

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
26 October 2006 (26.10.2006)

PCT

(10) International Publication Number
WO 2006/113797 A2

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2006/014727

(22) International Filing Date: 19 April 2006 (19.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/109,776 20 April 2005 (20.04.2005) US

(71) Applicant (for all designated States except US):
VERISIGN, INC. [US/US]; 487 East Middlefield
Road, Mountain View, California 94043 (US).

(72) Inventor: **CHRISTENSEN, Gerald, Todd**; 778 Owl
Court, Louisville, Colorado 80027 (US).

(74) Agents: **ROSINI, James, E.** et al.; **KENYON &**
KENYON LLP, 1500 K Street, N.W., Suite 700, Washing-
ton, DC 20005 (US).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV,
LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI,
NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,
SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,
RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA,
GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: SENDER IDENTIFICATION SYSTEM AND METHOD

(57) Abstract: A database is queried based upon data contained in a message to obtain sender identification information, at least part of which is not contained in the message as it was sent. The sender identification information is presented to a recipient, which can send a signal accepting or rejecting the message based upon the sender identification information. If an accept signal is entered, the message can be forwarded to the recipient and/or rendered to the recipient.



WO 2006/113797 A2

SENDER IDENTIFICATION SYSTEM AND METHOD

Field of the Invention

The field of the invention is messaging, and in particular the transmission of
5 ancillary information pertaining to a message.

Background of the Invention

Caller identification ("Caller ID") systems are known in the art wherein a
caller's telephone number is sent along with a telephone call to the called party. The
10 calling party's telephone number is presented to the called party, who can then
decide whether to take the call. Likewise, caller ID information is stored in
answering machine systems and presented to the called party when the messages are
received. In this way, a called party can decide whether or not to listen to a message
based upon the displayed caller ID information, and can quickly return such a call if
15 desired.

New telecommunications technologies have been developed for platforms
that can also support telephony, such as the wireless telephone. For example, Short
Message Service ("SMS") permits text messages of up to certain number characters
to be sent and received via the network operator's message center to and from any
20 suitable device (e.g., a cell phone, a computer connected to the Internet, etc.) using a
SMS Center. An SMS Center is a telecommunications platform that stores and
forwards SMS messages. Similarly, Multimedia Message Service ("MMS") permits
the delivery of text, audio, graphics, video, audio and executable code to a recipient
through a MMS Center. A MMS Center is a telecommunications platform that stores
25 and forwards multimedia messages. Each gateway can serve a subset of entities
communicating via MMS.

A known MMS system is shown in Figure 1. MMS center A 101 is coupled
through the Internet 102 to an Inter-Carrier MMS Center 103 and MMS center B
104. When originator 105 and recipient 106 are served by the same MMS center, the
30 MMS message is handled by that MMS center. However, when the originator and
recipient are served by different MMS centers, the message is sent from the
originating MMS center (e.g., MMS center A 101) to Inter-Carrier MMS center 103,
which processes the message and sends it to the MMS center that serves the

recipient (a "terminating MMS center,") e.g., MMS center B 104. The originator can be a person or a computer program (e.g., an application.)

Such new telecommunications technologies would benefit from the ability to convey sender identification information along with a message. This could help
5 prescreen unwanted messages from being sent on to a recipient, assist the recipient in deciding whether or not to view a SMS or MMS message, and help the recipient to review, search and find stored SMS and MMS messages based on corresponding stored sender information.

10 **Brief Description of the Drawings**

Figure 1 shows a prior art messaging system.

Figure 2 shows a messaging system where an identity database can be accessed by a Centralized Processing Agent in accordance with an embodiment of the present invention.

15 Figure 3 shows a flow diagram where identity information can be associated with a message by a Centralized Processing Agent in accordance with an embodiment of the present invention.

Figure 4 shows a flow diagram where identity information can be associated with a message by a Centralized Processing Agent in accordance with another embodiment
20 of the present invention.

Figure 5 shows a messaging system where an identity database can be accessed by an Originating Application in accordance with an embodiment of the present invention.

Figure 6 shows a flow diagram where identity information can be associated with a
25 message by an Originating Application in accordance with an embodiment of the present invention.

Figure 7 shows messaging system where an identity database can be accessed by a Terminating Application in accordance with an embodiment of the present invention.

30 Figure 8 shows a flow diagram where the identity information can be associated with a message by a Terminating Application in accordance with an embodiment of the present invention.

Figure 9 shows a network topology for provisioning and administering identity information in accordance with an embodiment of the present invention.

Detailed Description

In accordance with embodiments of the present invention, sender information is sent to the recipient of a message. As used herein, “message” includes
5 any data transmission, such as a MMS message, a SMS message, a SMTP message (e-mail), etc. “Message” also includes content, where “content” includes ringtones, music, graphics, games, other binary, executable or interpretable code, whether contained in the body of a message or associated with a message as an attachment, etc., that is sent from a person or an application to a recipient. A service in
10 accordance with an embodiment of the present invention correlates the sender information with the message and causes the sender information to be sent to the recipient or an agent of the recipient.

A system in accordance with an embodiment of the present invention is shown in Figure 2. Centralized Processing Agent 201 can be coupled via a network
15 202 (such as a SS7 switching network, the Internet or another IP network, etc.) directly or through a Service Control Point 203 to an Identity Database 204. Centralized Processing Agent 201 can, for example, function as an Inter-Carrier message center, a SMTP server, etc. Centralized Processing Agent 201 can also be coupled to a Message and Content Storage Database 205, which can store messages
20 and/or sender information associated with messages to be forwarded later to or towards their intended recipients. Centralized Processing Agent 201 can communicate with Originating Application 206 and Terminating Application 207 using any suitable protocol through any suitable network 210, such as the Internet, a wireless network, a LAN, a combination of networks, etc. Originating Application
25 206 can be a computer application that can act as an intermediary between Originating Entity 208 and Centralized Processing Agent 201. An Originating Entity 208 can be an entity (such as a person or computer application) that first originates the message. Likewise, Terminating Application 207 can be a computer application that can act as an intermediary between Centralized Processing Agent 201 and
30 Terminating Entity 209. Terminating Entity 209 can be an entity (such as a computer application or person) that is the final actual or intended destination for the message. In some embodiments of the present invention, Centralized Processing Agent 201 can communicate directly with Originating Entity 208 and/or

Terminating Entity 209, without communicating with an Originating Application 206 and/or Terminating Application 207, respectively.

Centralized Processing Agent 201 or Service Control Point 203 can formulate a query for Identity Database 204 based upon message data pertaining to a message received in this embodiment of the present invention at the Centralized Processing Agent 201. Identity Database 204 can be accessed using SS7, XML or any other suitable protocol. Message data can include all or part of the received message and/or information about the message, such as the source address of the message, the originating telephone number, the originating e-mail address, the originating IP address, a device identifier of the originating device, and/or any other information suitable for use as a basis for looking up information regarding a property (such as the identity) of the Originating Entity 208 or some other intermediary entity between the Originating Entity 208 and the Terminating Entity 209. Identity Database 204 stores information about senders, such as a photograph, graphic, video clip and/or audio clip associated with a sender. The sender information can be correlated with message data. In this way, Identity Database 204 can correlate certain data that can be part of the message with other identity information that may not be part of the message as it was sent. Based upon the results of the query, Centralized Processing Agent 201 or Service Control Point 203 can cause sender information to be associated with the message. The sender information that can be associated with the message can be delivered, processed and/or used as discussed in greater detail below.

