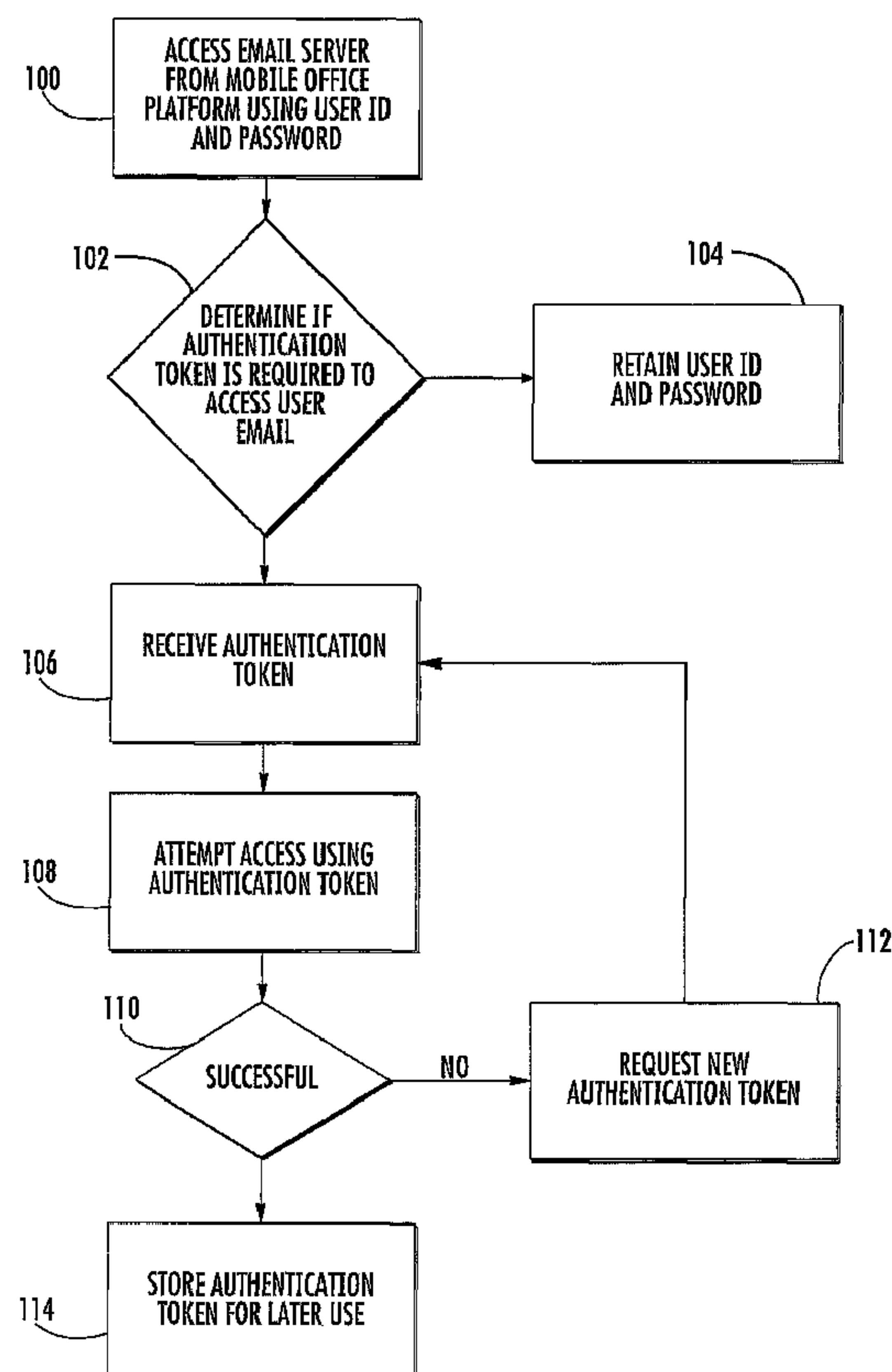




(86) Date de dépôt PCT/PCT Filing Date: 2005/09/28
(87) Date publication PCT/PCT Publication Date: 2007/05/18
(45) Date de délivrance/Issue Date: 2013/12/17
(85) Entrée phase nationale/National Entry: 2008/03/18
(86) N° demande PCT/PCT Application No.: US 2005/035005
(87) N° publication PCT/PCT Publication No.: 2007/055680
(30) Priorité/Priority: 2005/09/28 (US11/237096)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01)
(72) Inventeur/Inventor:
GORTY, SURYANARAYANA MURTHY, US
(73) Propriétaire/Owner:
BLACKBERRY LIMITED, CA
(74) Agent: BORDEN LADNER GERVAIS LLP

(54) Titre : SYSTEME ET PROCEDE PERMETTANT D'AUTHTENTIFIER UN UTILISATEUR POUR ACCES A UN
COMPTE DE COURRIERS ELECTRONIQUES AU MOYEN D'UN JETON D'AUTHTENTIFICATION
(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A USER FOR ACCESSING AN EMAIL ACCOUNT USING
AUTHENTICATION TOKEN



(57) Abrégé/Abstract:

A system authenticates a user for accessing an electronic mailbox of the user from a remote device and obtaining electronic mail (email). An email server is provided by an email service provider and contains the electronic mailbox of the user. A mobile office



(57) **Abrégé(suite)/Abstract(continued):**

platform is operative for accessing the email server and determines if an authentication token is required to access the electronic mailbox of the user. An authentication token is received from the email server or other server if an authentication token is required. Access is attempted to the electronic mailbox of the user using the authentication token. The authentication token is stored for subsequent use by the user to access their electronic mailbox if access to the electronic mailbox using the token has been successful.

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
18 May 2007 (18.05.2007)

PCT

(10) International Publication Number
WO 2007/055680 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2005/035005

(22) International Filing Date:
28 September 2005 (28.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **TEA-MON SYSTEMS, INC.** [US/US]; 1180 NW Maple Street, Suite 201, Issaquah, WA 98027 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **GORTY, Suryanarayana, Murthy** [IN/US]; 10177 224th Avenue NE, Redmond, WA 98053 (US).

(74) Agents: **WARTHER, Richard, K.** et al.; 255 S. Orange Avenue, Suite 1401, Orlando, FL 32801 (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, 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.

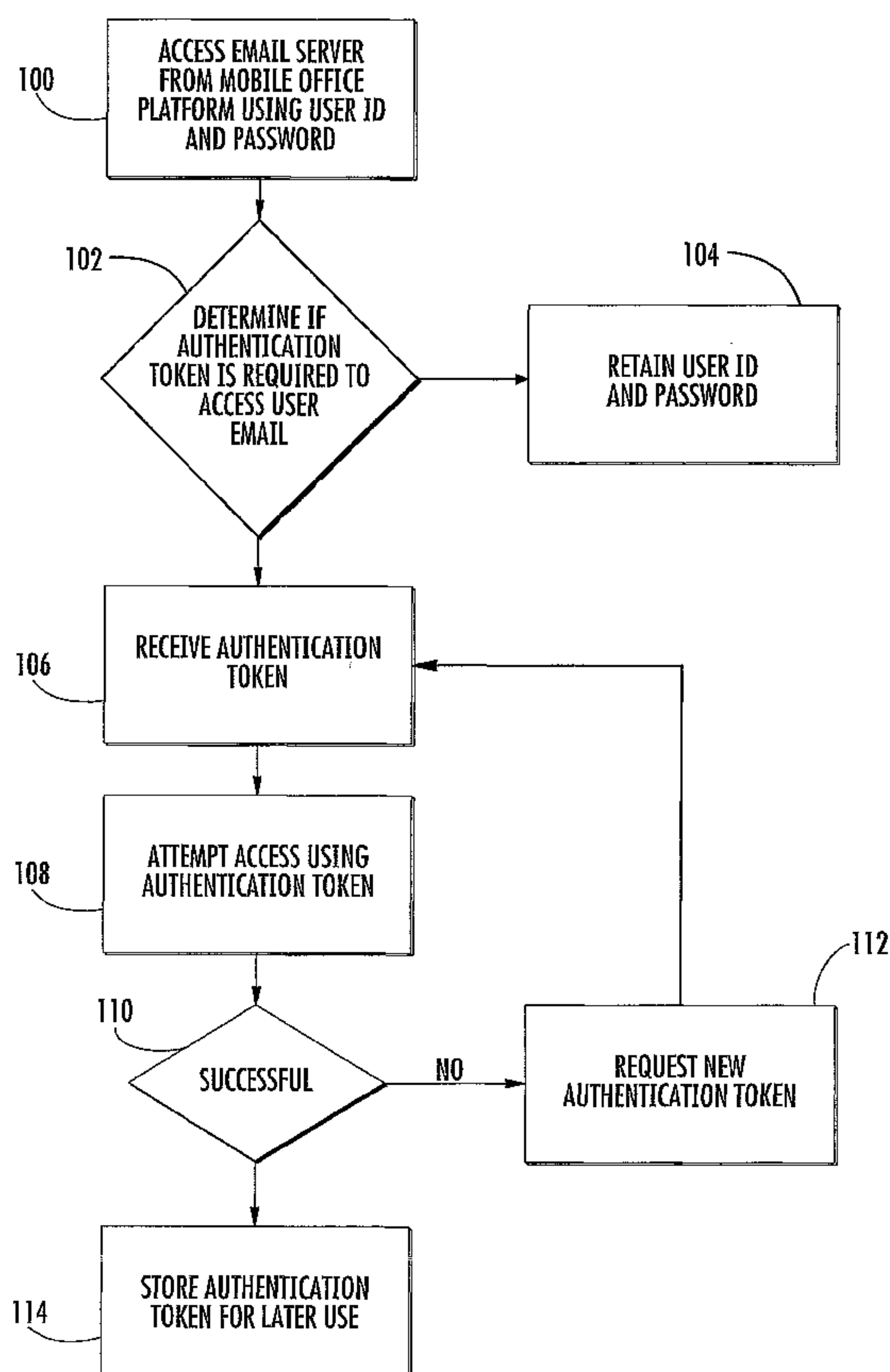
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, 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:

— with international search report

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

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A USER FOR ACCESSING AN EMAIL ACCOUNT USING AUTHENTICATION TOKEN



(57) Abstract: A system authenticates a user for accessing an electronic mailbox of the user from a remote device and obtaining electronic mail (email). An email server is provided by an email service provider and contains the electronic mailbox of the user. A mobile office platform is operative for accessing the email server and determines if an authentication token is required to access the electronic mailbox of the user. An authentication token is received from the email server or other server if an authentication token is required. Access is attempted to the electronic mailbox of the user using the authentication token. The authentication token is stored for subsequent use by the user to access their electronic mailbox if access to the electronic mailbox using the token has been successful.

