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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/29757 A1

(51) International Patent Classification⁷: G06K 9/00, G06F 11/00

(21) International Application Number: PCT/US00/23781

(22) International Filing Date: 29 August 2000 (29.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/422,280 20 October 1999 (20.10.1999) US

(71) Applicant: YODLEE.COM, INC. [US/US]; 3600 Bridge Park Way 2nd Floor, Redwood Shores, CA 94065 (US).

(72) Inventors: DASWANI, Neil; 18 Ashbrook Drive, Edison, NJ 00820 (US). INALA, Suman, Kumar; 3707 Poinciana Drive, Apt. 154, Santa Clara, CA 95051 (US). SATYAVOLU, Ramakrishna; 3707 Poincianna Drive, Apt. 154, Santa Clara, CA 95051 (US). LEE, Ji; 3480 Grenada Avenue, Apt. 254, Santa Clara, CA 95051 (US). IDEMA, Matthew; 3825 Scott Street, Apt. 303, San Francisco, CA 94123 (US).

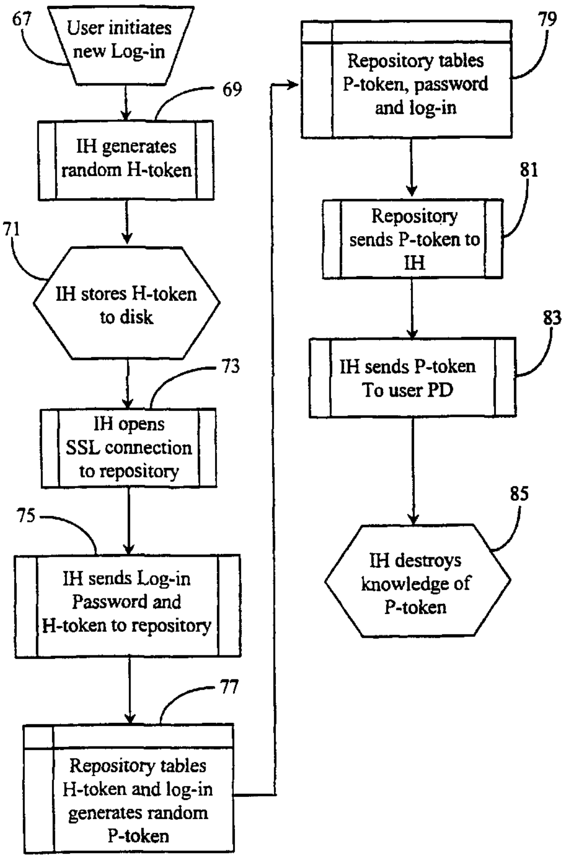
(74) Agent: BOYS, Donald, R.; P.O. Box 187, Aromas, CA 95004 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PROVIDING SECURE AUTHENTICATION OF PORTABLE DEVICES THROUGH INTERNET HOST SERVERS


67
User initiates new Log-in
69
IH generates random H-token
71
IH stores H-token to disk
73
IH opens SSL connection to repository
75
IH sends Log-in Password and H-token to repository
77
Repository tables H-token and log-in generates random P-token
79
Repository tables P-token, password and log-in
81
Repository sends P-token to IH
83
IH sends P-token To user PD
85
IH destroys knowledge of P-token

(57) Abstract: A system for instant log-in (67) to network servers and services from portable devices through computer-station Internet hosts has first software executing on the computer station, including a location code (H-token) (69) generator and a storage location reserved for the H-token (69), second software executing on the network server, including a password code (P-token) (79) generator, and one or more tables relating P-tokens (79), H-tokens (69), and subscriber's user names and passwords, third software executing on the PD (83), and a storage location on the PD (83) reserved for a P-token (79) different than the user's password. Upon a log-in (67) request signal to the IH (85) from the PD (83), the IH (85) opens a communication link to the network server, requests the P-token (79) from the PD (83), and, receiving the P-token (79), furnishes both the P-token (79) and the IH-stored (71) H-token (69), if any, to the network server, and the network server, only upon finding a match between P-token (79), H-token (69), and a valid subscriber, validates log-in (67) without requesting user name and password. Methods are provided for generating new P-tokens (79) by enabled servers, sending the new P-tokens (79) to enabled PDs (83), and associating the new tokens with users and location codes, to validate new PDs (83) to the system, and also for generating new H-tokens (69), validating new Internet Hosts to the system.

WO 01/29757 A1

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *With international search report.*

Method and Apparatus for Providing Secure Authentication of Portable Devices Through Internet Host Servers

by inventor(s)

Neil Daswani, Matthew Idema, Sam Inala, Ji Lee, Ramakrishna Satyavolu

Field of the Invention

The present invention is in the field of secure network protocols related to transferring data across a data network to a receiving device and pertains more particularly to methods and apparatus for authenticating various portable devices such as personal digital assistants (PDAs) and the like for operation on a secure network link.

Cross-Reference to Related Documents

The present invention is related in some aspects to a patent application entitled ***"Method and Apparatus for Restructuring of Personalized Data for Transmission from a Data Network to Connected and Portable Network Appliances"***, S/N 09/398,320, which is related also to U.S. patent application S/N 09/323,598 filed on 6/1/1999 and entitled ***"Method and Apparatus for Obtaining and Presenting WEB Summaries to Users"***, which is a continuation in part (CIP) of patent application S/N 09/208,740 entitled ***"Method and Apparatus for Providing and Maintaining a User-Interactive Portal System Accessible via Internet or other Switched-Packet-Network"*** filed on 12/08/98, disclosures of which are incorporated herein in their entirety by reference.

Background of the Invention

Portable communication devices capable of linking to a data network such as the Internet are now being provided with more memory capabilities than has been usual in the past. This development has allowed users to store much more information on their portable devices than was previously possible. For example, a personal digital assistant (PDA) such as 3-Com's Palm Pilot™ now has up to 2 MB of memory. Such a PDA can store approximately 6,000 addresses, 5 years worth of scheduled appointments, and up to 200 e-mail messages.

In addition to the capability of storing more information on such as a PDA, users typically have much personal information stored in "back-end" database servers located anywhere on a data network such as the Internet. Companies such as Hotmail™ and Yahoo™ use these back-end servers to store e-mail and other message information for users.

Generally, a user wishing to access his or her e-mail account or other information account from a portable internet-capable device such as a PDA must have the device authenticated to the server storing the desired information. Conduit software on a cooperating PC is responsible for synchronizing the data on the portable device with the data in such a back-end server. The synchronization process is generally known in the art and involves replacing data on the portable with new updated data from the server and vice versa. In the simple case of e-mail, the conduit application downloads any new mail from the server and uploads any new mail authored by a user operating the PDA. In addition to e-mail, conduit programs are available for synchronizing data from many different types of data sources.

A problem with the prior art methods and systems is that for a user to successfully access and receive data to a portable device (PD) he or she must provide an appropriate password and log-in information to access the site. In other words, the data source must know the portable device by configuration and password. A user having many different sites that are routinely accessed would have to remember many passwords, log-in codes, screen names, etc. in order to successfully interact with all the sites. Moreover, conduit software programs that accomplish data synchronization tasks between network data sources and portable devices are typically proprietary in nature and configured only for one host that oversees the data sources. Such a host is typically the provider of the conduit application, which resides on a user's PC.

