headers, as validation server does not intend to identify the sender's edge MTA.

Continuing the preceding example, receiving client **621** transmits a validation request to validation server **680**, including the headers extracted from the e-mail message received from client computer **611**.

With reference now to step **740**, the validation server identifies known entities from the headers included in the validation request. In some embodiments, the validation server includes an authentication or validation database, which contains entries describing known, trustworthy entities. The validation server attempts to match the headers included in validation request with these known entities.

With reference now to step **750**, the validation server prepares a validation response. In some embodiments, the validation response includes information regarding each entity described in the validation request, e.g., for each different entity identified in the headers included in the validation request, whether that entity is known, and how to handle authentication of the e-mail message. In some embodiment, the validation server can retrieve handling instructions corresponding to various known entities from the authentication database; alternatively, the validation server may generate such handling instructions. As discussed previously, these handling instructions may vary across different embodiments, but may include information such as the location and display instructions for confidence icons corresponding to identify known entities, or instructions on what the client to display if authentication is unsuccessful.

With reference now to step **760**, the validation server transmits a validation response, in response to the validation request. The validation server returns the validation results to the requesting client, as well as appropriate handling instructions. As discussed previously, the formats and protocols utilized in transmissions between the requesting client and the validation or authentication server may vary, across different embodiments.

Continuing the preceding example, validation server **680** attempts to identify known entities from the validation request provided by receiving client **621**. Validation server **680** accesses validation database **685**, and attempts to match users and/or domains identified in the headers included in the validation request with a list of known entities included database **605**. Validation server **680** also prepares a validation response for receiving client **621**, including the location of and display instructions for a confidence icons corresponding to sending domain **610**.

With reference now to step **770**, the client attempts to authenticate the e-mail message. In different embodiments, different approaches may be utilized for authentication. In one embodiment, for example, the client identifies the sender's edge MTA from the "Received:" headers included in the e-mail message. The client then performs a sender policy framework (SPF) check, to determine if that MTA is permitted to send e-mail for, or on behalf of, one of the known entities identified by the validation server.

With reference now to step **780**, the client follows the handling instructions provided by the validation server. In some embodiments, the handling instructions transmitted by the validation server instruct the client on what actions to perform if authentication is successful, as well as any special actions to take if authentication is unsuccessful. In one embodiment, if authentication succeeds, the client is instructed to display a confidence icon in a manner so as to indicate to a user that this e-mail message has been authenticated, e.g., the client may retrieve a confidence icon associated with a trusted entity, and display it within the "From:" field of the displayed e-mail.

Continuing the preceding example, receiving client **621** attempts to validate the message received from client computer **611**. The "Received:" headers included in the e-mail message are parsed, and edge MTA **615** is identified. Receiving client **621** then performs an SPF check, by accessing DNS server **670** and domain recordation records **675** to determine if edge MTA **615** is authorized to send e-mail on behalf of sending domain **610**. If edge MTA **615** is authorized, the e-mail message is successfully authenticated. Receiving client **621** may then retrieve a confidence icon corresponding to sending domain **610**, e.g., a company logo from a specified location accessible through Internet **699**, and display that confidence icon when the e-mail message is viewed by a user.

Embodiments of the present invention are thus described. While the present invention has been described in particular embodiments, it should be appreciated that the present

invention should not be construed as limited by such embodiments, but rather construed according to the following claims.

What is claimed is:

1. A computer-implemented method of authenticating an e-mail message, wherein the e-mail message is sent by a first entity in a manner purporting to be on behalf of a second entity, and wherein the second entity is a legal entity not inherently associated with the first entity, the computer-implemented method comprising:

extracting a plurality of e-mail headers from said e-mail message;

from the extracted plurality of e-mail headers, identifying a sending edge mail transfer agent (MTA) associated with the first entity;

from said e-mail message, identifying the second entity and a domain associated with the second entity;

retrieving via a wide area network (WAN) a record in association with the domain of the second entity, and processing the record to determine whether the identified sending edge MTA associated with the first entity is explicitly identified by the record as authorized to send said e-mail messages on behalf of the second entity; and

responsively authenticating said e-mail message.