WO 2007/055680 A1

**SYSTEM AND METHOD FOR AUTHENTICATING A USER FOR
ACCESSING AN EMAIL ACCOUNT USING AUTHENTICATION TOKEN**

Field of the Invention

[0001] The present invention relates to the field of communications systems, and, more particularly, to electronic mail (email) communications systems and related methods.

Background of the Invention

[0002] Electronic mail (email) has become an integral part of business and personal communications. As such, many users have multiple email accounts for work and home use. Moreover, with the increased availability of mobile cellular and wireless local area network (LAN) devices that can send and receive emails, many users wirelessly access emails from mailboxes stored on different email storage servers (e.g., corporate email storage server, Yahoo, Hotmail, AOL, etc.).

[0003] Yet, email distribution and synchronization across multiple mailboxes and over wireless networks can be quite challenging, particularly when this is done on a large scale for numerous users. For example,

different email accounts may be configured differently and with non-uniform access criteria. Moreover, as emails are received at the wireless communications device, copies of the emails may still be present in the original mailboxes, which can make it difficult for users to keep their email organized.

[0004] One particularly advantageous "push" type email distribution and synchronization system is disclosed in U.S. Patent No. 6,779,019 to Mousseau et al., which is assigned to the present Assignee. This system pushes user-selected data items from a host system to a user's mobile wireless communications device upon detecting the occurrence of one or more user-defined event triggers. The user may then move (or file) the data items to a particular folder within a folder hierarchy stored in the mobile wireless communications device, or may execute some other system operation on a data item. Software operating at the device and the host system then synchronizes the folder hierarchy of the device with a folder hierarchy of the host system, and any actions executed on the data items at the device are then automatically replicated on the same data items stored at the host system, thus eliminating the need for the user to manually replicate actions at the host system that have been executed at the mobile wireless communications device.

[0005] The foregoing system advantageously provides great convenience to users of wireless email communication devices for organizing and managing their email messages. Yet, further convenience and efficiency features may be desired in email distribution and synchronization systems as email usage continues to grow in popularity. For example, certain email service

providers are no longer allowing third-party providers to access accounts using a password and user identifier (ID), for example, an email address, even though the user provides this information to the third-party provider. Instead, these email service providers do not want this information to be stored on third-party systems, and have instead required that such third parties use authentication tokens generated by the email service provider for accessing the user email account. Some third-party systems initially log-on using the user ID and password supplied from the user. The email service provider provides the token, and the system deletes the password and user ID, then stores the authentication token for future use. This is not always advantageous and authentication tokens may not be required for different accounts.

Brief Description of the Drawings

[0006] Other objects, features and advantages of the present invention will become apparent from the detailed description of the invention which follows, when considered in light of the accompanying drawings in which:

[0007] FIG. 1 is schematic block diagram of a direct access electronic mail (email) distribution and synchronization system.

[0008] FIG. 2 is a schematic block diagram of an exemplary embodiment of user interface components of the direct access proxy of the system of FIG. 1.

[0009] FIG. 3 is a schematic block diagram of an exemplary embodiment of the Web client engine of the system of FIG. 1.

[0010] FIGS. 4 is a schematic block diagram of an exemplary embodiment of the mobile office platform engine machine for use in the system of FIG. 1.

[0011] FIG. 5 is a schematic block diagram of an exemplary embodiment of the database module of the system of FIG. 1.

[0012] FIG. 6 is a high-level flowchart showing an example of a method that can be used for authenticating a user to obtain electronic mail (email) using authentication tokens.

[0013] FIG. 7 is a schematic block diagram illustrating an exemplary mobile wireless communications device that can be used with the Direct Access system shown in FIG. 1.

Detailed Description of the Preferred Embodiments

[0014] Different embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments are shown. Many different forms can be set forth and described embodiments should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope to those skilled in the art. Like numbers refer to like elements throughout, and prime notation is used to indicate similar elements in alternative embodiments.

[0015] A system authenticates a user for accessing an electronic mailbox of the user from a remote device and obtains electronic mail (email). The email server is provided by an email service provider that includes the electronic mailbox of the user. A mobile office platform is operative for accessing the email server

provided by the email service provider. A determination is made if an authentication token is required to access the electronic mailbox of a user. The authentication token is received from the email server if an authentication token is required. Access to the electronic mailbox of the user is attempted using the authentication token. The authentication token is stored for subsequent use by the user to access their electronic mailbox if access to the electronic mailbox using the authentication token has been successful.

[0016] In another aspect, a mobile wireless communications device receives user email from the mobile office platform. A database is operative with the mobile office platform and stores the authentication token for subsequent use when the user attempts access through the mobile office platform, which can include an email server and a direct access proxy for accessing and retrieving user emails from the electronic mailbox of the user. The mobile office platform includes a database for storing the authentication token for subsequent use when the user attempts access to the electronic mailbox of the user through the mobile office platform.

[0017] The mobile office platform is also operative for initially accessing the electronic mailbox for the user identification and email address. The mobile office platform is also operative for discarding the user identification and email address if the authentication token can access the electronic mailbox of the user. The mobile office platform can also be operative for retaining the user identification and email address if an authentication token is not

required for accessing the electronic mailbox of the user.

[0018] A method and computer-readable medium having computer-executable instructions with the described functions is also set forth.

[0019] Referring initially to FIG. 1, a direct access (DA) email distribution and synchronization system **20** allows direct access to different mail sources, allowing messages to be transferred directly to a mobile wireless handheld device from a source mailbox. As a result, different mail stores need not be used for integrated external source mail accounts, and a permanent copy of an email in a local email store is not required.

[0020] Although this diagram depicts objects as functionally separate, such depiction is merely for illustrative purposes. It will be apparent to those skilled in the art that the objects portrayed in this figure can be arbitrarily combined or divided into separate software, firmware or hardware components. Furthermore, it will also be apparent to those skilled in the art that such objects, regardless of how they are combined or divided, can execute on the same computing device or can be arbitrarily distributed among different computing devices connected by one or more networks.

[0021] The direct access system **20** enables email users or subscribers to have email from third-party email services pushed to various mobile wireless communications devices **25**. Users need not create a handheld email account to gain direct access to an existing external email account. The direct access system **20** may operate without performing aggregation as used in some prior art systems, in which emails are

aggregated from multiple different source mailboxes to a single target mailbox. In other words, email need not be stored in an intermediate target mailbox, but instead may advantageously be accessed directly from a source mail store.

[0022] As illustrated in FIG. 1, the direct access system **20** illustratively includes a Web client (WC) engine **22** and a mobile office platform (MOP) **24**. These Web client engine **22** and mobile office platform **24** operate together to provide users with direct access to their email from mobile wireless communications devices **25** via one or more wireless communications networks **27**, for example. Both the Web client engine **22** and the mobile office platform **24** may be located at the same location or at separate locations, and implemented in one or more servers. The web client engine **22** illustratively includes a port agent **30** for communicating with the wireless communications devices **25** via the wireless communications network(s) **27**, a worker **32**, a supervisor **34**, and an attachment server **36**, which will be discussed further below. An alert server **38** is shown in dashed lines, and in one preferred embodiment, is not used, but could be part of the system in yet other embodiments.

[0023] The mobile office platform **24** illustratively includes a DA proxy **40**, and a proxy application programming interface (API) **42** and a cache **44** cooperating with the DA proxy. The mobile office platform **24** also illustratively includes a load balance and cache (LBAC) module **46**, an event server **48**, a universal proxy (UP) Servlet **54**, an AggCron module **56**, a mobile office platform (MOP) engine **58**, and a database (DB) engine **60**, which will be discussed in further detail below. The Least Recently Used (LRU)

cache **41** caches new messages, and can release messages and objects that were least recently used.

[0024] The supervisor **34** processes new mail notifications that it receives from the direct access proxy **40**. It then assigns a job, in the form of a User Datagram Protocol (UDP) packet, to the least-loaded worker **32**, according to the most recent UDP heartbeat the supervisor **34** has received. For purposes of this description, heartbeat is a tool that monitors the state of the server. Additionally, the supervisor **34** will receive a new service book request from the direct access proxy **40** to send service books to the mobile wireless communication device for new or changed accounts. A service book can be a class that could contain all service records currently defined. This class can be used to maintain a collection of information about the device, such as connection information or services, such as an email address of the account.

[0025] The worker **32** is an intermediary processing agent between the supervisor **34** and the port agent **30**, and responsible for most processing in the Web client engine **22**. It will retrieve e-mail from a universal proxy **54**, via a direct access proxy, and format e-mail in Compressed Multipurpose Internet Mail Extension (CMIME) as a type of Multipurpose Internet Mail Extension, and send it to the port agent **30**, for further processing. Its responsibilities include the following tasks: (1) messages sent to and received from the handheld; (2) message reply, forward and more requests; (3) Over The Air Folder Management operation (OTAFM); (4) attachment viewing; and (5) service book.