In a system known to the inventor and referenced under the documents listed in the Cross-Reference to Related Documents section, data may be collected, aggregated, and restructured to be delivered to or held for access for a variety of wireless portable devices including PDAs, cellular phones, and even such as paging devices. The system uses a data center for interfacing various portable devices that operate on usually wireless communication networks, and PC interfaces for communicating with such as PDAs and like peripherals. The system is capable of aggregating data from many sources into a common data store with each updated data summary tagged to a user ID. However, this system requires that a user of a portable device supply device configuration and authentication information to the service for accessing summary data. Therefore, a password and log-in is still required, at least for the aggregate service, in order to operate within the scope of the data gathering and presentation system known to the inventors.

It is desired that users of portable devices be relieved of a requirement for storing a variety of passwords, log-in names and the like on their machines for accessing various data sources. Although the data-gathering and presentation service, known also as an Internet portal service, maintains, and manages passwords and log-in names or codes for subscribers, authentication to the service still must be completed whenever a subscriber wishes to synchronize his or her portable device with aggregated data. Prior-art data synchronization methods do not offer optimum security or convenience as was described further above.

What is clearly needed is a method and apparatus for secure authentication and data synchronization that eliminates the need for a user to provide password or log-in information to access a routinely-visited data source, and offers a protection against a single-point security breech of the data gathering and presentation service. Such a method and apparatus would be a convenience to users that routinely access more than one network-based data source from a portable device such as a PDA.

Summary of the Invention

In a preferred embodiment of the present invention a system for providing instant, automatic, and secure log-in to a network server for a portable device (PD) logging in to the network server via a first computer station acting as an Internet Host (IH) for the PD is provided, the system comprising first software executing on the computer station, including a location code (H-token) random number generator and a storage location reserved for the H-token; second software executing on the network server, including a password code (P-token) random number generator, and one or more tables relating P-tokens, H-tokens, and subscriber's user names and passwords; and third software executing on the PD, and a storage location on the PD reserved for a P-token generated by the different than the user's password. Upon a log-in request signal to the IH from the PD, the IH opens a communication link to the network server, requests the P-token from the PD, and, receiving the P-token, furnishes both the P-token and the IH-stored H-token, if any, to the network server, and the network server, only upon finding a match between P-token, H-token, and a valid subscriber, validates log-in without requesting user name and password.

In embodiments of the present invention, the first time a subscriber requests log-in from a PD having no valid stored random-number P-token, the network server requests the subscriber's user name and password, then creates a randomly-generated P-token, which is transmitted to the IH, and from the IH to the PD, where the PD stores the code for future log in operations. Also in embodiments of the invention, the first time a subscriber requests log-in from a PD having a valid P-token through an IH having no valid stored H-token, the IH randomly generates a new H-token, stores the new H-token in the storage location reserved for it, then furnishes the P-token and the new H-token to the network server, which requests user name and password for log in, and receiving a valid user name and password, grants log-in, and stores the new H-token associated with the user and the P-token for future log-in operations, thus validating a new IH location for valid instant log-in.

In preferred embodiments, in the absence of either a valid P-token or a valid H-token, the network server requests user name and password for log-in, and refuses log-in if the user name and password are not for a valid subscriber. The network server in many useful applications is a Web server connected to the Internet.

In another aspect of the invention a method for providing instant, automatic, and secure log-in to a network server for a portable device (PD) logging in to the network server via a first computer station acting as an Internet Host (IH) for the PD is provided, the method comprising steps of (a) upon receiving a log-in request signal by the IH from the PD, opening by the IH a communication link to the network server, requesting by the IH a password code (P-token) from the PD, and, receiving the P-token, furnishing both the P-token and an IH-stored H-token to the network server; and (b) upon finding a match by the network server between P-token, H-token, and a valid subscriber, validating log-in without requesting user name and password.

In a preferred embodiments of the method there is a step for, the first time a subscriber requests log-in from a PD having no valid stored random-number P-token, requesting by the network server the subscriber's user name and password, then creating a randomly-generated P-token, transmitting the new P-token to the IH, and from the IH to the PD, and the PD storing the new P-token for future log in operations.

Also in preferred embodiments there is a step for, , the first time a subscriber requests log-in from a PD having a valid P-token through an IH having no valid stored H-token, the IH randomly generating a new H-token, storing the new H-token in the storage location reserved for it, then furnishing the P-token and the new H-token to the network server, which requests user name and password for log in, and receiving a valid user name and password, granting log-in, and storing the new H-token associated with the user and the P-token for future log-in operations, thus validating a new IH location for valid instant log-in. In the absence of either a valid P-token or a valid H-token, the network server requests user name and password for log-in, and refuses log-in if the user name and password are not for a valid subscriber.

In many useful applications of the methods of the invention the network server is a Web server connected to the Internet.

For the first time with systems and methods according to preferred embodiments of the present invention, taught in enabling detail below, users of PDs logging onto network servers and services through computer hosts, may enjoy instant and automatic secure one-button log-in.

Brief Description of the Drawing Figures

Fig. 1 is an overview of a data-sync connection between a network data source and a portable device according to prior art.

Fig. 2 is an overview of a data-sync process between a network data source and a portable device according to an embodiment of the present invention.

Fig. 3 is a block diagram illustrating token generation and storage according to an embodiment of the present invention.

Fig. 4 is a process flow diagram illustrating logical steps for accomplishing a first time registering of a new host from a portable device according to an embodiment of the present invention.

Fig. 5 is a process flow diagram illustrating logical steps for accomplishing a routine data-sync process from a portable device according to an embodiment of the present invention.

Fig. 6 is a process flow chart illustrating a fail to authenticate scenario wherein a portable device was compromised.

Fig. 7 is a process flow diagram illustrating a fail to authenticate scenario wherein the network host was compromised.

Description of the Preferred Embodiments

In order to provide users of network-capable portable devices (PDs) with ultimate convenience in a secure operating environment, the inventor provides a method and apparatus for data synchronization between a PD and a network-based data source that requires no password or log-in information to be repetitively provided to authenticate a user for the purpose of accessing personal information. The method and apparatus of the present invention is taught in the enabling disclosure below.

Fig. 1 is an overview of a network architecture to illustrate a data-sync connection between a network data source and a portable device according to prior art. In this simple, prior-art example, a data-communication network 9 comprises a data packet network (DPN) 11, which in this case is the Internet, and an internet-service-provider (ISP) 13.

Network 11 may be another type of data packet network instead of the Internet such as perhaps a private or corporate wide area network (WAN) as long as Transfer Control Protocol/Internet protocol (TCP/IP) or other suitable network protocols are supported.

Internet 11 may include any geographical portion of the global Internet network including such as data sub-nets. Internet 11 has an Internet backbone 27 distributed throughout, which represents the many lines and connections which comprise the wired Internet as is known in the art.