2. The computer-implemented method of claim 1, wherein the domain is a second domain, and wherein identifying the second entity comprises identifying a first domain independent from the first entity from the extracted plurality of e-mail headers, identifying the second entity from the first domain, wherein the first domain is not authorized by the second entity, and identifying the second domain as a domain authorized by the second entity.

3. The computer-implemented method of claim 2, wherein the record comprises a sender policy framework (SPF) record, wherein the SPF record is associated with the second domain, and wherein processing the SPF record comprises determining whether the SPF record for the second domain explicitly identifies the identified sending edge MTA associated with the first entity.

4. The computer-implemented method of claim 1, wherein:

identifying the second entity and the domain associated with the second entity comprises,

from the extracted plurality of e-mail headers, identifying one or more domains of prior senders which are not inherently associated with the first entity,

transmitting a request via a WAN to a validation service, wherein the validation service is to compare the one or more domains with a list of known, trustworthy entities having names similar to the one or more domains, and

receiving a response from the validation service which provides information to identify a SPF record corresponding to one of the known, trustworthy entities;

retrieving the record comprises retrieving the SPF record corresponding to the one of the known, trustworthy entities; and

the processing comprises processing the SPF record so as to determine whether the identified sending edge MTA is explicitly identified by the one of the known, trustworthy entities as authorized to send said e-mail messages on behalf of the one of the known, trustworthy entities.

5. The computer-implemented method of claim 4, wherein extracting the plurality of e-mail headers comprises extracting each "Sender:" and "Reply-To:" header present in said e-mail message, such that the one or more domains comprises at least one domain derived from a "Sender:" or "Reply-To:" header which was present in said e-mail message.

6. The computer-implemented method of claim 4, wherein said computer-implemented method further comprises receiving instructions from the validation service which are specific to the one of the known, trustworthy entities, and causing delivery of the e-mail message, responsive to the authenticating, in a manner will cause presentation to a recipient of the e-mail message of verification information where the presentation is customized to the one of the known, trustworthy entities.

7. The computer-implemented method of claim 6, wherein the verification information comprises a visual indication specified by the one of the known, trustworthy entities.

8. The computer-implemented method of claim 6, wherein the verification information comprises a confidence icon specified by the one of the known, trustworthy entities.

9. The computer-implemented method of claim 4, wherein the validation service is to compare the one or more domains with the list of known, trustworthy entities to identify a condition where the one or more domains represent a fraudulent sender having a name similar to one of the known, trustworthy entities in the list, and wherein the response from the validation service is to identify the one of the known, trustworthy entities, such that a SPF record of the at least one SPF record corresponds to the one of the known, trustworthy entities in the list and not the fraudulent sender.

10. The computer-implemented method of claim 1, wherein identifying the sending edge mail transfer agent (MTA) associated with the first entity comprises extracting a "From:" header of the e-mail message, and deriving the identified sending edge MTA from the extracted "From:" header.

11. The computer-implemented method of claim 1, wherein said computer-implemented method further comprises responsive to the authenticating, causing the e-mail message to be delivered to a recipient in a manner where the e-message will be displayed in a manner that explicitly conveys that the e-mail message has been verified to have been sent on behalf of the second entity.

12. An apparatus for authenticating an e-mail message, wherein the e-mail message is sent by a first entity in a manner purporting to be on behalf of a second entity, and wherein the second entity is a legal entity not inherently associated with the first entity, said apparatus comprising instructions stored on non-transitory, machine-readable media, said instructions when executed to cause at least one computer to:

extract a plurality of e-mail headers from said e-mail message;

from the extracted plurality of e-mail headers, identify a sending edge mail transfer agent (MTA) associated with the first entity;

from said e-mail message, identify the second entity and a domain associated with the second entity;

retrieve via a wide area network (WAN) a record in association with the domain of the second entity, and process the record to determine whether the identified sending edge MTA associated with the first entity is explicitly identified by the record as authorized to send said e-mail messages on behalf of the second entity; and

responsively authenticate said e-mail message.

13. The apparatus of claim 12, wherein the domain is a second domain, and wherein said instructions when executed are to cause the at least one computer to identify a first domain independent from the first entity from the extracted plurality of e-mail headers, to identify the second entity from the first domain, wherein the first domain is not authorized by the second entity, and to identify the second domain as a domain authorized by the second entity.