A flow diagram in accordance with an embodiment of the present invention is shown in Figure 3. Originating Entity 208 (such as a person) sends a message 301 to Originating Application 206 which can process the message and/or send it 302 to Centralized Processing Agent 201. Alternatively, Originating Application 206 can automatically send the message 302 to Centralized processing Agent 201. For example, Terminating Entity 209 can subscribe to receive multimedia weather alerts from a weather web site, which can function as Originating Application 206. In one embodiment, Centralized Processing Agent 201 can determine if the message is to be associated with sender information. This can be done by comparing the destination address (e.g., destination wireless telephone number, e-mail address, etc.) of the message to a list of such destination addresses that require associated sender information. Such a list can be stored in a database (not shown) coupled to

Centralized Processing Agent 201. Alternatively, Centralized Processing Agent 201 can cause all incoming messages to be associated with sender information.

For a message that requires associated sender information, Centralized Processing Agent 201 (or Service Control Point 203) formulates and sends to
5 Identity Database 204 a query 303 based on message data. Based upon the response 304 from Identity Database 204, Centralized Processing Agent 201 can cause sender identification information to be associated with the message. The message data can include an originating cellular telephone number, source e-mail address, source IP address, business identifier, geo-location data or other information that is in or can
10 be derived from the message and that pertains to the sender. The response from Identity Database 204 can be a photograph, a graphic, text, audio, video and/or animation information associated with the sender. The message and associated sender information 305 can be sent from Centralized Processing Agent 201 to Terminating Application 207. For example, the sender information can be sent as an
15 envelope or header along with the body of the message to Terminating Application 207.

Terminating Application 207 can send the message and sender identification information 306 to Terminating Entity 209. For example, Identity Database 204 can store records that correlate a photograph of the sender with the message.
20 Terminating Application 207 can cause the photograph to be displayed to the user (e.g., on a cell phone display) and provide the Terminating Entity 209 with the option of having the message rendered (e.g., displayed, played, etc.) based upon the photograph. If Terminating Entity does not want to view, listen to or accept the message, Terminating Entity 209 can send a signal 307 to Terminating Application
25 207, e.g., by pressing a button on a cell phone key pad. In that case, the message can be deleted. A signal 308 can also be sent from Terminating Application 207 to Centralized Processing Agent 201 (and ultimately to the Originating Application 206 and/or Originating Entity 208) indicating if the message was accepted, rejected, rendered, etc. It should be noted that a message can be sent directly from an
30 Originating Entity 208 to Centralized Processing Agent 201 or through an Originating Application 206 in accordance with the present invention. Likewise, a message can be sent directly from Centralized Processing Agent 201 to a Terminating Entity 209, or through a Terminating Application 207.

In another embodiment, the sender information associated with the message can be evaluated at Terminating Application 207 to determine if the message is spam, i.e., an unsolicited message that the recipient does not wish to see.

Terminating Application 207 can perform this function using any suitable anti-spam method as is known in the art. In that case, Terminating Application 207 can block messages determined to be spam from being sent to Terminating Entity 209. Such a spam determination can be made by any entity that handles the message and to which associated sender information is available in various embodiments of the present invention, such as Originating Application 206, Centralized processing Agent 201, Terminating Application 207, etc.

Figure 4 shows a flow diagram in accordance with another embodiment of the present invention. In this embodiment, identity information 401 can be sent without the associated message from Centralized Processing Agent 201 to Terminating Application 207, while the message itself is stored at, for example, Message and Content Storage Database 205. The identification information is presented to Terminating Entity 209. Based upon the identification information, Terminating Entity 209 sends an accept or reject signal 402 to Terminating Application 207. Based upon this accept or reject signal, Terminating Application 207 can send a message 403 to Centralized Processing Agent 201 requesting that the associated message be sent or not sent, respectively, to Terminating Application 207. If the message 404 is sent, then Terminating Application 207 can forward it 405 to Terminating Entity 209.

Figure 5 shows a system in accordance with another embodiment of the present invention. Here, Originating Application 208 can query identity database 204 through network 202 based upon information pertaining to a message, such as data that is part of the message. Such message information can include all or part of the message itself and/or information about the message. Originating Application 206 can cause the response to the query (e.g., sender identification information) to be associated with the message. It can then send the message and associated sender information through a network 210 (such as the Internet) to a Terminating Application 207 or a Terminating Entity 209. Originating Application 206 can also be coupled to Message and Content Storage Database 205, which can store message and/or sender information data.

Figure 6 shows a message flow in accordance with an embodiment of the present invention in which an originating application can associate sender information with a message. Originating Entity 208 can send a message 301 to Originating Application 206, which can query 601 Identity Database 204 based upon message information, such as data that is part of the message. It can use the response 602 to associate with the message identity information that may not be part of the message as it was sent. Originating Application 206 can cause the message and associated sender information 603 to be sent to Terminating Application 207, which can solicit 604 an accept or reject signal 605 from Terminating Entity 209. Based upon this signal 605, Terminating Application 207 can send a request 606 to Originating Application 206 to send the message, which Terminating Application 207 can receive 607 and then send 608 to Terminating Entity 209.

Figure 7 shows a system in accordance with another embodiment of the present invention in which a terminating application can associate sender information with a message. Originating Application 206 can send a message through a network such as the Internet 210 to Terminating Application 207. Terminating Application 207 can be coupled to Identity Database 204, e.g., through signaling network 202 and to a Message and Control Storage Database 205. Terminating Application 207 can formulate a query based upon message information to Identity Database 204 and, based upon the response, cause sender information to be associated with the message. The sender information can be sent along with the message to a Terminating Entity (not shown), which can accept or delete the message based upon the sender information. Likewise, the sender information can be sent without the message to the Terminating Entity. In this case, the message can be stored in Message and Content Storage Database 205. The Terminating Entity can send and accept or reject signal to Terminating Application 207, which can then forward the message or not forward it, respectively, based upon the content of the signal from the Terminating Entity.

Figure 8 shows a flow diagram in accordance with an embodiment of the present invention as described in connection with Figure 7. An Originating Entity 208 can send a message 301 to an Originating Application 206, which can send it along 801 to Terminating Application 209. Terminating Application 209 can query 802 Identity Database 204 for sender information 803. Terminating Application 209 can send the sender information 804 to the Terminating Entity 207 and receive an

accept or reject signal 805 in return. If content of the accept or reject message 805 is to accept the message associated with the sender information, the Terminating Application 209 can send the message 806 to the Terminating Entity 207.

Alternatively, Terminating Application 209 can send both the message and the
5 associated sender information to Terminating Entity 207, which can locally decide whether to render the message or delete it based upon the sender information.

In yet other embodiments, Terminating Entity 209 can receive a message but not fully display it to the user. Terminating Entity 209 can cause identity
10 information to be associated with the received message by formulating a query based upon message information (such as message data) and sending it to Identity Database 204. Identity Database can return identity information associated with the sender of the message. This identity information can be displayed to the user that can be utilized by the user as the basis for entering an accept or reject signal at Terminating Entity 209. If an accept indication is detected at Terminating Entity
15 209, then the message itself is rendered to the user. If a reject indication is detected at Terminating Entity 209, then the message can be deleted. An indication as to whether the message was accepted and/or deleted can be sent back to the originator.