[0026] The port agent **30** acts as a transport layer between the infrastructure and the rest of the Web

client engine 22. It is responsible for delivering packets to and from the mobile wireless communications device. To support different integrated mailboxes with one device, more than one service book can be used, and each service book can be associated with one integrated mailbox. A port agent 30 can include one Server Relay Protocol (SRP) connection to a relay, but it can also handle multiple SRP connections, and each connection may have a unique Globally Unique Identifier (GUID) associated with a service book. The attachment server 36 provides service for document/attachment conversion requests from workers 32.

[0027] The direct access proxy 40 provides a Web-based Distributed Authoring and Versioning (WebDAV) interface that is used by the worker 32 to access account and mailbox information. This provides functionality to create, change and move documents on a remote server, e.g., a Web server. The direct access proxy 40 typically will present an asynchronous interface to its clients. The LBAC module 46 is used by a notification server and the Web client engine 22 components to locate the proper DA proxy for the handling of a request. The universal proxy Servlet 54 abstracts access to disparate mail stores into a common protocol. The event server 48 responds to notifications of new messages from corporate servers 52 and/or mail service providers 50, which may be received via the Internet 49, for example. The notifications are communicated to the direct access proxy 40 by the AggCron module 56 and the event server 48 so that it may initiate checking for new mail on source mailboxes 51, 53 of the mail service providers 50 and/or corporate servers 52. The proxy API can be a Simple Object Access Protocol (SOAP) Daemon 42 and is the

primary interface into a database **60**, which is the primary data store for the mobile office platform **24**. The AggCron module **56** may also periodically initiate polling for new messages as well.

[0028] FIG. 2 is a high-level block diagram showing user interface components of the direct access proxy **40**. More particularly, the direct access proxy **40** illustratively includes an identifier module **72** with various downstream proxy modules for different communication formats, such as a Wireless Application Protocol (WAP) proxy module **74** and a Hypertext Markup Language (HTML) proxy module **76**. Of course, it will be appreciated by those skilled in the art that other types of proxy modules for other communications formats may also be used.

[0029] The identifier module **72** provides a centralized authentication service for the direct access system **20** and other services. An authentication handshake may be provided between an ID service and direct access system **20** to ensure that users have the proper credentials before they are allowed access to the direct access system **20**. The ability to switch from managing a Web client to a direct access system, or vice versa, may occur without requiring the user to re-enter any login credentials. Any Web client and direct access may share session management information on behalf of a user.

[0030] The WAP proxy **74** provides a wireless markup language (WML)-based user interface for configuring source mailboxes with the mobile office platform **24**. The HTML proxy **76** provides an HTML-based user interface for configuring of source mailboxes in the MOP **24**. The proxy API **42** (SOAP Daemon) is the primary interface into the database **60**. The engine **58** is a protocol

translator that connects to a source mailbox to validate configuration parameters. The database 60 is the primary user data store for the mobile office platform 24.

[0031] FIGS. 3, 4 and 5 illustrate respective Web client engine machines 80 (FIG. 3), an engine machine 82 (FIG. 4), and database machine 84 (FIG. 5). The Web client engine machine 80 illustratively includes the supervisors 34, workers 32, and port agents 30. Relays 86 cooperate with the port agents 30 using a GUID.

[0032] The engine machine 82 illustratively includes a direct access proxy 40, HTML proxy 76, WAP proxy 74, PDS module 88, UP Servlet 54, LBAC module 46, a sendmail module 90, an secure mail client (SMC) server 92, a secure sockets layer (SSL) proxy 94, an aggregation engine 96, and event server 48. The SMC server 92 cooperates with corresponding SMC modules resident on certain corporate networks, for example, to convey email data between the mobile office platform 24 and source mailboxes. The database machine 84 may include an aggregation application programming interface (API) 100 as a SOAP Daemon, an administration console 102, an aggregation database 104, the AggCron module 56, an SMC directory server 106, and a send mail module 91.

[0033] The various components of the Web client engine 22 may be configured to run on different machines or servers. The component binaries and configuration files may either be placed in a directory on the network or placed on a local disk that can be accessed to allow the appropriate components to run from each machine. In accordance with one exemplary implementation, deployment may include one supervisor, two workers, and one port agent for supporting 30,000

external source mailboxes, although other configurations may also be used. Actual production deployment may depend on the results of load, performance and stress testing, as will be appreciated by those skilled in the art.

[0034] For the mobile office platform **24** direct access components, modules and various functions, machines are typically installed in two configurations, namely engine machines (FIG. 4) and database machines (FIG. 5). While these machines may have all of the above-described components installed on them, not all of these components need be active in all applications (e.g., aggregation may be used with systems that do not support push technology, etc.). Once again, actual production deployment may depend on the results of load, performance and stress testing.

[0035] The mobile office platform **24** architecture in one known technique advantageously uses a set of device/language-specific eXtensible Stylesheet Language (XSL) files, which transform application data into presentation information. In one non-limiting example, a build process takes a non-localized XSL and generates a localized XSL for each supported language. When the XSL is used, it is "compiled" in memory and cached for repeated use. The purpose of pre-localizing and caching the templates is to reduce the CPU cycles required to generate a presentation page.

[0036] Branding may also be performed. Initially, a localized XSL may build a WAP application to access aggregated email accounts. A WAP proxy application may be localizable and support multiple WAP devices. For each logical page of an application, a device-specific XSL may be created, which may be localized for each language/country supported. This rendering scheme may

support not only WAP devices, but also SMTP, HTML and POP proxies, for example. In branding, each page of a given application may be customized for each different brand.

[0037] The branding of a page may be accomplished through XSL imports, including the use of a Java application programming interface (API) for XML processing (JAXP) feature to resolve the imports dynamically. This need not require that each combined page/brand template be compiled and cached. By way of example, in a sample template directory, first and second pages for a single language/country may be combined with branded counterparts to generate a plurality of distinct template combinations. It is also possible to profile memory requirements of an application by loading templates for a single language, device/application and brand. An HTML device may include a set of templates that are large compared to other devices.

[0038] In one known technique, the mobile office platform **24** advantageously builds processes and takes non-localized files and language-specific property files and combines them to make each non-localized XSL into an XSL for each supported language. A separate XSL for each language need not be used, and the language factor may be removed from the memory usage equation. A JAXP API may be used to extend XSL with Java classes. The extensions may take various forms, for example, including extension elements and extension functions. A template may be transformed by creating and initializing an extension object with a locale and passing an object to a transformer. The system can remove multiple imports and use less memory. HTML templates can use template importing to enable template

reuse, much like Java classes, and reuse other Java classes through a mechanism like derivation or importing.

[0039] In the direct access system **20**, users receive email on their mobile wireless communications devices **25** from multiple external accounts, and when replying to a received message, the reply-to and sent-from address integrity is preserved. For example, for a user that has an integrated Yahoo! account (user@yahoo.com) and a POP3 account (user@pop3.com), if they receive an email at user@yahoo.com, their replies generated from the device **25** will appear to come from user@yahoo.com. Similarly, if a user receives an email at user@pop3.com, their replies will appear to come from user@pop3.com.

[0040] Selection of the "sent from" address is also available to a user that composes new messages. The user will have the ability to select the "sent from" address when composing a new message. Depending on the source mailbox type and protocol, the message may also be sent through the source mail service. This functionality can be supported by sending a configuration for each source mailbox, for example, as a non-limiting example, a service book for each source mailbox **51**, **53** to the mobile wireless communications device **25**.

[0041] As noted above, a service book is a class that may include all service records currently defined. This class may be used to maintain a collection of information about the device, such as connection information. The service book may be used to manage HTTP connections and mail (CMIME) information such as account and hierachy. At mobile wireless communications devices **25**, a delete service book request may be sent

when a source mailbox **51, 53** is removed from the account. The service book may also be resent to the device **25** with a viewable name that gives the user some indication that the selection is no longer valid.

[0042] A sent items folder may also be "synchronized." Any device-originated sent messages may be propagated to a source account and stored in a sent mail folder, for example. Also, messages deleted on the device **25** may correspondingly be deleted from the source mailbox **51, 53**. Another example is that device-originated marking of a message as read or unread on the device **25** may similarly be propagated to the source mailbox **51, 53**. While the foregoing features are described as source-dependent and synchronizing one-way, in some embodiments certain synchronization features may in addition, or instead, propagate from the source mailbox/account to the handheld device, as will be appreciated by those skilled in the art.

[0043] When available, the mail service provider or corporate mail server may be used for submission of outgoing messages. While this may not be possible for all mail service providers or servers, it is preferably used when available as it may provide several advantages. For example, subscribers to AOL will get the benefit of AOL-specific features like parental controls. Furthermore, AOL and Yahoo users, as non-limiting examples, will see messages in their sent items folder, and messages routed in this manner may be more compliant with new spam policies such as Sender Policy Framework (SPF) and Sender Id. In addition, messages sent via corporate mail servers **52** will have proper name resolution both at the global address list level and the personal level. It should be understood, however, that the use of the mail service

provider **50** to deliver mail may be dependant on partner agreements and/or protocol, depending upon the given implementation.

[0044] The architecture described above also advantageously allows for features such as on-demand retrieval of message bodies and attachments and multiple folder support. Moreover, a "this-is-spam" button or indicator may be used allowing company labels and other service provider-specific features when supported by an underlying protocol, as will be appreciated by those skilled in the art.

[0045] One particular advantage of the direct access system **20** is that a user need not configure an account before integrating additional accounts. However, a standalone email address may be used, and this address advantageously need not be tied to a mailbox size which the subscriber is required to manage. For example, the email account may be managed by an administrator, and any mail could be purged from the system after a pre-determined period of time (i.e., time-based auto-aging with no mailbox limit for all users).

[0046] Additionally, all aspects of any integrated email account creation, settings and options may advantageously be available to the user from their mobile wireless communications device **25**. Thus, users need not visit an HTML site and change a setting, create a filter, or perform similar functions, for example. Of course, an HTML site may optionally be used.