Three data servers (DS) 21, 23, and 25 are illustrated within Internet 11 and connected to backbone 27. Servers 21-25 are, in this prior art example, assumed to be "data sources" known in the art for serving data that is held for and requested by users. Users in many cases operate by connecting directly to data servers 21-25, or may alternatively connect and download data through such as a host server (HS) 19 illustrated at far left. The types of data that may be held will depend on the nature of the data server and somewhat on the nature of the portable device used to gain access. Typically servers 21 through 25 hold e-mail, bank-account information, securities trading information and the like.

ISP 13 is adapted, in this prior-art example, for providing Internet services as known in the art. Illustrated within ISP 13 are a main connection server 15 and a modem bank 17, illustrated herein as a single modem icon. Main server 15 is directly connected to Internet 11.

A personal computer (PC) 31 is illustrated in this example as having an active Internet connection to Internet 11 through ISP 13 via a telephone line 29 and by virtue of modem bank 17 as is typical in the art of Internet access. PC 31 is thus an Internet

Host (IH) for a PDA 33 in this architecture. Line 29 may be a normal telephone line, an integrated services digital network (ISDN) line(s), or any other suitable wired connection. Other alternative Internet-access methods are known in the art and may be used. This prior art example illustrates the most common method (PC/modem).

PC 31 represents an exemplary user's PC that will act as an IH when the user is operating a connected peripheral device such as a PDA 33 illustrated to the right of PC 31. In this case PDA 33 maintains a wireless connection to PC 31 as illustrated by the dotted double arrow. The wireless connection may be such as a line-of-sight infra red system as known in the art. PDA 33 may also be connected to PC 31 by hard-wire connection, such a RS-232, TCP/IP, conventional serial port, Universal Serial Bus (USB), or any other suitable protocol.

This prior art example illustrates a simple data-sync connection between PDA 33 and any one of data servers 21-25, either directly or through a host server 19. In the practice of this prior art example, a conduit software application 35 is provided to run on PC 31 at a user's discretion. Software 35 is responsible for synchronizing data between PDA 33 and any one, or all of servers 21-25.

When a user operating PDA 33 desires to synchronize data with data stored on servers 21-25, he must first authenticate PDA 33 to the target data store via manual password and log-in requirement illustrated as manual operation 37. This log-in may alternatively be accomplished at IH 31. Once properly authenticated SW 35 may access secure data at servers 21-25 and synchronize the data with data already stored on PDA 33.

Typically, because each data server is a separate and non-cooperating entity, there will be more than one password and log-in requirement for the user to obtain authentication for all subscribed data.

One with skill in the art will recognize that the prior-art example represented herein may require considerable user resource in effecting synchronization of data between PDA 33 and a plurality of data sources such as those that would include servers 21-25.

Fig. 2 is an overview of an architecture for illustrating data-sync operations between network data-sources and various portable devices according to an embodiment of the present invention.

In a preferred embodiment of the present invention, a unique authentication system for portable network devices is provided to be used in conjunction with a data gathering and presentation service that is already known to the inventors. One such service is that disclosed in the cross-referenced patent application 09/323,598 wherein Web summaries are gathered and made available to users operating any network-capable appliance including portable devices. The preferred embodiment also includes a previously disclosed enhancement described in the related application entitled ***"Method and Apparatus for Abstract Restructuring of Personalized Data for Transmission from a Data Network to Varied Connected and Portable Network Appliances"*** wherein data to portable devices may be aggregated and restructured for such devices based on device model and device-specific software protocol. It is to be understood, however, that practice of the invention is not limited to such aggregating and restructuring services.

In some other embodiments, the method and apparatus of the present invention may be implemented with other existing data gathering systems such as may be known in the art. In still other embodiments, the method and apparatus of the present invention may be used in conjunction with a system that is adapted solely for providing data to specific or varied portable devices.

Referring again to Fig. 2, communication network 10 comprises Internet network 11, ISP 13, a data center 48, and at least one exemplary wireless data network represented herein by element number 14. Internet 11 may be another type of data packet network instead of the Internet, such as perhaps a private or corporate wide area network (WAN) as long as Transfer Control Protocol/Internet protocol (TCP/IP) or other suitable network protocols are supported.

Internet 11 may comprise any geographical portion of the global network including such as data sub-networks connected thereto. Internet backbone 27 represents the many lines and connection points making up the wired Internet as was described in Fig. 1. In this embodiment, three Web servers (WS) 39, 41, and 43 are illustrated within Internet 11 and connected to backbone 27.

Servers 39-43 are, in this embodiment, file servers known in the art for serving data in such as hypertext markup language (HTML), XML, or other suitable languages associated with electronic information pages known as WEB pages in the art. A portal Server (PS) 38 is shown as an Internet-connected Web server, and represents an aggregating service as known to the inventors and taught in individual ones of the cross-referenced documents.

For example, WS 39 may be an on-line bank server containing general information and links to more personal data (source data) such as user account information, loan information, user profile information and the like. WS 41 may be a main server for an instant messaging company. Information pages contained therein may contain links to message servers, user account information, and so on. WS 43 may be a server providing stock tracking and purchase services to individuals through the Internet. Web servers 39-43 are not related to or affiliated with each other in this example. In prior art, a user would have to negotiate with each WS 39-43 separately in order to get access to source data hosted by such servers. It should also be noted here that there are many server combinations used by companies practicing their trades on the Internet. In most instances, separate machines are used for holding separate kinds of data such as for secure information as opposed to general information. However, this is not always true as some companies may combine all information and data on one powerful machine.

ISP 13 is enabled, in this example, for providing Internet access services as known in the art. Illustrated within ISP 13 are a main connection server 15, a host server (HS) 37, and a modem bank 17. Main connection server 15 is directly connected to Internet 11. Server 15 is adapted to maintain user Internet connections and other normal ISP interface routines. HS 37 provides enhanced services for the ISP, to provide, for example, Internet access for miscellaneous PDs via a data center 48 communicating by a satellite 16 with PDs 32-36. In this enhancement data protocols may be changed to protocols commonly used by PDs by unique software not shown in this illustration.

A Portal Server 38 in the Internet in this embodiment is enabled to aggregate data from other Internet Web servers, such as servers 39-43, and to provide aggregated data to subscribers, as taught in the cross-referenced documents. In this aspect, a data repository 45 contains data about individual subscribers to the service of the present invention. Repository 45 may be an optical storage facility or any other convenient facility that is adapted for warehousing data. Repository 45 is illustrated as connected to PS 38. In addition to holding data specific to individual subscribers such as account information, address parameters, user ID and authorization data, repository 45 may also hold aggregated data gathered from such as Internet 11 before being delivered to or being accessed by users. Also residing in repository 45 is a database (DB) 55 that contains tabled encrypted data representing multiple user passwords and log-in codes organized in tables that are essential to practicing the device authentication methods of the present invention. Such tables and their contents are described in further detail below.

HS 37 is connected to a data center 48 by a data link 47. Data center 48, among other tasks, provides an Internet interface to HS 37 for various wireless data networks represented by network 14. Network 14 is further characterized by the illustration of a communication satellite 16, which exhibits an exemplary wireless data link connection to data center 48 as illustrated by a dotted double arrow. As previously described, network 14 may be plural in the sense that plural wireless data networks specific to certain communication devices may accomplish an interface to HS 37 through such as satellite 16 or another type of wireless transceiver/receiver and data center 48.