In one embodiment, Terminating Entity 209 can be caused to obtain associated identity information with a message by running or interpreting an
20 executable or interpretable program sent as part of the received message or as an attachment to the received message. The executable or interpretable program can contain instructions adapted to be executed by a processor at Terminating Entity 209 to formulate a query based upon the received message (e.g., the source telephone number, the source IP address, content in the body of the message, etc.) and send it
25 to Identity Database 204. The instructions can be executed by the processor to receive the response from Identity Database 204, cause it to be displayed in some form to the user, and detect an accept or reject indication from the user. Based on the detected indication, the instructions can be executed by the processor to either render the message to the user or not.

30 Identity information can also be associated with a message at the outset by Originating Entity 208, which can formulate a query and send it to Identity Database 204 to obtain identity information that can be associated with the message. The message and associated identity information can be sent to a recipient that can

evaluate the identity information as a basis for accepting and/or passing on the message itself.

In accordance with an embodiment of the present invention, Originating Entity 208 can be a cell phone, a software application (e.g., at a web site), etc. For example, Originating Entity 208 can be a cell phone utilized by a user to send a text, audio, video or other kind of message to another user at a different cell phone, e.g., Terminating Entity 209. Originating Entity 208 can be a software program running at a weather web site that automatically sends a message in any suitable media, such as a short animated graphic showing weather patterns move across a geographic area, every day at the same time to a subscriber with a computer or cell phone (Terminating Entity 209.)

Originating Application 206 and Terminating Application 207 can be local messaging centers responsible for storing and forwarding messages to and from their respective sets of originating and terminating entities, e.g., sets of cell phone customers. For example, Originating Application 206 can be a local messaging center operated by Sprint for Sprint messaging customers, and Terminating Application 207 can be operated by MCI for messaging MCI customers. Alternatively, they can be operated by the same carrier for subscribers in different geographic locations, e.g., Originating Application 206 can be in Chicago and Terminating Application 207 can be in Cleveland.

Centralized processing Agent 201 can be an inter-carrier message center responsible for routing and/or storing and forwarding messages between messaging centers, and/or associating identity information with a message. Central Processing Agent 201 can be operated by a carrier, by a third party service provider, or by any suitable party.

Anti-spam features can be implemented in embodiments of the present invention utilizing the identity information associated with a message. For example, at any point along the path taken by the message and/or identity information (e.g., any entity from and including Originating Entity 208 to and including Terminating Entity 209, including Originating Application 206, Centralized Processing Agent 201, Terminating Application 207, etc.) a filter can be applied that can block or pass on the message and/or identity information based upon, for example a blacklist. In this embodiment, a set of identity information items (e.g., photographs, textual representations of users names, vide clips, audio clips, etc.) can be maintained on a

blacklist. An entity along the transmission path can compare identity information associated with a message to the blacklist. If the identity information is on the blacklist, then the message and/or identity information can not be forwarded to the next entity in the transmission path, can be deleted, can be specially labeled as a
5 result of being associated with a blacklist, etc. Similarly, a whitelist can be maintained where the message and/or identity information is only forwarded if the identity information associated with the message is also on a whitelist, can be specially labeled as a result of being associated with a whitelist, etc. This can be done for identity information such as audio clips, video clips and photographs by
10 comparing a hash, Message Authentication Code ("MAC"), digital signature, etc., of the identity information with a list of hashes, MACs, digital signatures, etc. on the blacklist or whitelist. Special labels can include setting a flag or associating some other kind of label with the message and/or identity information, such as "warning," "pornographic," "whitelist-approved," etc.

15 Likewise, more complex filtering techniques can be used in accordance with embodiments of the present invention. For example, a profile can be stored that is associated with any entity in the message path, where the profile includes a policy for handling a message based upon its associated identity information. For example, a profile for John Smith can include policy rules such as, "If identity information
20 indicates message is from Paul Johnson, then forward message only during regular business hours"; "If identity information indicates message is from Acme Corporation, mark message URGENT and forward immediately"; "If message is not from Beta Corporation, then authenticate sender before forwarding"; "Delete any message that is associated with authenticated sender identity information"; etc. Any
25 suitable rule can be implemented in the profile and enforced. In particular, the profile can store policy rules correlated with the appropriate identity information. An entity in the transmission path can consult the database storing the identity and rule information, find the rule, if any, associated with the identity information that is associated with the message, and then perform the action or actions prescribed by
30 the rule.

In an embodiment of the present invention, an entity in the transmission path can receive a message and first determine if sender identity information should be caused to be associated with the message based upon address data in the message for the intended recipient. For example, the intended recipient can be required to

subscribe to a service that associates sender identity information with a message to the recipient, and permits the recipient or another entity in the transmission path to take some action with respect to the message. Identity information can be stored in Identity Database 204, which can associate certain data that can be contained in the message, such as a source IP address, a sender telephone number, business identifier, geo-location data, all or part of a domain name, header information, etc. with sender identity information that may not be contained in the message, such as a photograph of the sender, a video clip, an audio clip, animation, text (e.g., the sender's name and/or location, etc.) A query that includes data that can be contained in the message is formulated and sent to Identity Database 204, which sends a response containing the associated sender information that may not be in the message, e.g., a photograph, video clip, text, etc.

Figure 9 shows a system for provisioning and administering identity information in accordance with an embodiment of the present invention. A Provisioning and Administrator Server 901 is coupled to Identity Database 204 and Digital Certificate database 902 through a network 903 such as the Internet. Identity Database 204 can include identity information of various forms including, but not limited to, text, numeric text, alpha-numeric text, photographs, graphics, animation, video content, audio content, executable code, etc. The system can permit a database administrators to associate identity information with data such as Mobile Identification Numbers, Electronic Serial Numbers, Automatic Number Identification, Geo-location data, e-mail addresses, Instant Messaging pseudonyms and other aliases, etc., that can be obtained during the operation of data messaging and/or content services. The identity information with which this data can be associated can include a text version of a sender's name, a photograph or graphic of the sender or sender's organization, a video clip representative of the sender, an audio clip such as an audio greeting from the sender, etc. Security can be maintained using digital certificates. For example, the integrity of digitally signed identity information can be verified by the Provisioning and Administrator Server 801 by consulting the Digital Certificate Database 902.

Authentication can be implemented in accordance with embodiments of the present invention. For example, a subscriber profile can specify that a successful challenge/response must be exchanged with Originating Entity 208 and/or Originating Application 206 before a message is to be forwarded to Terminating

Entity 209. For example, an entity in the transmission path can send a query to an Originating Entity 208 asking Originating Entity 208 to enter his mother's maiden name. The entry is compared to a stored version of the correct answer, and the message can be forwarded only if there is a correct match. Otherwise, the message
5 can be deleted. Likewise, sender information can be digitally signed by the sender and/or by a Certification Authority. The signature can be checked by an entity in the transmission path. If the signature cannot be successfully verified, then the message can be deleted. Otherwise, the message can be forwarded and/or read. Also, multi-factor authentication schemes can be implemented, for example, at Originating
10 Entity 208 (e.g., a first cell phone) and Terminating Entity 209 (e.g., a second cell phone.) A one time password can be generated using a first secret stored at Originating Entity 208 along with, for example, a Personal Identification Number (PIN) known only to a user of the first cell phone. Terminating Entity 209 can require that the one time password be verified by any entity in the transmission path.
15 If the one time password is not successfully verified, then the message can be deleted. Otherwise, the message can be forwarded and/or read.