[0047] As a system Internet email service with the direct access system **20** grows, ongoing emphasis may advantageously be placed on the administrative site to provide additional information to carrier administrators, support teams, and similar functions.

However, in some instances a mail connector may be installed on a personal computer, and this functionality may not always be available from the mobile wireless communications device.

[0048] The Web client engine **22** may advantageously support different features including message to handheld (MTH), message from handheld (MFH), forward/reply a message, request to view more for a large message (e.g., larger than 2K), request viewing message attachment, and over the air folder management (OTA FM). These functions are explained below.

[0049] For an MTH function, each email account integrated for a user is linked with the user device through a Web client service book. For each new message that arrives in the Web client user mailbox, a notification that contains the new message information will typically be sent to a Web client engine supervisor component (FIG. 3), which in turn will assign the job to an available worker with the least load in the system. The chosen worker **32** will validate the user information and retrieve the new message from the user source mailbox and deliver it to the user device.

[0050] In an MFH function, MFH messages associated with a Web client service book are processed by the Web client engine **22** and delivered to the Internet **49** by the worker **32** via the simple mail transfer protocol (SMTP) or native outbox. If a user turns on the option to save the sent message to the sent items folder, the direct access proxy will save a copy of the sent message to this folder.

[0051] In a Forward/Reply/More function, the user can forward or reply an MTH or MFH message from the mobile wireless communications device **25** as long as the

original message still existed in the direct access proxy cache or in user mailbox. For MTH, the worker **32** may send the first 2K, for example, or the whole message (whatever is less) to the user device. If the message is larger than 2K, the user can request MORE to view the next 2K of the message. In this case, the worker **32** will process the More request by retrieving the original message from the user source mailbox, and send back the 2K that the device requests. Of course, in some embodiments more than 2K of message text (or the entire message) may be sent.

[0052] In an attachment-viewing function, a user can view a message attachment of a popular document format (e.g., MS Word, MS Power Point, MS Excel, Word Perfect, PDF, text, etc.) or image format (GIF, JPEG, etc). Upon receiving the attachment-viewing request, which is implemented in a form of the More request in this example, the worker **32** can fetch the original message from the user source mailbox via the direct access proxy, extract the requested attachment, process it and send result back to the user device. The processing requires that the original message has not been deleted from the user Web client mailbox.

[0053] In the save sent message to sent items folder function, if the user turns this option on, the worker **32** places a copy of each MFH message sent from the user device in the user sent items folder in the mailbox. In over the air folder management, the Web client OTAFM service maintains any messages and folders in the user mailbox synchronized with the user device over the air.

[0054] Whenever a message in the user source mailbox is Moved/Deleted, the associated message on the device may also be Moved/Deleted accordingly, and vice-versa. When a message is Moved/Deleted on the device, the

associated message in the user Web client mailbox may also be Moved/Deleted accordingly. Similarly, when a folder is Added/Removed/Renamed from the user Web client mailbox, the associated folder on the device may be Added/Removed/Renamed, and vice-versa.

[0055] The system **20** may advantageously support different subsets of various messaging features. For example, in the message to handheld function, the mobile office platform **24** may be responsible for connecting to the various source mailboxes **51**, **53** to detect new emails. For each new mail, a notification is sent to the Web client engine **22** and, based on this notification, the supervisor **34** chooses one of the workers **32** to process that email. The chosen worker will fetch additional account information and the contents of the mail message from the direct access proxy **40** and deliver it to the user device **25**.

[0056] In a message sent from handheld function, the MFH could be given to the direct access proxy **40** from the Web client worker **32**. In turn, the mobile office platform **24** delivers a message to the Internet **49** by sending through a native outbox or sending it via SMTP. It should be understood, however, that the native outbox, whenever possible, may provide a better user experience, especially when taking into account current anti-spam initiatives such as SPF and sender Id.

[0057] In a message deleted from handheld function, when a message is deleted from the device **25**, the Web client engine **22** notifies the mobile office platform **24** via the direct access proxy **40**. As such, the mobile office platform **24** can delete the same message on the source mailbox.

[0058] When handling More/Forward/Reply/Attachment viewing requests, the Web client worker **32** may request

an original mail from the direct access proxy **40**. It will then process the request and send the results to the mobile wireless communications device **25**. The architecture may additionally support on-demand retrieval of message parts and other upgrades, for example.

[0059] Upon the integration of a new source mailbox **51, 53**, the service book notification from the alert server **38** may be sent to the supervisor **34**, which assigns this notification to a worker **32** for sending out a service record to the device. Each source mailbox **51, 53** may be associated with a unique service record. In this way, each MFH message is linked with a source mailbox **51, 53** based on the service record on the device.

[0060] The system **20** may also poll the integrated external mailboxes periodically to check for new mail and to access any messages. The system **20** may further incorporate optimizations for polling bandwidth from an aggregation component allowing a quick poll. The system **20** can also advantageously support a large active user base and incorporate a rapidly growing user base.

[0061] The topology of load balancing can be based on the size of a component's queue and its throughput. These load statistics can be monitored by a mechanism in one example called the UDP Heartbeat, as described before. If a component is overloaded or has a large queue size, the component will have less chance to get an assigned job from other components. In contrast, a component will get more assigned jobs if it completes more jobs in the last few hours than other components. With this mechanism, the load could distribute over heterogeneous machine hardware, i.e., components

running on less power machines will be assigned fewer jobs than those on machines with more power hardware.

[0062] General load balancing for any mobile office platform components can be accomplished through the use of a load balancer module, for example, a BIG-IP module produced by F5 Networks of Seattle, Washington. BIG-IP can provide load balancing and intelligent layer 7 switching, and can handle traffic routing from the Internet to any customer interfacing components such as the WAP and HTML proxies. The use of a BIG-IP or similar module may provide the application with pooling capabilities, fault tolerance and session management, as will be appreciated by those skilled in the art.

[0063] Typically, access to a single source mailbox **51**, **53** can be from a single direct access proxy **40** over a persistent connection. Any requests on behalf of a particular user could persist to the same machine in the same direct access clustered partition. As certain components are system-wide and will be handling work for users across many partitions, these components can be designed to determine which direct access partition to communicate with on a request-by-request basis.

[0064] The load balancer and cache (LBAC) **46** may support this function. The LBAC **46** is a system-wide component that can perform two important functions. The first of these function is that it provides a mapping from the device PIN to a particular direct access proxy **40**, while caching the information in memory for both fast access and to save load on the central database. Secondly, as the direct access proxy **40** will be run in clustered partitions, the LBAC **46** may distribute the load across all direct access proxies within any partition.

[0065] The LBAC 46 can be formed of different components. For example, the code which performs the load balancing can be an extended version of a secure mail connector. The code can also perform lookups to the central database and cache the results (LBAC).

[0066] In one non-limiting example, when a worker requires that a direct access proxy 40 perform work, it provides the LBAC 46 with a device PIN. The LBAC 46 will discover which partition that PIN is associated with by looking in its cache, or retrieving the partition identifier from a central database (and caching the result). Once the partition is known, the LBAC 46 then consults its cache to see which direct access proxy in that partition has been designated to handle requests for that PIN. If no mapping exists, the LBAC requests the PDS to create a new association on the least loaded DA proxy 40 (again caching the result). Finally, the LBAC 46 responds to the worker 32 with the connection information for the proper direct access proxy to handle that particular request.

[0067] The secure mail connector may run in failover pairs, where one is an active master and the other is a secondary standby. Internal data structures may be replicated in real-time from the master to the standby. Multiple LBACs 46 can be run for scalability and fault tolerance, but typically would require an external connection balancing component, such as the BIG-IP component as explained before.

[0068] A receiving component in the Web client engine 22 saves the job that has been assigned to it from other components to a job store on the disk before processing. It can update the status of the job and remove the job from the job store when the job processing is completed. In case of component failure

or if the process is restarted, it can recover the jobs from the job store and, based on the current statuses of these jobs, continue processing these jobs to the next state, saving the time to reprocess them from the beginning.

[0069] Any recovery from the standpoint of MTH/MFH can be achieved through current polling behavior and on the Web client engine **22** recovery mechanisms. From within the mail office platform components, until a message has been successfully delivered to a Web client engine **22**, that message is not recorded in the partition database **60**. During the next polling interval, the system can again "discover" the message and attempt to notify the Web client engine **22**. For new mail events, if an event is lost, the system can pick up that message upon receiving the next event or during the next polling interval. For sources supporting notifications, this interval could be set at six hours, as one non-limiting example. For messages sent from the Web client engine **22**, and for messages that have been accepted by the Web client engine, recovery can be handled by different Web client engine components.

[0070] The Web client engine **22** may advantageously be horizontally and vertically scalable. Multiple supervisors **34** can be registered/configured with direct access proxies **40** to provide the distribution of the notification load and the availability of engine service. Multiple workers **32** and port agents **30** can run on the same machine or across multiple machines to distribute load and achieve redundancy. As the number of users grows, new components can be added to the system to achieve high horizontal scalability.

[0071] It is possible for a new component to be added to or removed from the system automatically

without down time. Traffic can automatically be delegated to a new component and diverted away from failed components. Each component within the mobile office platform **24** can be deployed multiple times to achieve horizontal scalability. To achieve vertical scalability, each mobile office platform **24** component can be a multi-threaded process with a configurable number of threads to scale under heavy load. Pools of connections can be used to reduce the overhead of maintaining too many open connections.

[0072] FIG. 6 is a high-level flowchart showing an example of a method that can be used for authenticating a user to obtain electronic mail (email) using an authentication token. A system can be used with the method shown in FIG. 1 and include functional components in addition to those shown in FIG. 1. Such components of the mobile office platform **24** can be operative as an email server and the cache **44**, DA proxy **40**, proxy API, database **60** and event server **48**, as well as other components, can be used for the method.