Within network 14 is illustrated a plurality of Internet-capable appliances, which are in this example, portable devices (PDs). These are a pager 32, a notebook computer 34, and a cellular telephone 36. In this example, appliances 32-36 broadcast data, which is picked up by such as satellite 16 and relayed to data center 48. Similarly, data arriving to such as satellite 16 from data center 48 is broadcast and picked-up by appliances 32, 34, and 36 as illustrated herein with dotted double arrows representing respective communication links. In the case of appliances 32 and 36, network 14 would be a cellular network as typically implemented for those devices.

In the case of notebook 34, network 14 may be a wireless Internet service using cellular or other suitable wireless technologies.

As previously described, main connection server 15 is connected to modem bank 17 as is known in the art of Internet access through an ISP. PC 31 is a user station operated by a user/subscriber to the data-gathering and presentation service, and is illustrated as connected to modem bank 17 by Internet connection line 29 as described in Fig. 1. Line 29 may be a normal telephone line, an integrated digital services network (ISDN) connection line, or any other suitable wired connection as was described in Fig. 1. PDA 33 is illustrated by a dotted double arrow as having a wireless communication link to PC 3, such as an infra-red communication link. This connection may also be by any suitable hard-wired link, such as serial, USB, and so on.

It was described in the background section that typical conduit software is used such as on a PC for synchronizing data between a data source and a portable device. It was also described that such software is generally proprietary in nature and covers only one host and affiliated data sources. The present invention provides a unique software application 51 that runs on any machine used as an Internet host (IH) for PDs. In this example the IH is PC 31. SW 51 enables instant and automatic security authentication for PDs according to embodiments of the present invention. Other instances of SW 51 are illustrated in this example as well. For example, an instance of SW 51 is provided on HS 37 to provide authentication services for PDs 32-36 connecting through data center 39. Yet another instance of SW 51 is provided to run on PS 38, and provides authentication services for requesting IH platforms for candidate PDs. There may be instances of SW 51 running on other Web servers as well. The several instances of SW 51 are not meant to indicate that the software is identical in each instance, but to indicate that the several instances are provided as compatible software which interact to provide the described features of the invention.

The device authentication methods of the present invention involve the use of binary strings (tokens). Some are generated randomly by SW 51 at IH devices, and some by SW51 at PS 38 or possibly at another Internet Web server. In a preferred embodiment, when a user operating an Internet-capable device, or a portable device having an Internet host such as PDA 33 or PDs 32-36 (Fig.1) wishes to synchronize data with PS 38 or another Web server enhanced with software according to an embodiment of the present invention,, he/she may simply initiate an automated secure process by depressing one button, making a single keystroke, or single-clicking with a mouse, for example.

Fig. 3 is a block diagram illustrating authentication architecture according to an embodiment of the present invention. PC Internet Host (IH) 31 or 37 has a number generator 57 (known in the art) adapted for generating random binary string tokens. This generator is a part of or associated with SW 51. The IH also has a non-volatile storage (may be local hard disk) 59 adapted for storing data.

The server-source with which data is to be synchronized, which is in this example Portal Server 38, has data repository 45 having data base 55 which is enabled by SW 51 to cooperate with IH devices and PDs to establish secure log-on according to embodiments oft he present invention. There is a number generator 58 provided for generating random binary string tokens as is generator 57 in IH 31,37. Database 55 stores user data including user ID, device configurations, and other user parameters as represented generally by a dotted rectangle labeled user block. Also maintained in database 55 are two tables, table 61, which is a password table, and table 63, which is a locations table. Database 55 may also comprise aggregated data represented by element number 65. Data 65 is requested synchronization-data collected from various Web sources by the data gathering and presentation service of the Portal Server 38.

Password table 61 stores user password tokens (P-tokens), user passwords, and user log-in names or codes. Locations table 63 stores user location tokens (H-tokens) and login names or codes. P-tokens are associated with H-tokens as described with reference to Fig. 2. Although only a single user-authentication data-set is represented in tables 61 and 63 in Fig. 3, it is noted that in actual practice, tables 61 and 63 will contain all of the authentication data-sets specific to all of the subscribers to the authentication service, all verified IH locations for each subscriber, and all P-tokens for PDs operated and verified for each subscriber.

The authentication system of the present invention is set up to provide easy one-button authentication for PDs through enabled IH devices, and to remember PDs authenticated to the system as well as which IH devices a user accesses for authentication. In the system of the invention instant authentication is enabled under the conditions that the user is a subscriber to the system, the PD used has been authenticated previously and has a stored P-token, and the IH through which the user attempts log-in is also authenticated to the system, having a stored H-token. Under these conditions the network server will have the P-token and the H-token stored and associated, and can quickly determine if the request for instant log-in is authentic.

There are four situations with which the system must deal in addition to the fully authenticated case of a valid subscriber with a valid PD and a valid IH. One is when a valid user/subscriber attempts to log-in through an authenticated IH with a new PD having enabling software but no P-token, this being a first-time use of the new PD with the system. Another is when a user with a valid PD attempts to log-in through a new IH. Still another is when both the PD and the IH are new to the system, but the user is a valid subscriber, and both the PD and the IH are enabled to operate with the system. The fourth situation is when a hacker attempts to log in, having found or stolen a valid PD, which will most likely occur through a non-valid IH.

In all cases other than a fully authenticated PD logging in through a fully authenticated IH, the system will ask for a user name and password. The first time a known user (subscriber) having a previously-used PD with a P-token logs on through a new IH device, he/she must provide a user name and password. In this initial process the IH device is identified (location) so subsequent log-ons may be automatic. If a user logs on from a different device, or new device other than one already identified in location tables at server-level, the user will be asked for log-in name and password again. If the new log-in is successful, the new H-token will be stored in location tables at server level, and added to the list of IH devices the user may use for automated access.

Fig. 4 is a process flow diagram illustrating steps for accomplishing first time registering of a new Internet host (IH) by logging in from a new PD according to an embodiment of the present invention. In this example, it is assumed that the user in the example has previously provided password and log-in information such as user name and password to the data server, in this example Portal Server 38. The example will be most easily understood with reference to both Figs. 3 and 4, and for simplicity will be assumed to involve PD 33, IH 31 and PS 38 as the network-level data source.

In step 67, the user initiates a log-in to the subscription service on PS 38 from PD 33, not before used for log-in using IH 31, not before used for log-in either. The user enters the correct password and log-in previously known to the secure server (38). IH 31, as a part of the process, generates a random H-token identifying IH 31 at step 69. At step 71, IH 31 stores the generated H-token to NV storage, such as to disk. For added security tokens are typically 32 bit binary words or longer, but may be shorter is desired.

In step 73 IH 31 opens a secure socket layer (SSL) connection (known in the art) to PS 38. In step 75, IH 31 sends the actual log-in, password and H-token to repository 45 at PS 38 over the secure connection. In step 77, repository 45 tables the generated H-token and the actual log-in name or code in table 63 of Fig. 3. Also at step 77, a random P-token is generated by the server (generator 58).