An embodiment of the present invention can be implemented by instructions stored on a medium or transmitted over a network, where the instructions are adapted to be executed by a processor to perform all or part of the method in
20 accordance with the present invention. An apparatus that implements an embodiment of the present invention can include such instructions stored in a memory coupled to a processor adapted to execute the instructions. Examples of memory include Random Access Memory, flash memory, Read Only Memory, a hard disk, a Compact Disc, and any other medium adapted to store digital
25 information. Examples of a processor include the Pentium IV processor manufactured by the Intel Corporation of Santa Clara, California. A processor can also be an Application Specific Integrated Circuit (ASIC) that embodies at least part of the method in accordance the present invention in hardware and firmware. The processor can also be coupled to a display, where a display is any device suitable for
30 rendering digital information in a perceptible manner. Examples of a display include a LCD screen, a CRT screen, a speaker, etc. The processor can also be coupled to an input device, such as a touch screen, keypad, microphone, etc.

The foregoing examples are meant to illustrate the present invention. One of ordinary skill in the art will appreciate that the full scope of the invention extends

beyond the examples discussed above. For example, while the examples describe the present invention with respect to a MMS messaging protocol, the present invention also encompasses embodiments in accordance with other protocols, such as SMS, EMS and WAP. For example, sender identification information can be associated
5 and used with a SMS or WAP message in much the same way as it is associated with a MMS message. These and other embodiments are within the scope of the present invention.

What is claimed is:

1. A method for messaging, including:
sending to an identity database a query based upon data included in a
received message;
5 receiving from the identity database information pertaining to the identity of
a sender of the message, including identity information that is not a part of the
message as it was sent; and
causing the identity information to be sent to a user;
receiving an accept or reject signal from a user that is based upon the identity
10 information sent to the user;
if an accept signal is received, then causing the message to be forwarded to
the user or to be rendered to the user.
2. The method of claim 1, further including determining whether to associate
15 identity information with the message based upon the address of the intended
recipient of the message.
3. The method of claim 1, wherein the sender of the message is a person, and
wherein the identity information includes a photograph of the person.
20
4. The method of claim 1, wherein the sender of the message is a person or a
computer application program, and wherein the identity information includes audio
representative of the person or computer application program.
- 25 5. The method of claim 1, wherein the sender of the message is a person or
computer program application, and wherein the identity information includes video
representative of the person or computer program application.
6. A medium storing instructions adapted to be executed by a processor to
30 perform steps including:
sending to an identity database a query based upon data included in a
received message;

receiving from the identity database information pertaining to the identity of a sender of the message, including identity information that is not a part of the message; and

causing the identity information to be sent to a user;

5 receiving an accept or reject signal from a user that is based upon the identity information sent to the user;

if an accept signal is received, then causing the message to be forwarded to the user or to be rendered to the user.

10 7. The medium of claim 6, further including instructions adapted to be executed by a processor to determine whether to associate identity information with the message based upon the address of the intended recipient of the message.

8. The medium of claim 6, wherein the sender of the message is a person, and
15 wherein the identity information includes a photograph of the person.

9. The medium of claim 6, wherein the sender of the message is a person or a computer application program, and wherein the identity information includes audio representative of the person or computer application program.

20

10. The medium of claim 6, wherein the sender of the message is a person or computer program application, and wherein the identity information includes video representative of the person or computer program application.

25 11. An apparatus for messaging, including:

A processor;

A display coupled to said processor;

An input device coupled to said processor; and

A memory coupled to said processor, said memory storing instructions

30 adapted to be executed by said processor to receive sender identification information associated with a message, wherein the sender information includes information that is not part of the message as it was sent, to render the sender identification information through said display and to receive through said input device an accept or reject signal based upon the sender identification information.

12. The apparatus of claim 6, wherein the sender of the message is a person, and wherein the identity information includes a photograph of the person.

5

13. The apparatus of claim 11, wherein the sender of the message is a person or a computer application program, and wherein the identity information includes audio representative of the person or computer application program.

10

14. The apparatus of claim 6, wherein the sender of the message is a person or computer program application, and wherein the identity information includes video representative of the person or computer program application.