14. The apparatus of claim 13, wherein the record comprises a sender policy framework (SPF) record, wherein the SPF record is associated with the second domain, and wherein said instructions when executed are to cause the at least one computer to determine whether the SPF record for the second domain explicitly identifies the identified sending edge MTA associated with the first entity.

15. The apparatus of claim 12, wherein said instructions when executed are to cause the at least one computer to:

from the extracted plurality of e-mail headers, identify one or more domains of prior senders which are not inherently associated with the first entity;

transmit a request via a WAN to a validation service, wherein the validation service is to compare the one or more domains with a list of known trustworthy entities having names similar to the one or more domains;

receive a response from the validation service which provides information to identify a SPF record corresponding to one of the known, trustworthy entities;

retrieve the SPF record; and

process the SPF record so as to determine whether the identified sending edge MTA is explicitly identified by the one of the known, trustworthy entities as authorized to send said e-mail messages on behalf of the one of the known, trustworthy entities.

16. The apparatus of claim 15, wherein said instructions when executed are to cause the at least one computer to extract each "Sender:" and "Reply-To:" header present in said e-mail message, such that the one or more domains comprises at least one domain derived from a "Sender:" or "Reply-To:" header which was present in said e-mail message.

17. The apparatus of claim 15, wherein said instructions when executed are to cause the at least one computer to receive instructions from the validation service which are specific to the one of the known, trustworthy entities, and to cause delivery of the e-mail message, responsive to the authenticating, in a manner will cause presentation to a recipient of the e-mail message of verification information where the presentation is customized to the one of the known, trustworthy entities.

18. The apparatus of claim 17, wherein the verification information comprises a visual indication specified by the one of the known, trustworthy entities.

19. The apparatus of claim 17, wherein the verification information comprises a confidence icon specified by the one of the known, trustworthy entities.

20. The apparatus of claim 15, wherein the validation service is to compare the one or more domains with the list of known, trustworthy entities to identify a condition where the one or more domains represent a fraudulent sender having a name similar to one of the known, trustworthy entities in the list, and wherein the response from the validation service is to identify the one of the known, trustworthy entities, such that a SPF record of the at least one SPF record corresponds to the one of the known, trustworthy entities in the list and not the fraudulent sender.

21. The apparatus of claim 12, wherein said instructions when executed are to cause the at least one computer to extract a "From:" header of the e-mail message, and to derive the identified sending edge MTA from the extracted "From:" header.

22. The apparatus of claim 12, wherein said instructions when executed are to cause the at least one computer to, responsive to the authentication, cause the e-mail message to be delivered to a recipient in a manner where the e-message will be displayed in a manner that explicitly conveys that the e-mail message has been verified to have been sent on behalf of the second entity.

23. The apparatus of claim 2, wherein said instructions comprise an e-mail client plug-in.

24. An apparatus for authenticating an e-mail message, wherein the e-mail message is sent by a first entity in a manner purporting to be on behalf of a second entity, and wherein the second entity is a legal entity not inherently associated with the first entity, said apparatus comprising instructions stored on non-transitory, machine-readable media, said instructions when executed to cause an e-mail client of at least one computer to:

extract a plurality of e-mail headers from said e-mail message;

from the extracted plurality of e-mail headers, identify a sending edge mail transfer agent (MTA) associated with the first entity;

from said e-mail message, identify the second entity and a domain associated with the second entity, including by causing the at least one computer to

from the extracted plurality of e-mail headers, identify one or more domains of prior senders which are not inherently associated with the first entity,

transmit a request via a WAN to a validation service, wherein the validation service is to compare the one or more domains with a list of known, trustworthy entities having names similar to the one or more domains, and

receive a response from the validation service which provides information to identify a SPF record corresponding to one of the known, trustworthy entities;

retrieve via a wide area network (WAN) the SPF record corresponding to the one of the known, trustworthy entities, and process the retrieved SPF record to determine whether the identified sending edge MTA associated with the first entity is explicitly identified by the record as authorized to send said e-mail messages on behalf of the one of the known, trustworthy entities; and

responsively authenticate said e-mail message and cause display of the e-mail message in the e-mail client in a manner that visually indicates that the e-mail message has been verified.

* * * * *