At step 79, repository 45 tables the generated P-token, actual password, and actual log-in name or code in table 61 of Fig. 3. At step 81, repository 45 sends the generated P-token to IH 33. At step 83, IH 31 sends the generated P-token to the user's requesting device, PD 33, where it is stored. At step 85, IH 31 eliminates all knowledge of the generated P-token at IH 31. A user is now configured through the system of the invention to automatically log-on and synchronize data from PD 33 with PS 38 through IH 31 without being required to repeat any authentication process such as re-entering a password or log-in. This may be done by a single-button input by the PD, for example. IH 31 has a stored, valid H-token and PD 33 has a stored and valid P-token.

It will be apparent to the skilled artisan that the process varies only in detail for the case where either the IH is new and the PD has a P-token, or the PD is new and the IH has an H-token. In either case the missing token will be generated and stored, and the system will require full user name and password before validating log-in.

Each time a user requests authentication through a new IH, the system will list another H-code to identify the new location. For example, the present user may now attempt to log-in to PS 38 through server 37 as IH. When the log-in is done, asking the user for name and password, a new H-code generated randomly by IH 37 will be listed in the location table at PS 38. A user may thus configure to have one-button service from any number of IHs by logging on through each.

Fig. 5 is a process flow diagram illustrating logical steps for accomplishing a routine data-sync authentication and process from a portable device according to an embodiment of the present invention. At step 87, a user initiates an authentication and synchronization procedure by a one-button input on his/her PD, such as PD 33, through IH 31. IH 31 has been used previously for such log-in and data sync. At step 88 IH 31 requests a P-token from PD 33. At step 89 PD 33 send the stored P-token to IH 31. At step 91, IH 31 retrieves the H-token from its own internal storage (location code).

At step 93, IH 31 sends the H-token and P-token to PS 38. In step 95, repository 45 at PS 38 looks for the P-token in table 61 in DB 55, and finding the P-token listed there obtains the corresponding password and log-in name or code listed in the table. At step 97, repository 45 looks for and obtains corresponding H-tokens listed in table 62 (Fig. 2).

If at step 99, one of the corresponding H-tokens matches the H-token sent to repository 45 by IH 31, then authentication is complete. At step 101 then, the repository sends all collected and aggregated data to IH 31. The user's device is then synchronized with the aggregated data at step 103.

After following the descriptions above, it will be apparent that there are several advantages to the system of the invention. To hack the system, for example, requires two points of entry. If an attacker finds or steals a user's PD, and also finds a kiosk or other Internet host that is enabled with compatible software, when that attacker initiates the transaction with the one-button input, the system will generate at the IH a new H-code, which will not be found listed on the network-level server. The server part of the system will then demand the name and password, which of course the attacker will not know. To cheat the system requires that the attacker not only acquire the PD, but attempt the authentication through an IH already configured by the user, such as the user's home or office PC.

The method and apparatus of the present invention may be practiced with the data gathering and presentation service as known to the inventors. The method and apparatus of the present invention may also be practiced with virtually any Internet host that has locally-stored data or controls connected data sources. It is only necessary that the server portion of software 51 be implemented on the network server to enable interaction with local Internet hosts through which users may log-in.

It will be apparent to the skilled artisan that there may be a variety of alterations made in the embodiments of the description described herein without departing from the spirit and scope of the invention. For example, tokens may be of varying length. Also, tokens need not be randomly generated numbers in every case. A P-token could instead be a secure cryptographic hash of a username/password combination for example. Steps of the process may be somewhat re-ordered. Internet data sources may be of many different sorts, and so on. An H-token could be device or chip IDs for the Internet Host (IH) CPU, for example. The spirit and scope of the present invention is limited only by the claims that follow.

What is claimed is:

1. A system for providing instant, automatic, and secure log-in to a network server for a portable device (PD) logging in to the network server via a first computer station acting as an Internet Host (IH) for the PD, the system comprising:

first software executing on the computer station, including a location token (H-token) generator and a storage location reserved for the H-token;

second software executing on the network server, including a password code (P-token) generator, and one or more tables relating P-tokens, H-tokens, and subscriber's user names and passwords; and

third software executing on the PD, and a storage location on the PD reserved for the P-token;

characterized in that, upon a log-in request signal to the IH from the PD, the IH opens a communication link to the network server, requests the P-token from the PD, and, receiving the P-token, furnishes both the P-token and the IH-stored H-token, if any, to the network server, and the network server, only upon finding a match between P-token, H-token, and a valid subscriber, validates log-in without requesting user name and password.

2. The system of claim 1 wherein the first time a subscriber requests log-in from a PD having no valid stored P-token, the network server requests the subscriber's user name and password, then creates a P-token, which is transmitted to the IH, and from the IH to the PD, where the PD stores the P-token for future log-in operations.

3. The system of claim 1 wherein the first time a subscriber requests log-in from a PD having a valid P-token through an IH having no valid stored H-token, the IH generates a new H-token, stores the new H-token in the storage location reserved for it, then furnishes the P-token and the new H-token to the network server, which requests user name and password for log in, and receiving a valid user name and password, grants

log-in, and stores the new H-token associated with the user and the P-token for future log-in operations, thus validating a new IH location for valid instant log-in.

4. The system of claim 1 wherein, in the absence of either a valid P-token or a valid H-token, the network server requests user name and password for log-in, and refuses log-in if the user name and password are not for a valid subscriber.

5. The system of claim 1 wherein the network server is a Web server connected to the Internet.

6. A method for providing instant, automatic, and secure log-in to a network server for a portable device (PD) logging in to the network server via a first computer station acting as an Internet Host (IH) for the PD, the method comprising steps of:

(a) upon receiving a log-in request signal by the IH from the PD, opening by the IH a communication link to the network server, requesting by the IH a password code (P-token) from the PD, and, receiving the P-token, furnishing both the P-token and an IH-stored location code (H-token) to the network server; and

(b) upon finding a match by the network server between P-token, H-token, and a valid subscriber, validating log-in without requesting user name and password.

7. The method of claim 6 further comprising a step for, the first time a subscriber requests log-in from a PD having no valid stored P-token, requesting by the network server the subscriber's user name and password, then creating a P-token, transmitting the new P-token to the IH, and from the IH to the PD, and the PD storing the new P-token for future log in operations.

8. The method of claim 6 further comprising a step for, the first time a subscriber requests log-in from a PD having a valid P-token through an IH having no valid stored H-token, the IH generating a new H-token, storing the new H-token in the storage location reserved for it, then furnishing the P-token and the new H-token to the network server, which requests user name and password for log in, and receiving a

valid user name and password, granting log-in, and storing the new H-token associated with the user and the P-token for future log-in operations, thus validating a new IH location for valid instant log-in.

9. The method of claim 6 wherein, in the absence of either a valid P-token or a valid H-token, the network server requests user name and password for log-in, and refuses log-in if the user name and password are not for a valid subscriber.