[0073] In this system, email can be provided by email service providers and the mobile office platform accesses mail on behalf of the user from these email service providers. The mobile office platform authenticates a user with a typical email server or other third-party server using the user's user identification, for example, the log-in ID, or email address and password. If an authentication token is required to access the user's email, the mobile office platform receives the authentication token from the server upon authentication. The mobile office platform attempts to access the user's email from the email server using this authentication token. If this is successful, and if it is possible for the mobile office

platform to always access the user's email using the authentication token, the mobile office platform would delete the user identification and password from the database and store the authentication token. It is also possible for the system to never store a user identification and password in the database. For example, upon receiving the configuration data from a user, the steps above can be attempted and the authentication token directly stored, discarding the user identification and password. From this point, access to the email server is done using the authentication token for actions such as downloading email and marking messages as read.

[0074] As shown in the flowchart of FIG. 6, the mobile office platform accesses the email server provided by the email service provider, for example, by using a user identification (ID) such as an email address or log-in ID and password (block 100). A determination is made if an authentication token is required to access the electronic mailbox of the user (block 102). If not, then the user ID and password can be retained (block 104). If the authentication token is required, then the mobile office platform receives an authentication token from the email server (block 106), which in some instances could be separate from the email service provider. An attempt is made to access the user electronic mailbox using the authentication token (block 108). A determination is made of success (block 110), and if not, then a new authentication token is required (block 112). An attempt is made again using the new authentication token. If the attempt was successful, the authentication token is stored for later use by the

user when accessing their electronic mailbox (block 114).

[0075] The mobile office platform **24** supports an email server function and includes the Direct Access proxy **40** for accessing and retrieving user emails from the electronic mailbox of the user. The database **60** shown at the mobile office platform **24** can store the authentication token for subsequent use, or a different database can be operative with the various illustrated components, modules and functions shown in FIGS. 1-5 for storing authentication tokens. The database could be on a different platform from the mobile office platform **24**.

[0076] The mobile office platform components are operative for initially accessing the electronic mailbox with a user identification and password. The mobile office platform can discard the user identification and password if the authentication token can access the electronic mailbox of the user. The mobile office platform can also be operative for retaining the user identification and password if an authentication token is not required for accessing the electronic mailbox of the user. The computer-readable medium having computer-executable instructions for executing the above-described functions can be included on the various servers or other components as described above.

[0077] The authentication token can operate by challenge/response or be a time-based code sequence, and in some instances, a separate password provided by the email service provider to authenticate a user. It is also possible to be a piece of information or code similar to a cookie to contain information, such as log-in or registration information, to access the

electronic mailbox of a user. Other types of tokens can be used as suggested by those skilled in the art.

[0078] In a challenge/response technique, the email server could create a "challenge" that is typically a random number sent to the third-party server. The mobile office platform could use its password or secret key to encrypt the challenge via an encryption algorithm or a one-way hash function and send the result back to the network as a response. An authentication system could perform the same cryptographic process on the challenge and compare its result to the response from the client. If there is a match, the authentication system can verify that the user has the correct password. Different types of authentication tokens can be used. The authentication system could reside on a different server than the email server.

[0079] An example of a handheld mobile wireless communications device **1000** that may be used is further described in the example below with reference to FIG. 7. The device **1000** illustratively includes a housing **1200**, a keypad **1400** and an output device **1600**. The output device shown is a display **1600**, which is preferably a full graphic LCD. Other types of output devices may alternatively be utilized. A processing device **1800** is contained within the housing **1200** and is coupled between the keypad **1400** and the display **1600**. The processing device **1800** controls the operation of the display **1600**, as well as the overall operation of the mobile device **1000**, in response to actuation of keys on the keypad **1400** by the user.

[0080] The housing **1200** may be elongated vertically, or may take on other sizes and shapes (including clamshell housing structures). The keypad may include a

mode selection key, or other hardware or software for switching between text entry and telephony entry.

[0081] In addition to the processing device **1800**, other parts of the mobile device **1000** are shown schematically in FIG. 7. These include a communications subsystem **1001**; a short-range communications subsystem **1020**; the keypad **1400** and the display **1600**, along with other input/output devices **1060**, **1080**, **1100** and **1120**; as well as memory devices **1160**, **1180** and various other device subsystems **1201**. The mobile device **1000** is preferably a two-way RF communications device having voice and data communications capabilities. In addition, the mobile device **1000** preferably has the capability to communicate with other computer systems via the Internet.

[0082] Operating system software executed by the processing device **1800** is preferably stored in a persistent store, such as the flash memory **1160**, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the random access memory (RAM) **1180**. Communications signals received by the mobile device may also be stored in the RAM **1180**.

[0083] The processing device **1800**, in addition to its operating system functions, enables execution of software applications **1300A-1300N** on the device **1000**. A predetermined set of applications that control basic device operations, such as data and voice communications **1300A** and **1300B**, may be installed on the device **1000** during manufacture. In addition, a personal information manager (PIM) application may be installed

during manufacture. The PIM is preferably capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application is also preferably capable of sending and receiving data items via a wireless network **1401**. Preferably, the PIM data items are seamlessly integrated, synchronized and updated via the wireless network **1401** with the device user's corresponding data items stored or associated with a host computer system.

[0084] Communication functions, including data and voice communications, are performed through the communications subsystem **1001**, and possibly through the short-range communications subsystem. The communications subsystem **1001** includes a receiver **1500**, a transmitter **1520**, and one or more antennas **1540** and **1560**. In addition, the communications subsystem **1001** also includes a processing module, such as a digital signal processor (DSP) **1580**, and local oscillators (LOs) **1601**. The specific design and implementation of the communications subsystem **1001** is dependent upon the communications network in which the mobile device **1000** is intended to operate. For example, a mobile device **1000** may include a communications subsystem **1001** designed to operate with the Mobitex™, Data TAC™ or General Packet Radio Service (GPRS) mobile data communications networks, and also designed to operate with any of a variety of voice communications networks, such as AMPS, TDMA, CDMA, PCS, GSM, etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device **1000**.

[0085] Network access requirements vary depending upon the type of communication system. For example, in the Mobitex and DataTAC networks, mobile devices are

registered on the network using a unique personal identification number or PIN associated with each device. In GPRS networks, however, network access is associated with a subscriber or user of a device. A GPRS device therefore requires a subscriber identity module, commonly referred to as a SIM card, in order to operate on a GPRS network.

[0086] When required network registration or activation procedures have been completed, the mobile device **1000** may send and receive communications signals over the communication network **1401**. Signals received from the communications network **1401** by the antenna **1540** are routed to the receiver **1500**, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP **1580** to perform more complex communications functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network **1401** are processed (e.g. modulated and encoded) by the DSP **1580** and are then provided to the transmitter **1520** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network **1401** (or networks) via the antenna **1560**.

[0087] In addition to processing communications signals, the DSP **1580** provides for control of the receiver **1500** and the transmitter **1520**. For example, gains applied to communications signals in the receiver **1500** and transmitter **1520** may be adaptively controlled through automatic gain control algorithms implemented in the DSP **1580**.

[0088] In a data communications mode, a received signal, such as a text message or web page download, is processed by the communications subsystem **1001** and is input to the processing device **1800**. The received signal is then further processed by the processing device **1800** for an output to the display **1600**, or alternatively to some other auxiliary I/O device **1060**. A device user may also compose data items, such as e-mail messages, using the keypad **1400** and/or some other auxiliary I/O device **1060**, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communications network **1401** via the communications subsystem **1001**.

[0089] In a voice communications mode, overall operation of the device is substantially similar to the data communications mode, except that received signals are output to a speaker **1100**, and signals for transmission are generated by a microphone **1120**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the device **1000**. In addition, the display **1600** may also be utilized in voice communications mode, for example to display the identity of a calling party, the duration of a voice call, or other voice call related information.

[0090] The short-range communications subsystem enables communication between the mobile device **1000** and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, or a Bluetooth™ communications module to provide for

communication with similarly-enabled systems and devices.

[0091] Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.

CLAIMS:

1. A system for authenticating a user for accessing an electronic mailbox of the user from a remote device and obtaining electronic mail (email), which comprises:

an email server provided by an email service provider and having at least one electronic mailbox of the user; and

a mobile office platform operative to poll the electronic mailbox of the user, retrieves email and pushes the email to the user, wherein the mobile office platform is operative for authenticating access to the electronic mailbox of the email server provided by the email service provider by:

determining if an authentication token is required to access the electronic mailbox of the user,

generating an authentication token from the email server if an authentication token is required,

attempting access to the electronic mailbox of the user using the authentication token,

storing the authentication token for subsequent use by the user to access the electronic mailbox of the user if access to the electronic mailbox using the authentication token has been successful, and

receiving a new authentication token from the email server if access to the electronic mailbox using the authentication token was not successful.

2. The system according to claim 1, which further comprises a mobile wireless communications device that receives user email from the mobile office platform.

3. The system according to claim 1, wherein the mobile office platform includes a computer readable medium on which is stored a database for storing the authentication token for subsequent use when the user attempts access through the mobile office platform.

4. The system according to claim 1, wherein said mobile office platform includes an email client server, and further including a direct access proxy for accessing and retrieving user emails from the electronic mailbox of the user.
5. The system according to claim 4, wherein said mobile office platform includes a computer readable medium on which is stored a database for storing the authentication token for subsequent use when the user attempts access to the electronic mailbox of the user through the mobile office platform.
6. The system according to claim 1, wherein said mobile office platform is operative for initially accessing the electronic mailbox with a user identification and email address.
7. The system according to claim 6, wherein said mobile office platform is operative for discarding the user identification and email address if the authentication token can access the electronic mailbox of the user.
8. The system according to claim 6, wherein said mobile office platform is operative for retaining the user identification and email address if an authentication token is not required for accessing the electronic mailbox of the user.
9. A method of authenticating a user for accessing an electronic mailbox of the user from a remote device and obtaining electronic mail (email), which comprises:
 - providing a mobile office platform that polls the electronic mailbox of a user located on an email server provided by an email service provider and pushes the email to the user, wherein the mobile office platform is operative for authenticating access to the electronic mailbox by:
 - determining if an authentication token is required to access the electronic mailbox of the user,
 - generating an authentication token from the email server if an authentication token is required,
 - attempting access to the electronic mailbox of the user using the authentication token,

storing the authentication token for subsequent use by the user if access to the electronic mailbox using the token has been successful, and

receiving a new authentication token from the email server if access to the electronic mailbox using the authentication token was not successful.