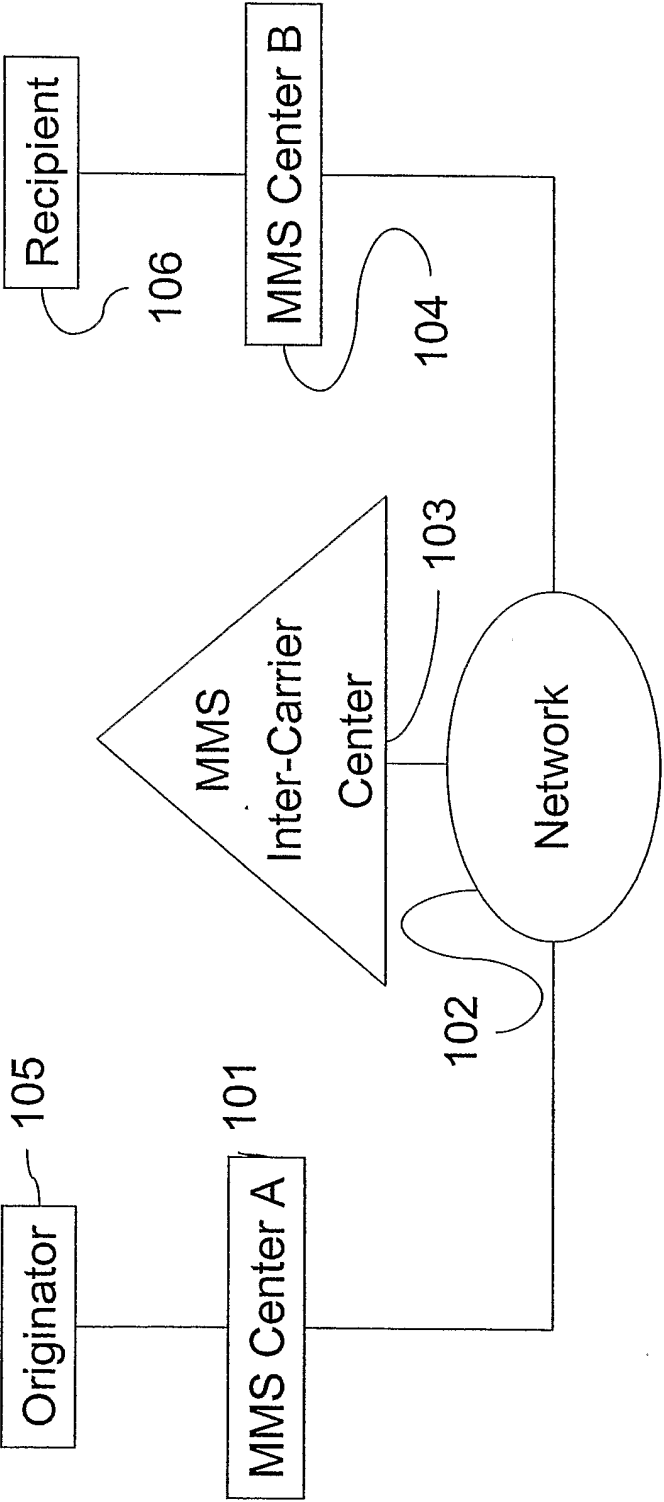


Figure 1
Prior Art

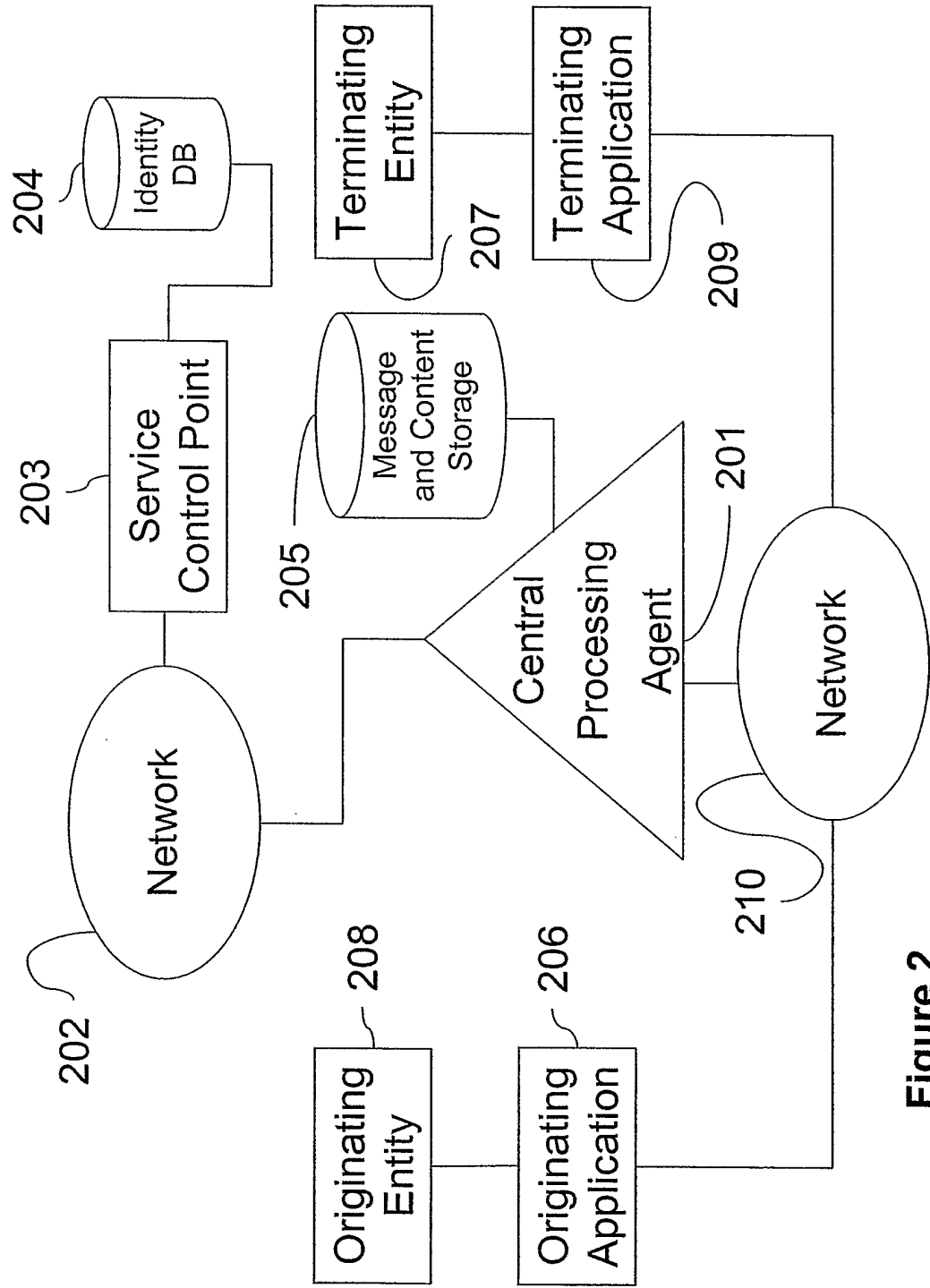


Figure 2