10. The method of claim 6 wherein the network server is a Web server connected to the Internet.

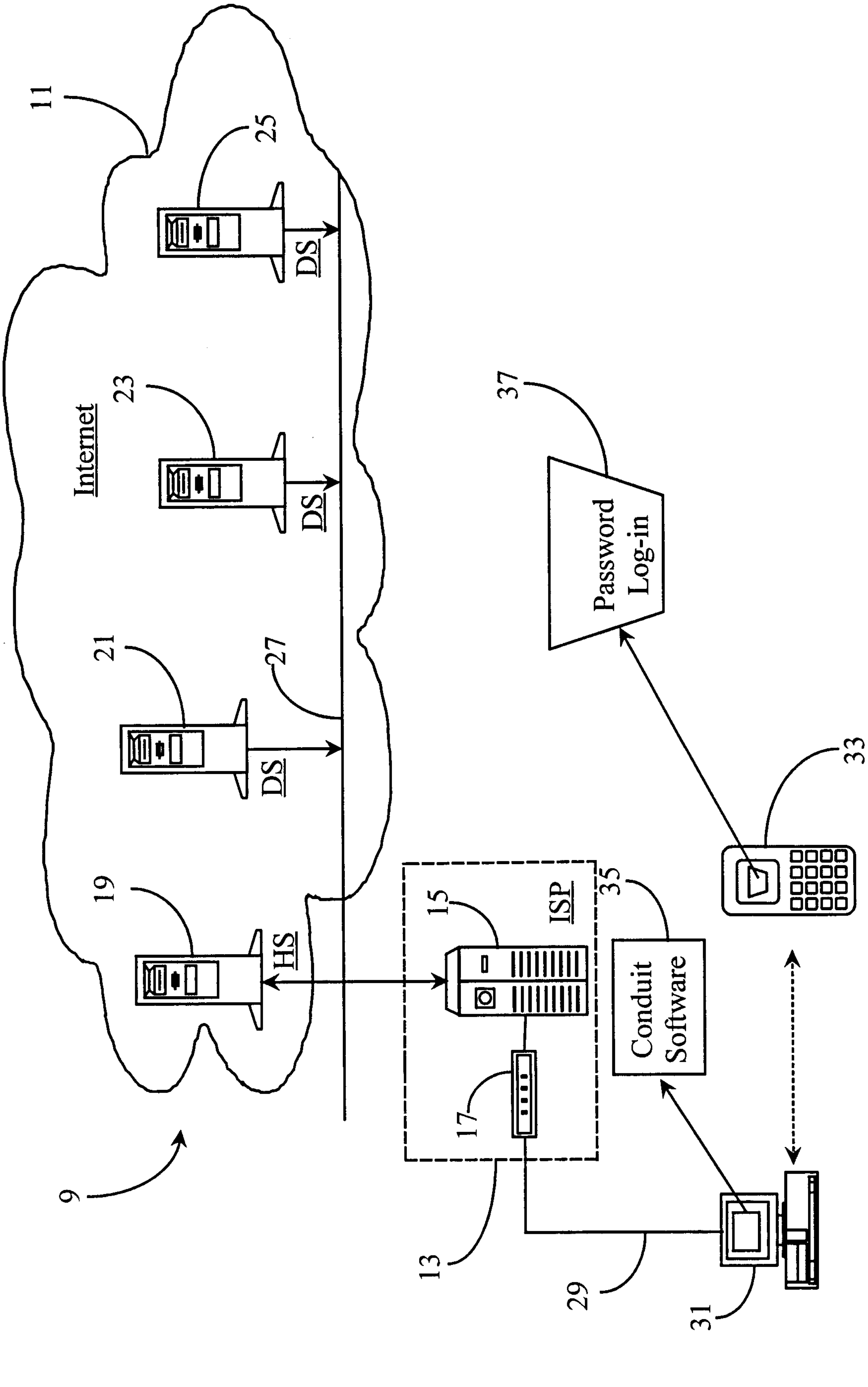

11
Internet
19
HS
21
DS
23
DS
25
DS
27
9
ISP
15
17
13
29
31
Conduit Software
35
33
Password Log-in
37

Fig. 1

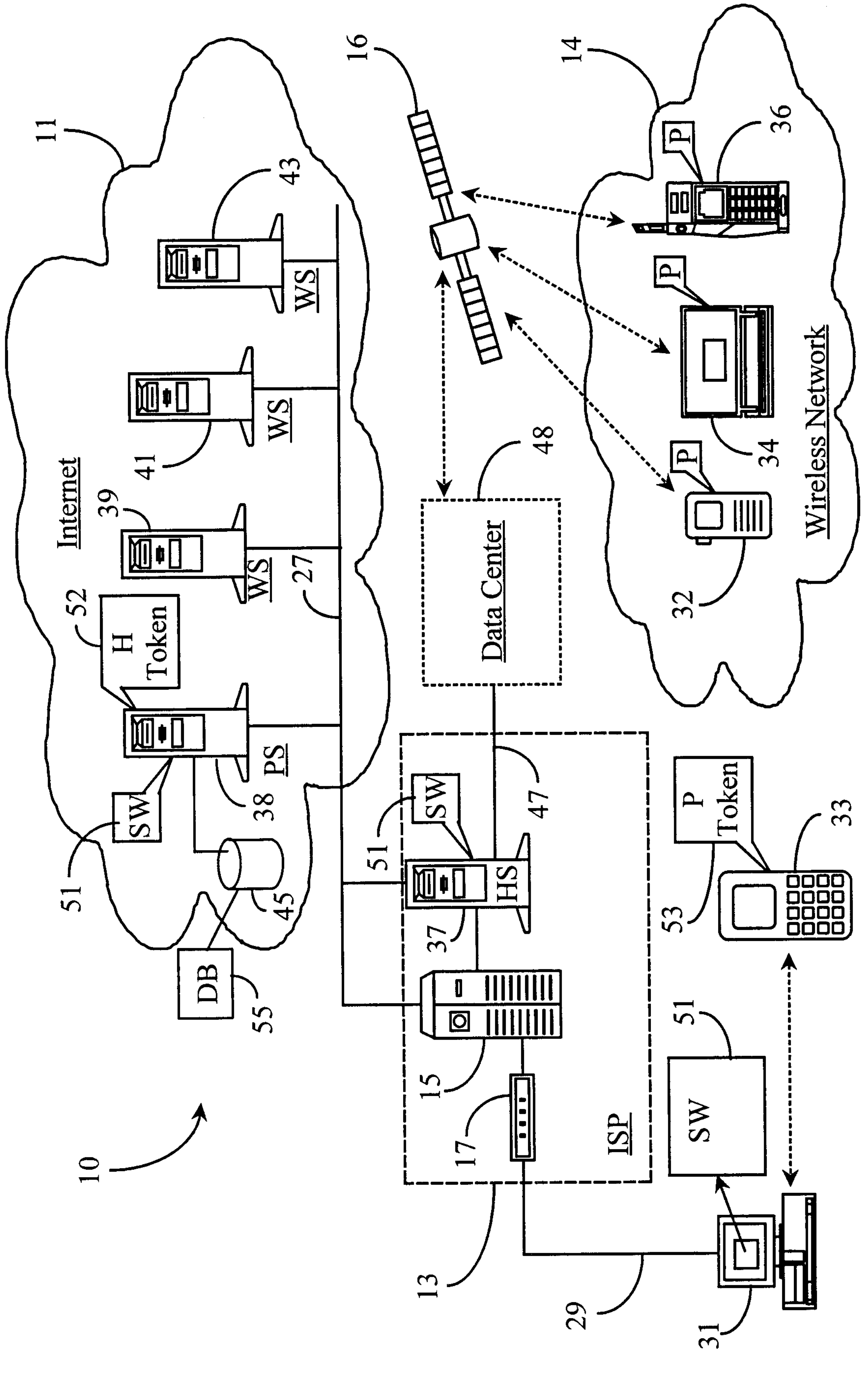

10
11
Internet
WS
WS
WS
PS
HS
H Token
52
SW
51
38
39
41
43
27
45
DB
55
37
SW
51
15
17
ISP
13
47
Data Center
48
16
14
P
36
P
34
P
32
Wireless Network
P Token
53
33
SW
51
29
31