10. The method according to claim 9, which further comprises accessing the electronic mailbox from a direct access proxy that retrieves and delivers any user email to the remote device of the user.

11. The method according to claim 9, which further comprises receiving user email on a mobile wireless communications device.

12. The method according to claim 9, which further comprises initially accessing the email server with a user identification and user email address.

13. The method according to claim 12, which further comprises discarding the user identification and email address if the electronic mailbox of the user is accessible with the authentication token.

14. The method according to claim 12, which further comprises retaining the user identification and email address if the electronic mailbox of the user is accessible without an authentication token.

15. The method according to claim 9, which further comprises storing the authentication token on a database for subsequent use when the user attempts access through a third-party email server.

16. A computer-readable medium having computer-executable instructions for executing functions comprising:

polling an electronic mailbox of a user at an electronic mail server that includes the electronic mailbox of a user when a user identification and password is entered such that electronic mail is pushed to a user after retrieving the electronic mail, and authenticating

access to the electronic mailbox of the user by:

determining if an authentication token is required to access the electronic mailbox of the user,

generating an authentication token from the email server if an authentication token is required,

attempting access to the electronic mailbox of the user using the authentication token,

storing the authentication token for subsequent use by the user to access their electronic mailbox if access to the electronic mailbox using the authentication token has been successful, and

receiving a new authentication token from the email server if access to the electronic mailbox using the authentication token was not successful.

17. The computer-readable medium according to claim 16, wherein the computer-executable instructions are operative for storing the authentication token on a database for subsequent use when the user attempts access.

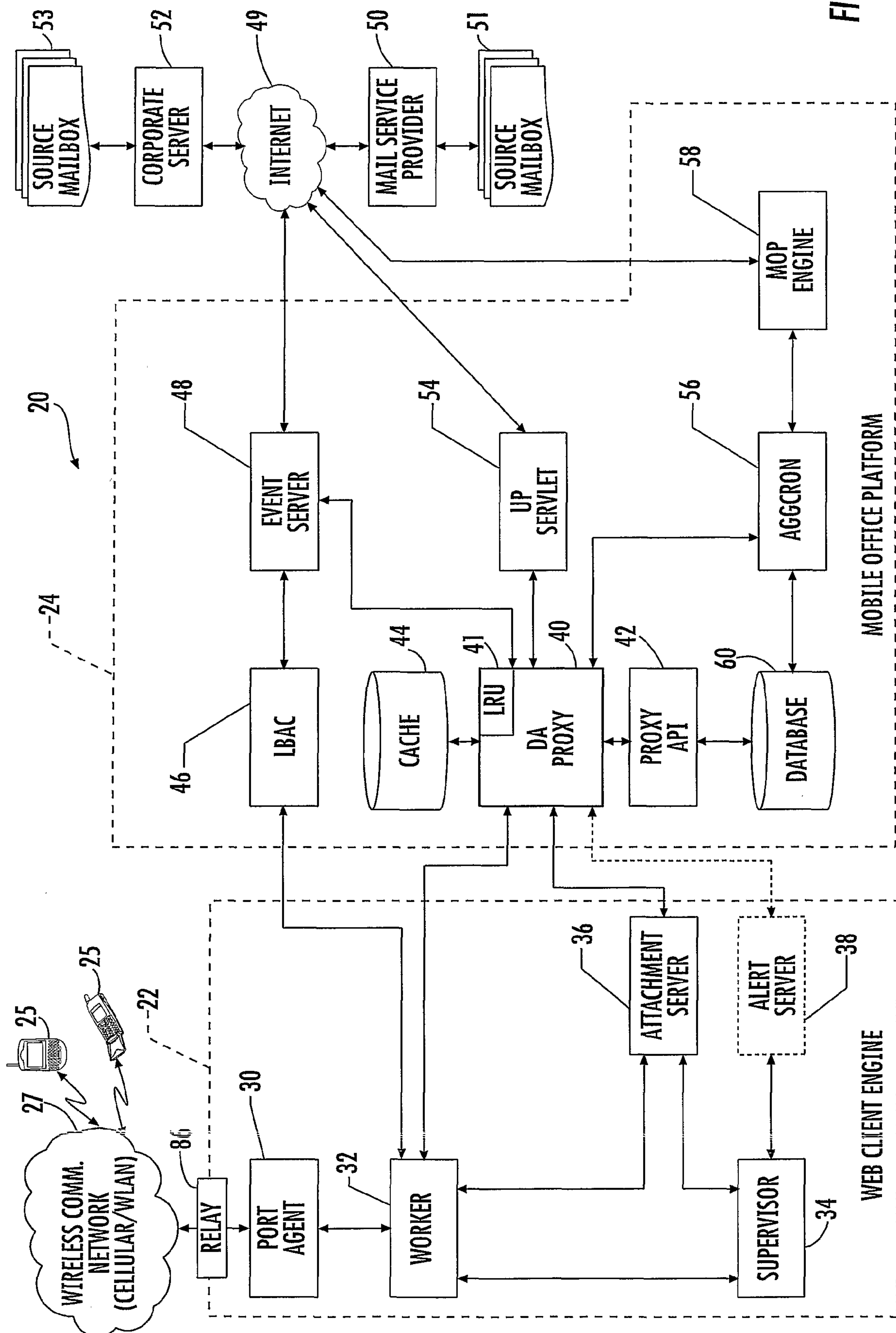
18. The computer-readable medium according to claim 16, wherein the computer-executable instructions are operative for delivering email messages to a mobile wireless communications device.

19. The computer-readable medium according to claim 16, wherein the computer-executable instructions are operative for accessing the email server with a user identification and email address.

20. The computer-readable medium according to claim 19, wherein the computer-executable instructions are operative for discarding the user identification and email address if the authentication token can access the electronic mailbox.

21. The computer-readable medium according to claim 19, wherein the computer-executable instructions are operative for retaining the user identification and email address if an authentication token is not required for accessing the electronic mailbox of the user.