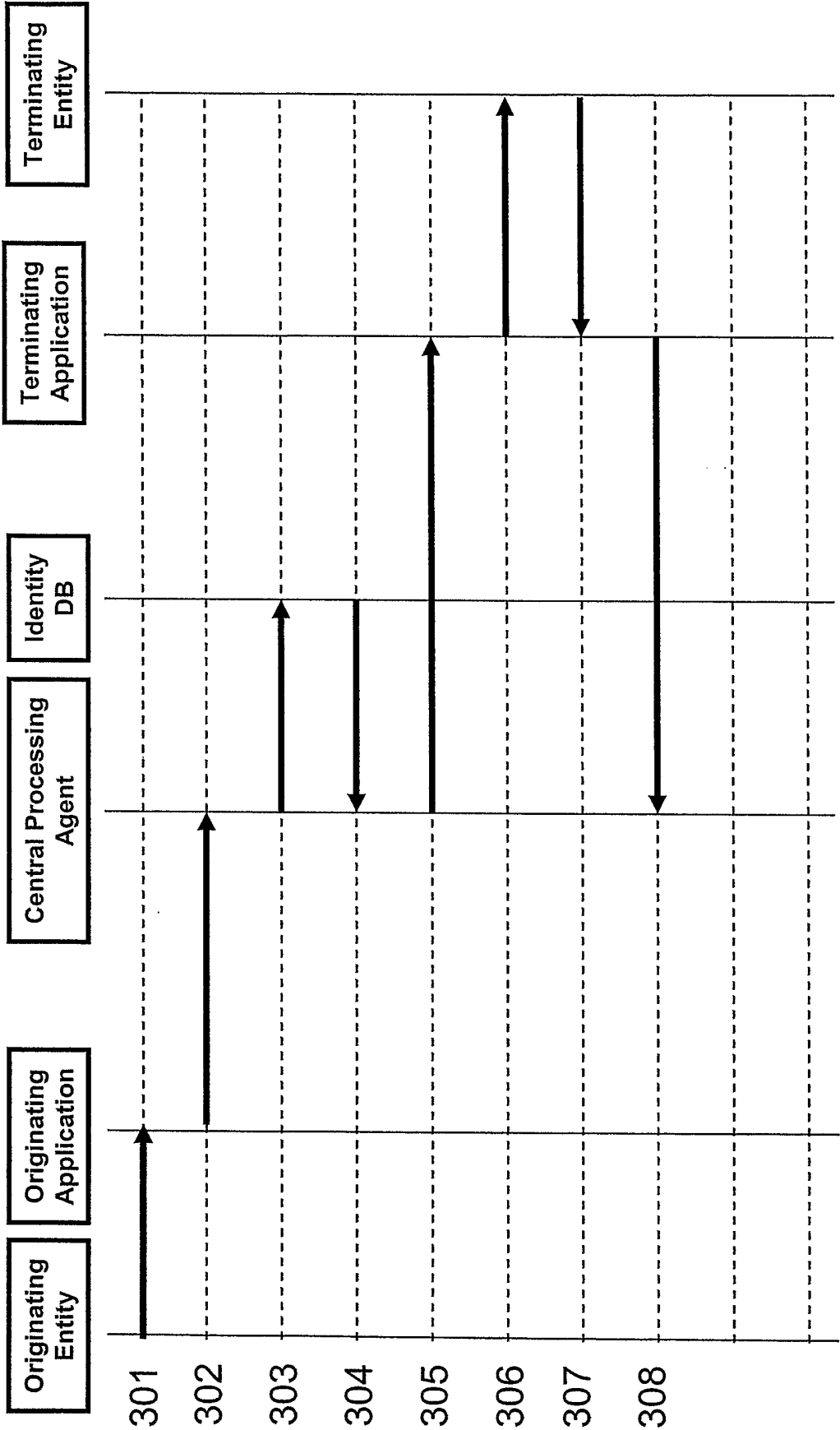


Figure 3

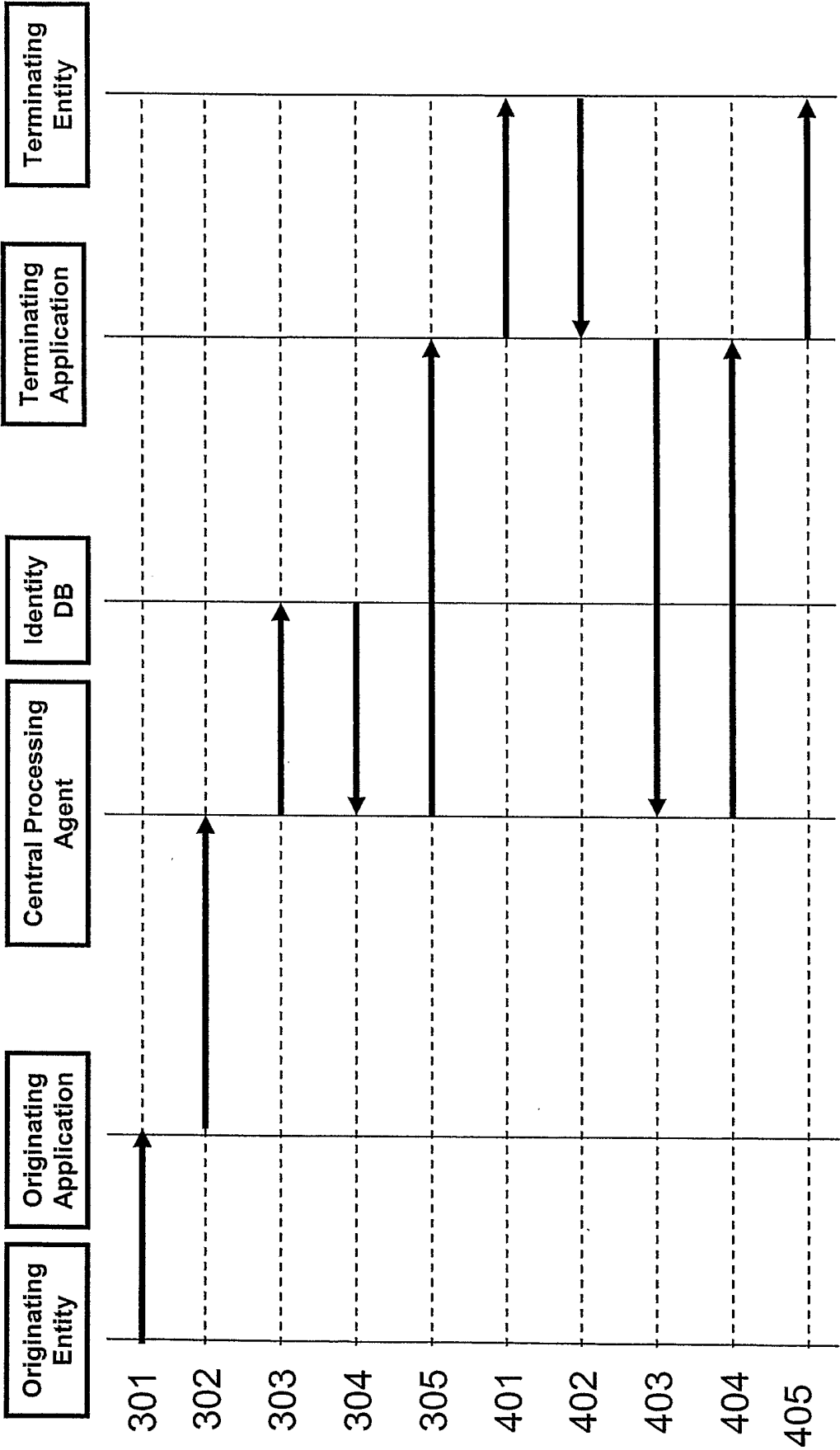


Figure 4