Fig. 2

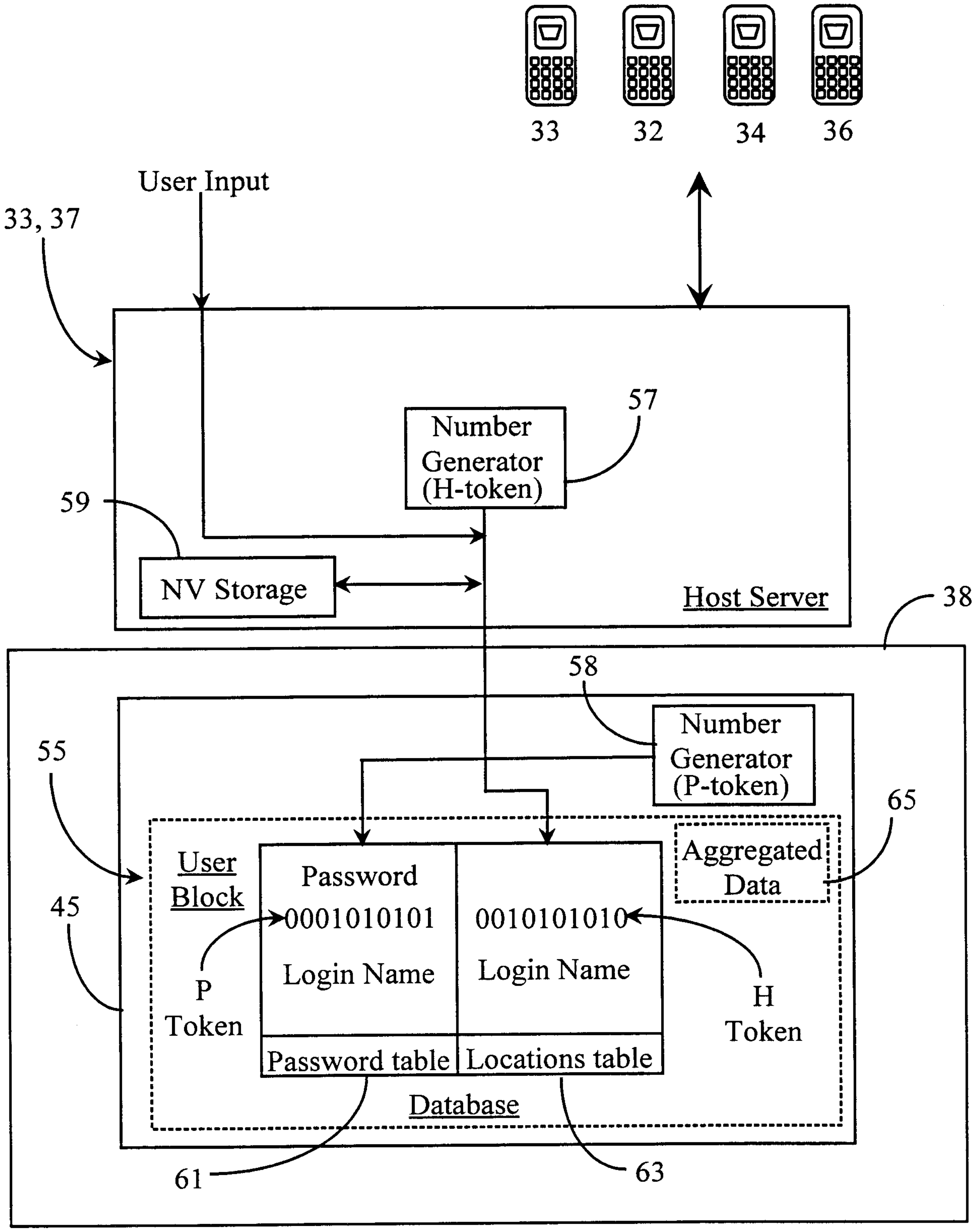

33
32
34
36
User Input
33, 37
Number Generator (H-token)
57
59
NV Storage
Host Server
38
58
Number Generator (P-token)
55
65
User Block
Password
0001010101
Login Name
0010101010
Login Name
Aggregated Data
45
P Token
H Token
Password table
Locations table
Database
61
63