FIG. 1



2/7

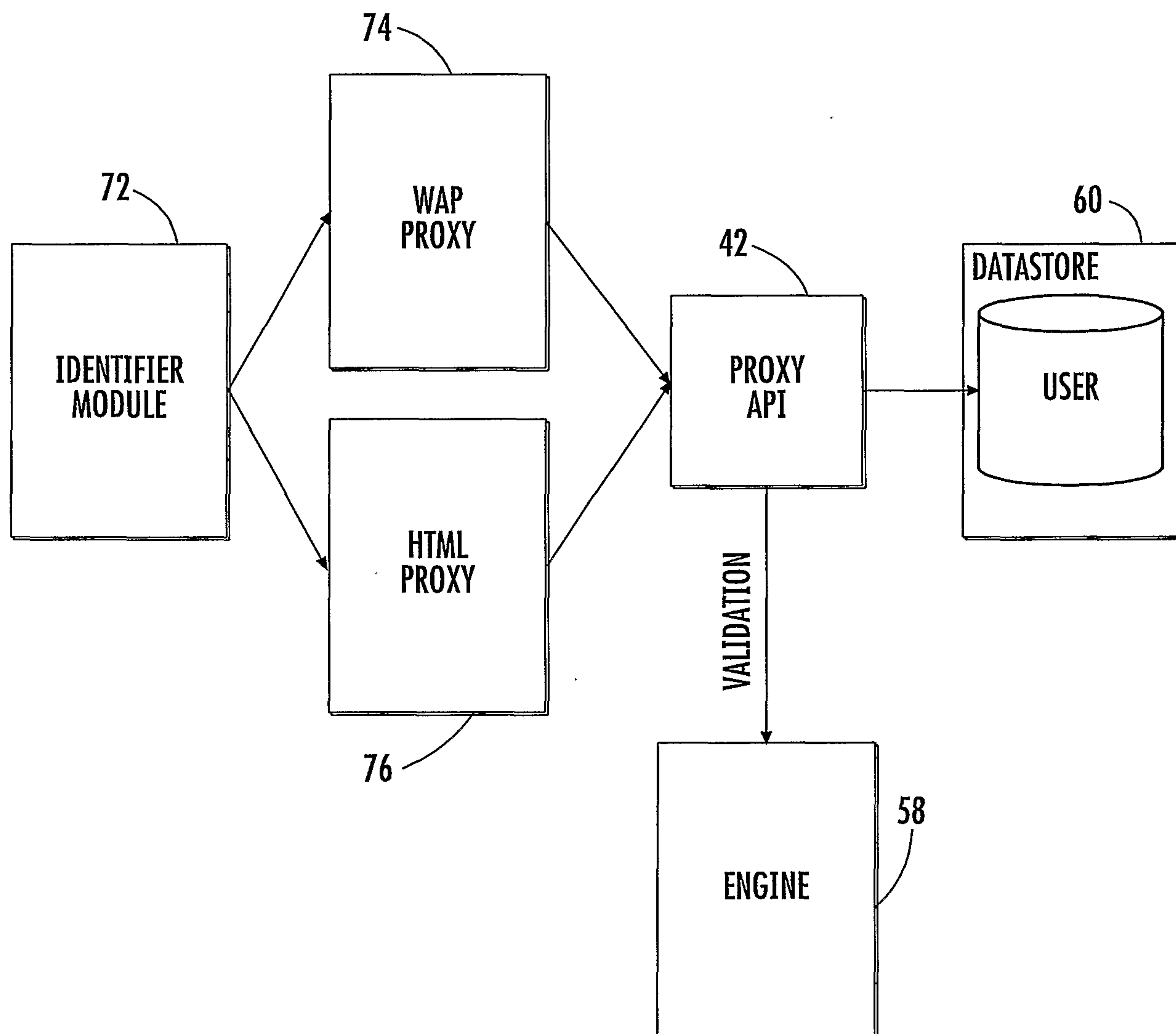


FIG. 2

3/7

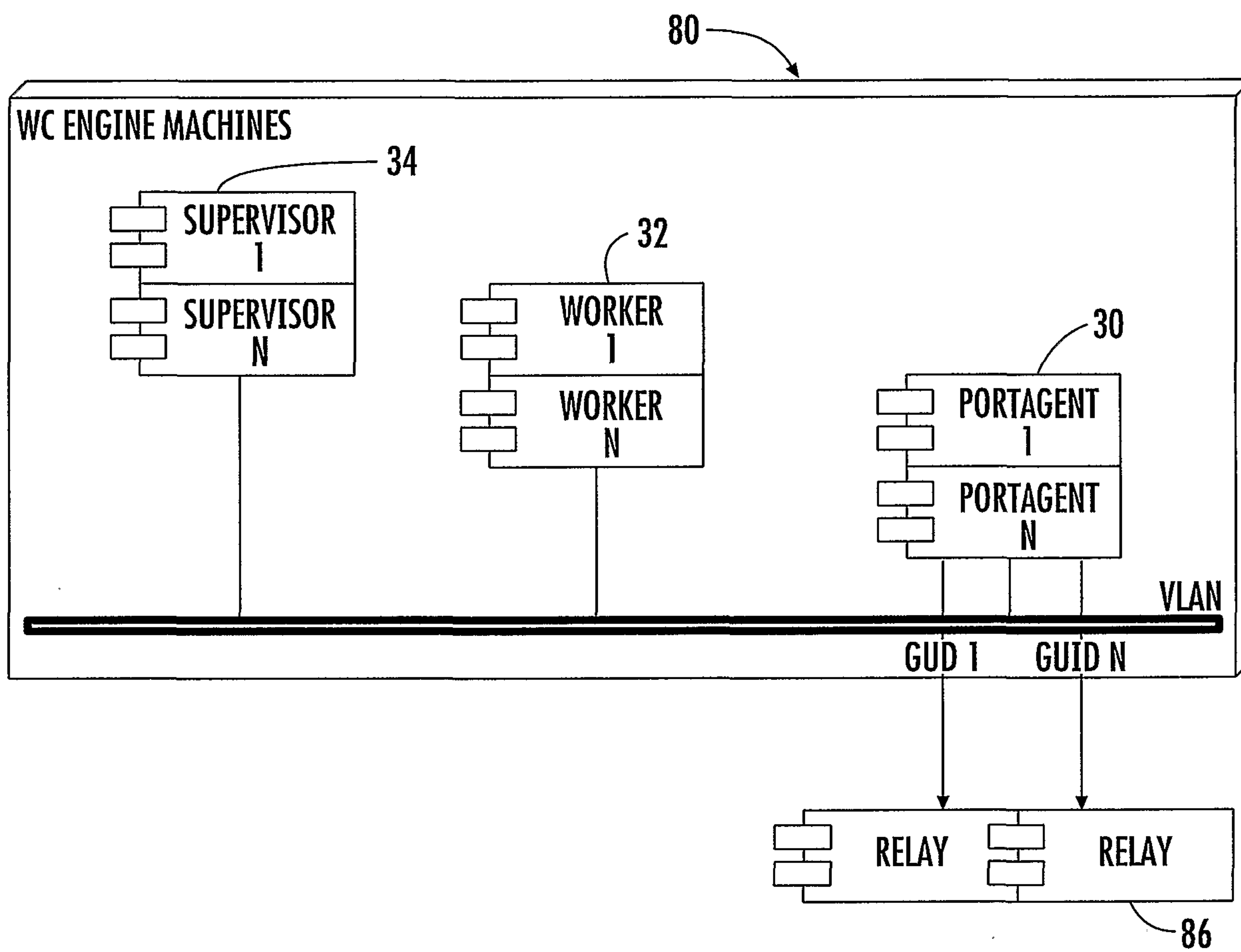


FIG. 3

4/7

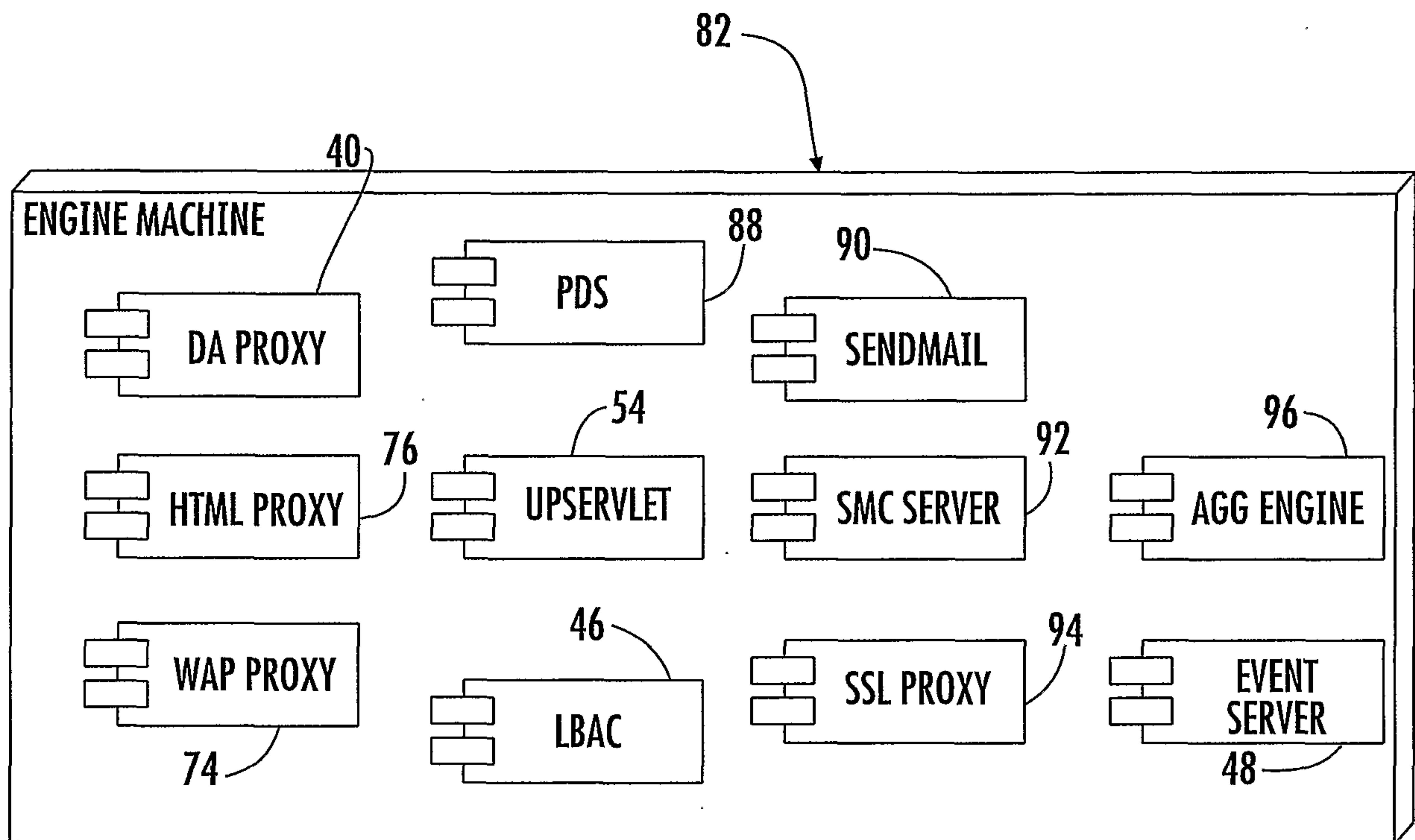