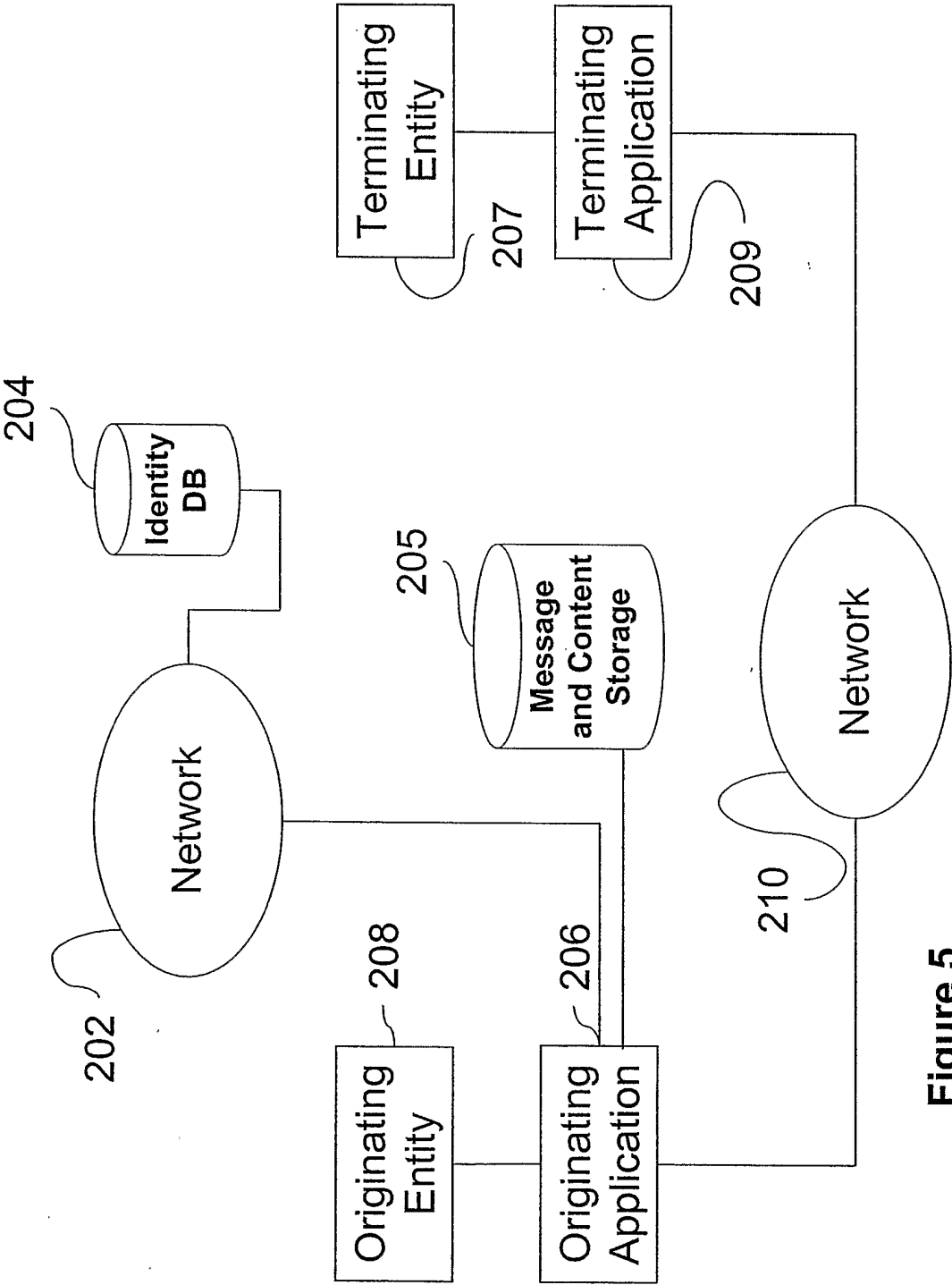


Figure 5

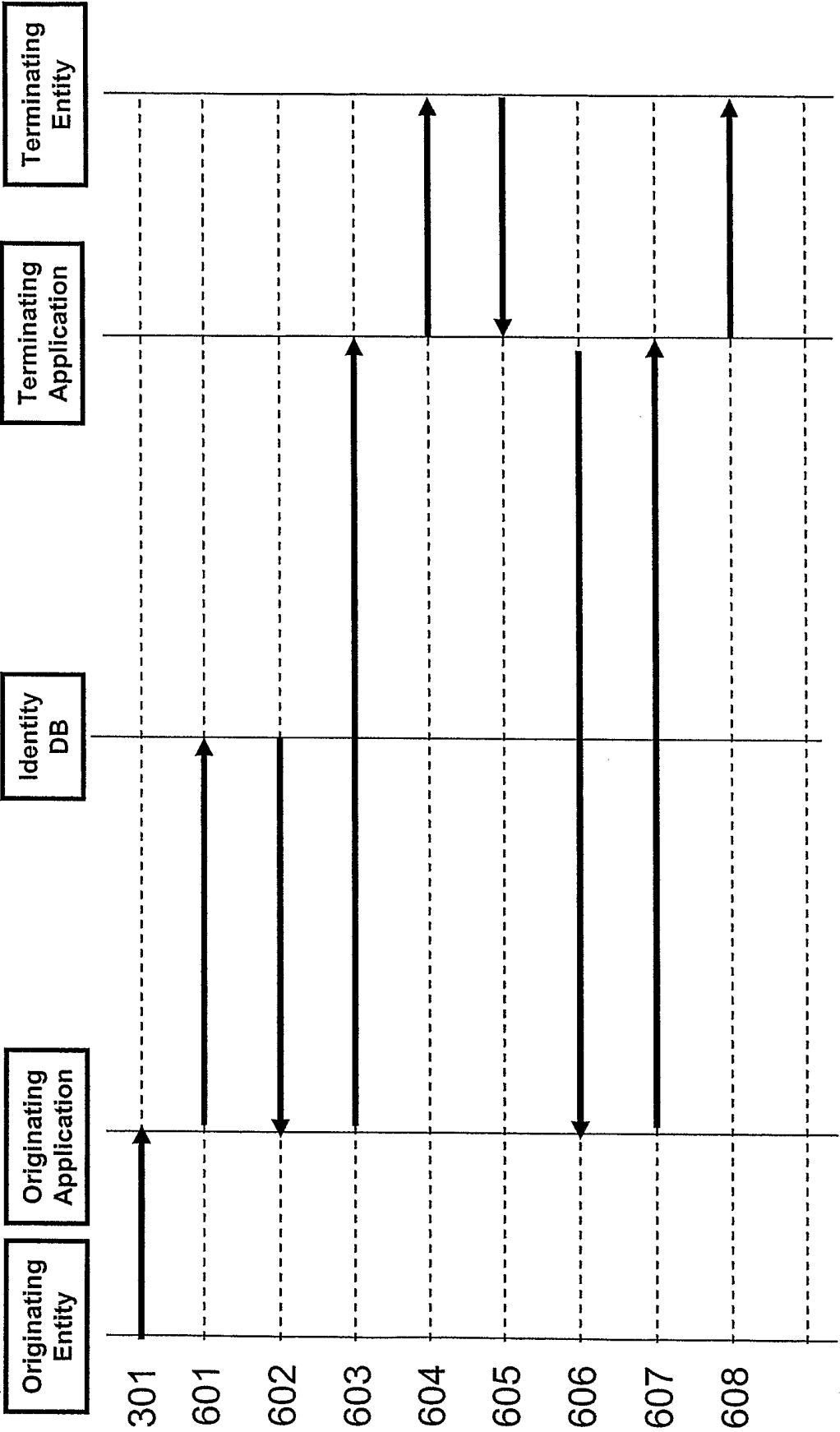


Figure 6

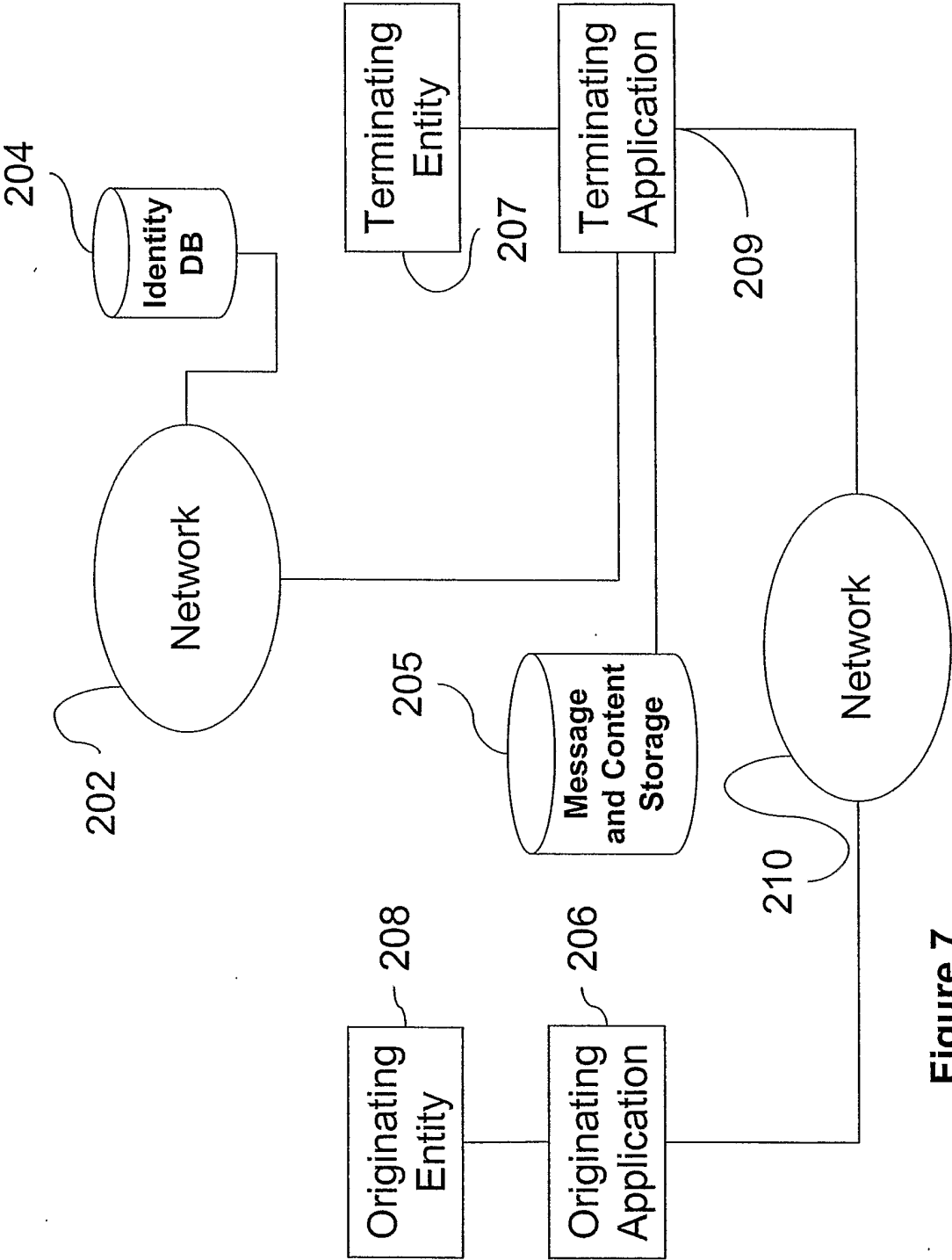