Fig. 3

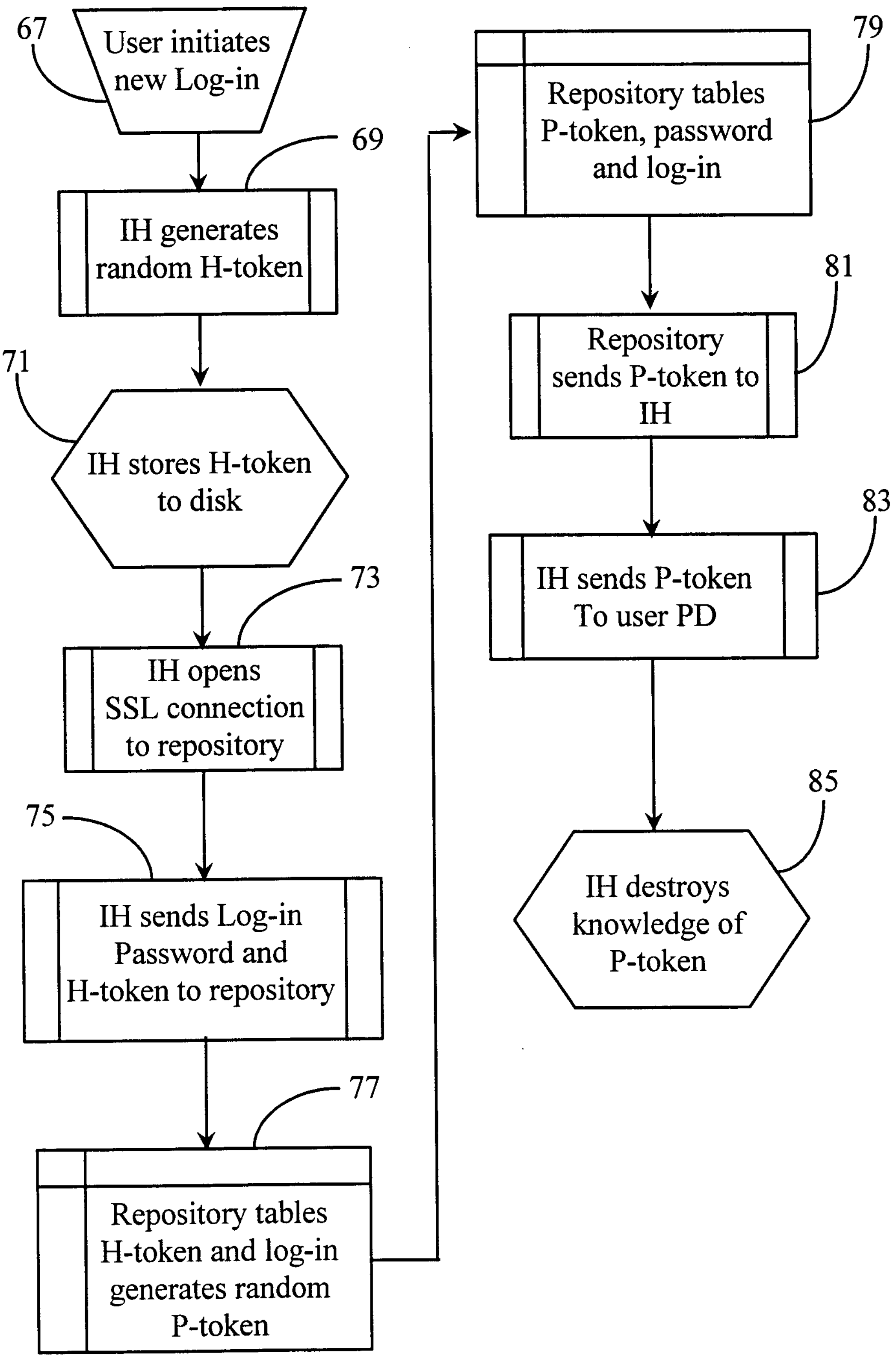

67
User initiates new Log-in
69
IH generates random H-token
71
IH stores H-token to disk
73
IH opens SSL connection to repository
75
IH sends Log-in Password and H-token to repository
77
Repository tables H-token and log-in generates random P-token
79
Repository tables P-token, password and log-in
81
Repository sends P-token to IH
83
IH sends P-token To user PD
85
IH destroys knowledge of P-token

Fig. 4

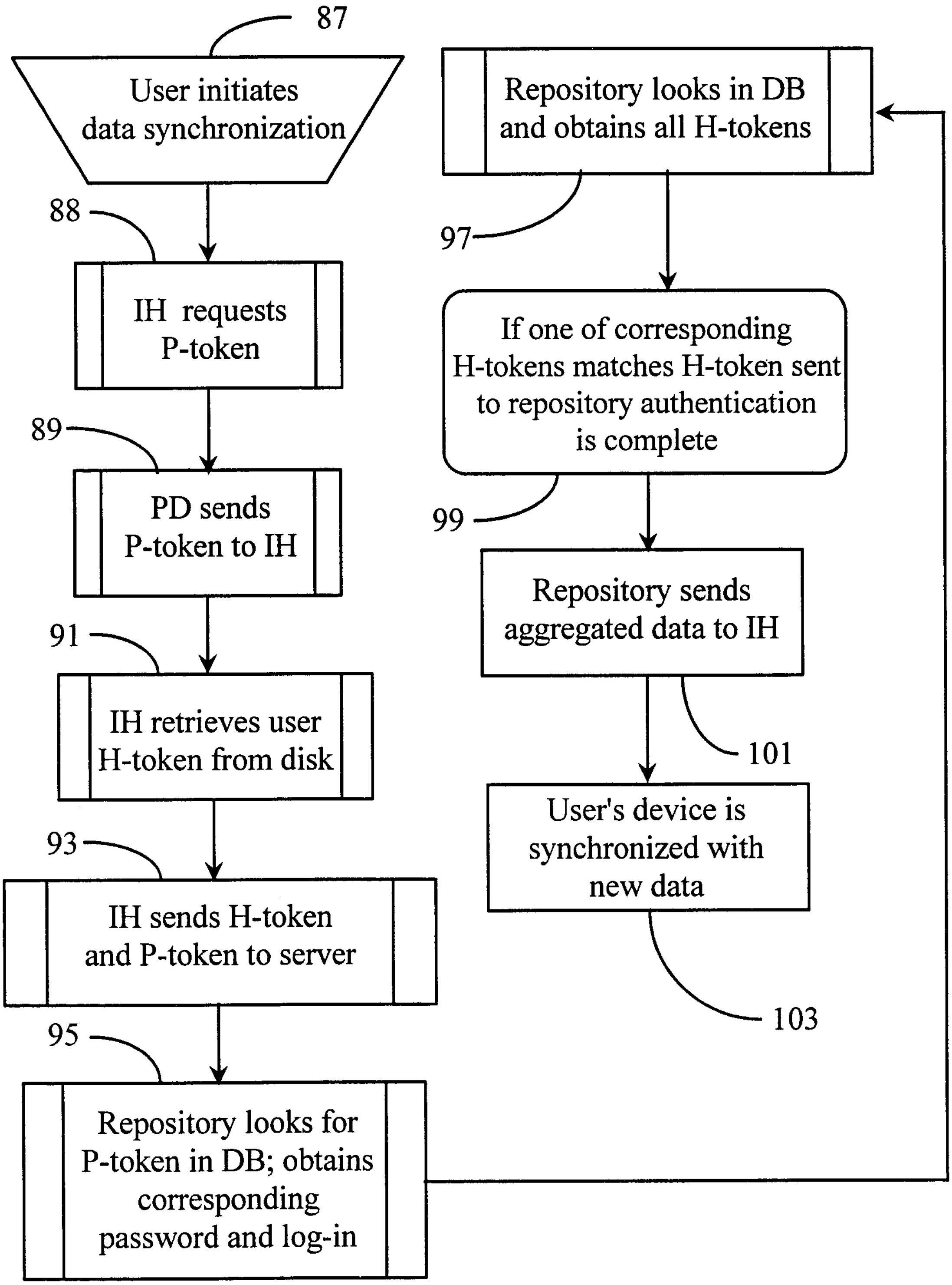

87
User initiates data synchronization
88
IH requests P-token
89
PD sends P-token to IH
91
IH retrieves user H-token from disk
93
IH sends H-token and P-token to server
95
Repository looks for P-token in DB; obtains corresponding password and log-in
Repository looks in DB and obtains all H-tokens
97
If one of corresponding H-tokens matches H-token sent to repository authentication is complete
99
Repository sends aggregated data to IH
101
User's device is synchronized with new data
103

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/23781

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06K 9/00; G06F 11/00
US CL : 713/200, 201, 202, 172; 705/69, 65, 66, 348/10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202, 172; 705/69, 65, 66, 348/10

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

none

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

none

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,892,900 A (GINTER et al.) 06 April 1999, col 1, lines 9-36, lines 41-67, col 2, lines 1-67, col 3, lines 1-67.	1-10
Y	US 5,613,012 A (HOFFMAN et al.) 18 March 1997, col 1, lines 14-67, col 2, lines 1-67, col 3, lines 1-67, col 4, lines 9-67.	1-10

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 26 SEPTEMBER 2000	Date of mailing of the international search report 17 NOV 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer Peggy Harrod BEAUSOLEIL ROBERT W. Jr.
Facsimile No. (703) 305-3230	Telephone No. (703) 305-3987