FIG. 4

5/7

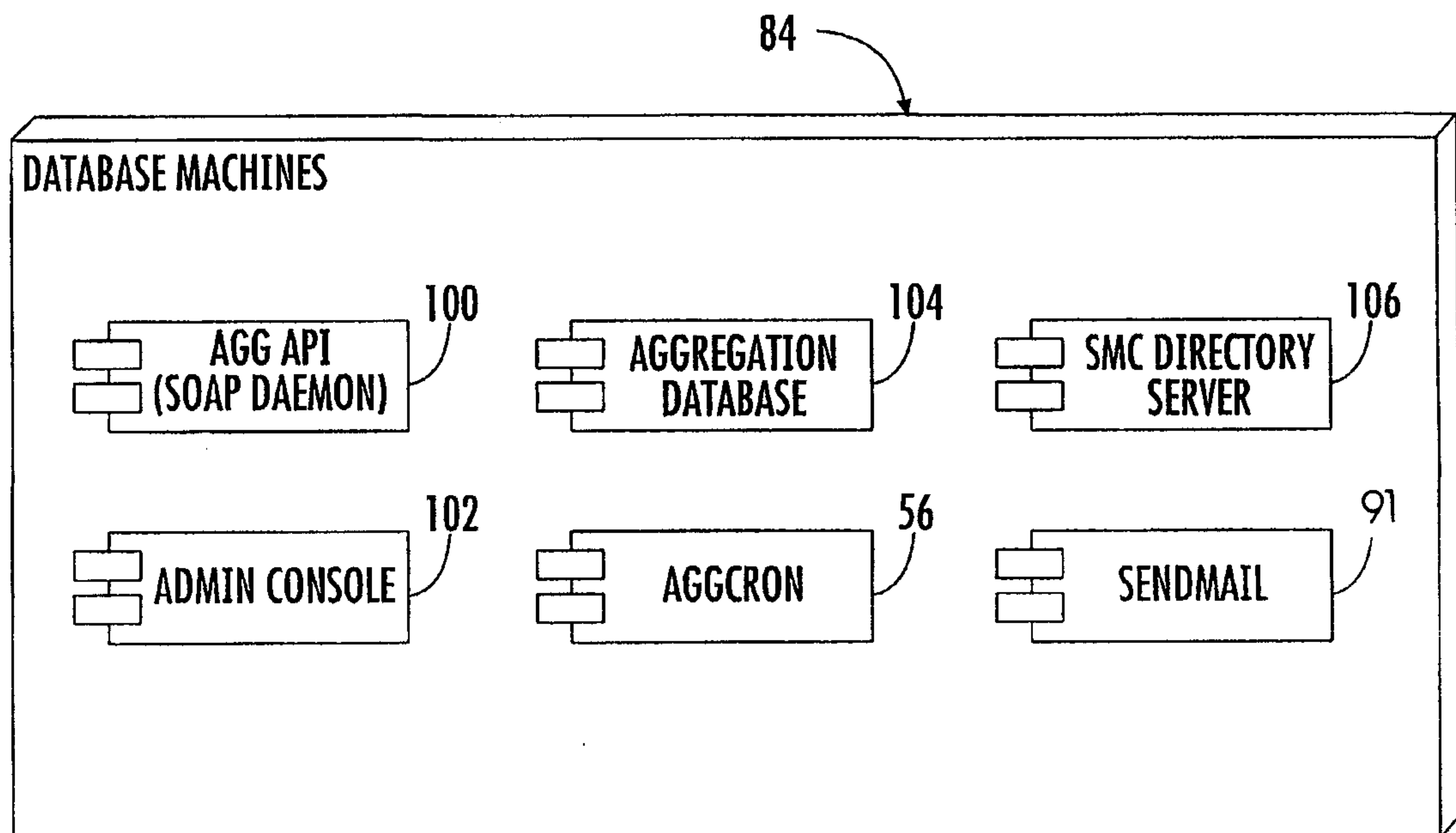


FIG. 5

6/7

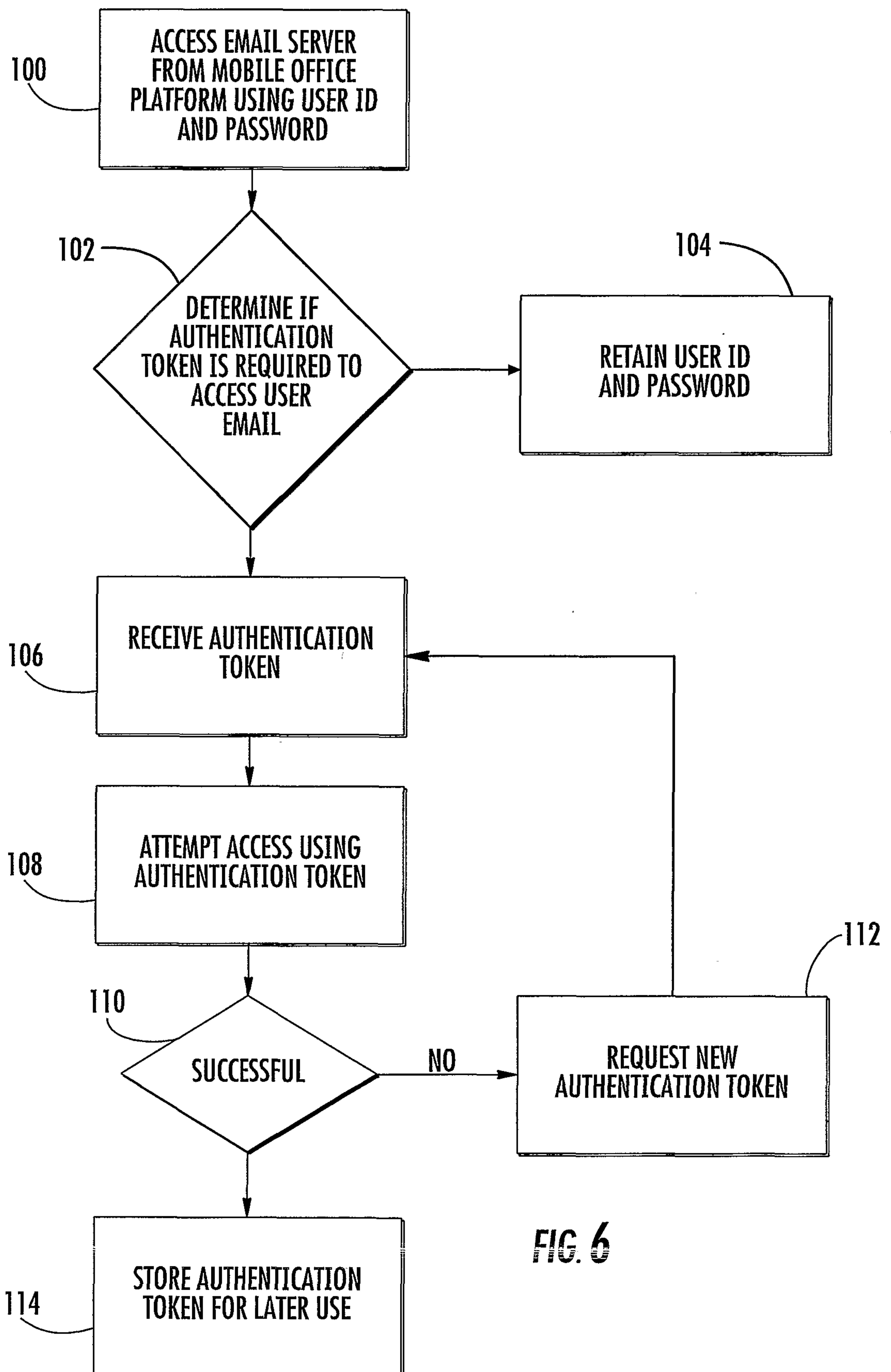


FIG. 6

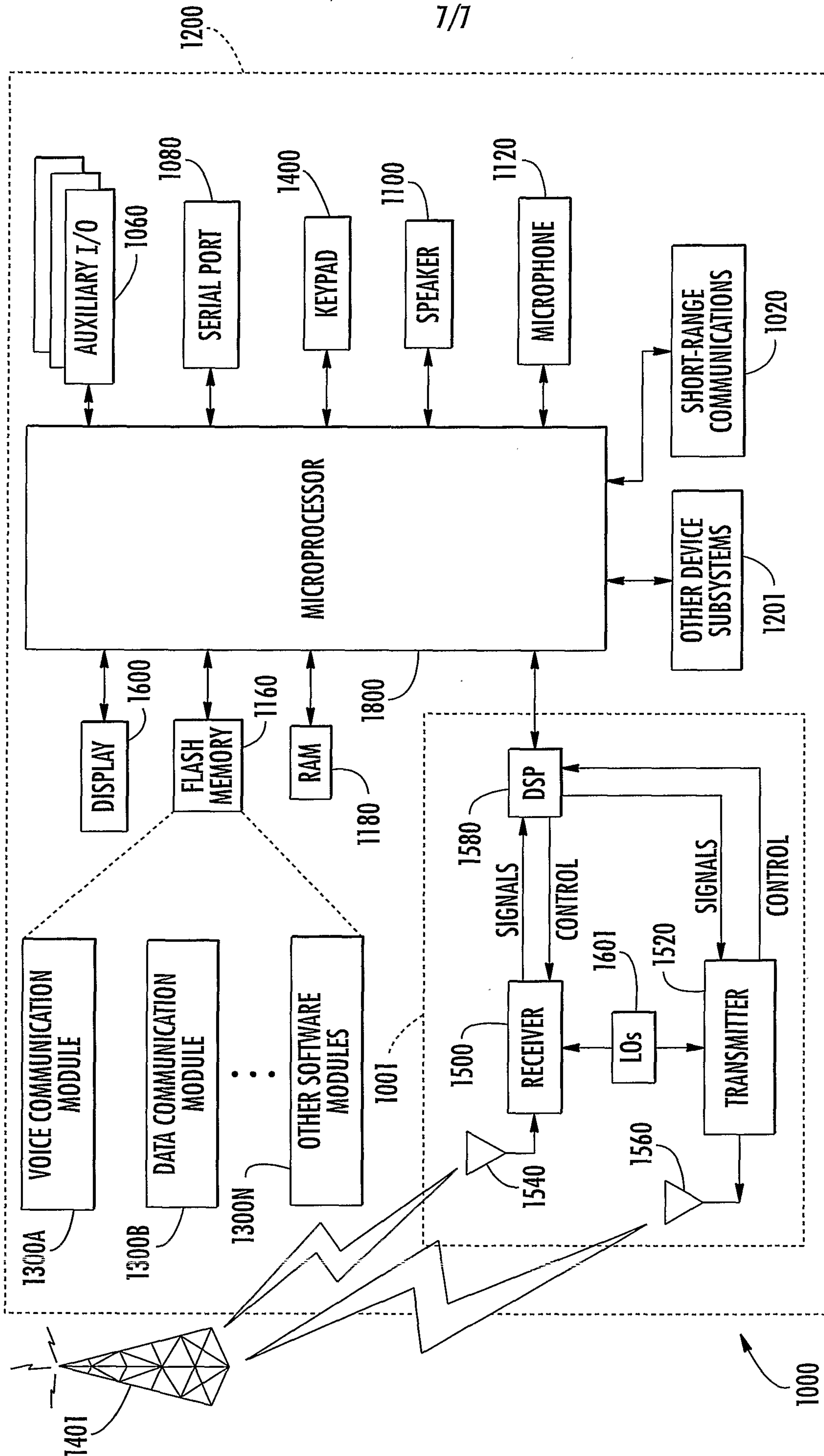


FIG. 7