Figure 7

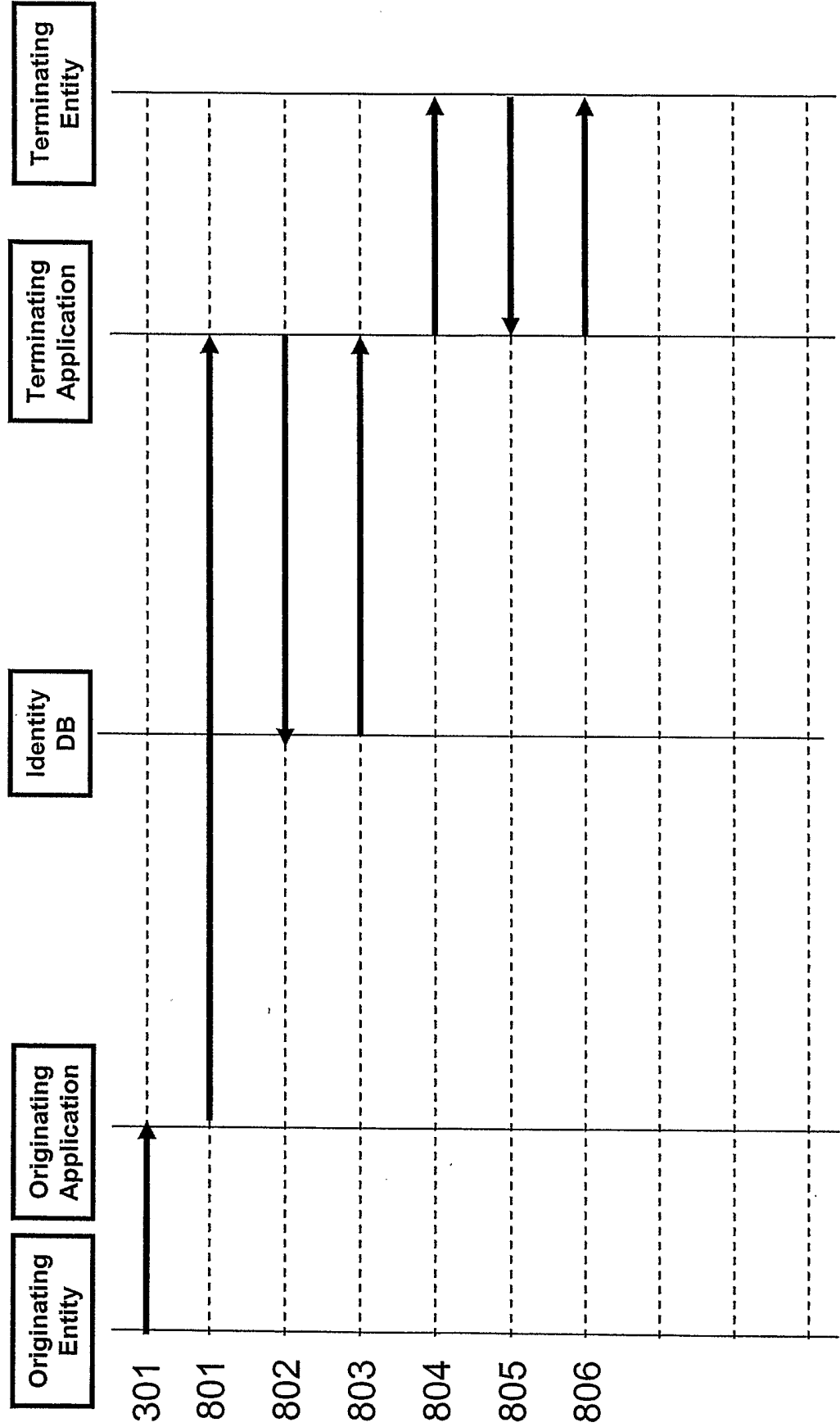


Figure 8

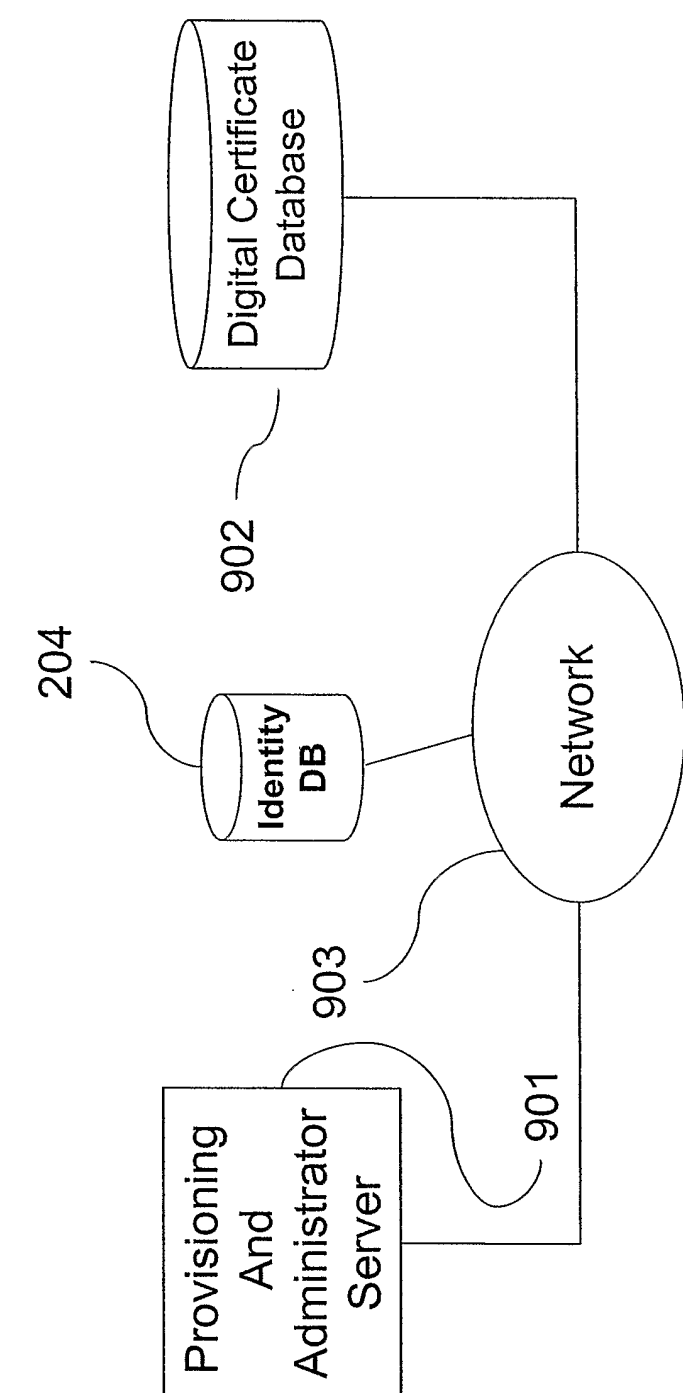


Figure 9