



(22) Date de dépôt/Filing Date: 2003/11/28

(41) Mise à la disp. pub./Open to Public Insp.: 2005/05/28

(45) Date de délivrance/Issue Date: 2011/10/18

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),  
*H04L 12/12* (2006.01), *H04L 12/22* (2006.01),  
*H04L 12/24* (2006.01), *H04L 12/28* (2006.01)

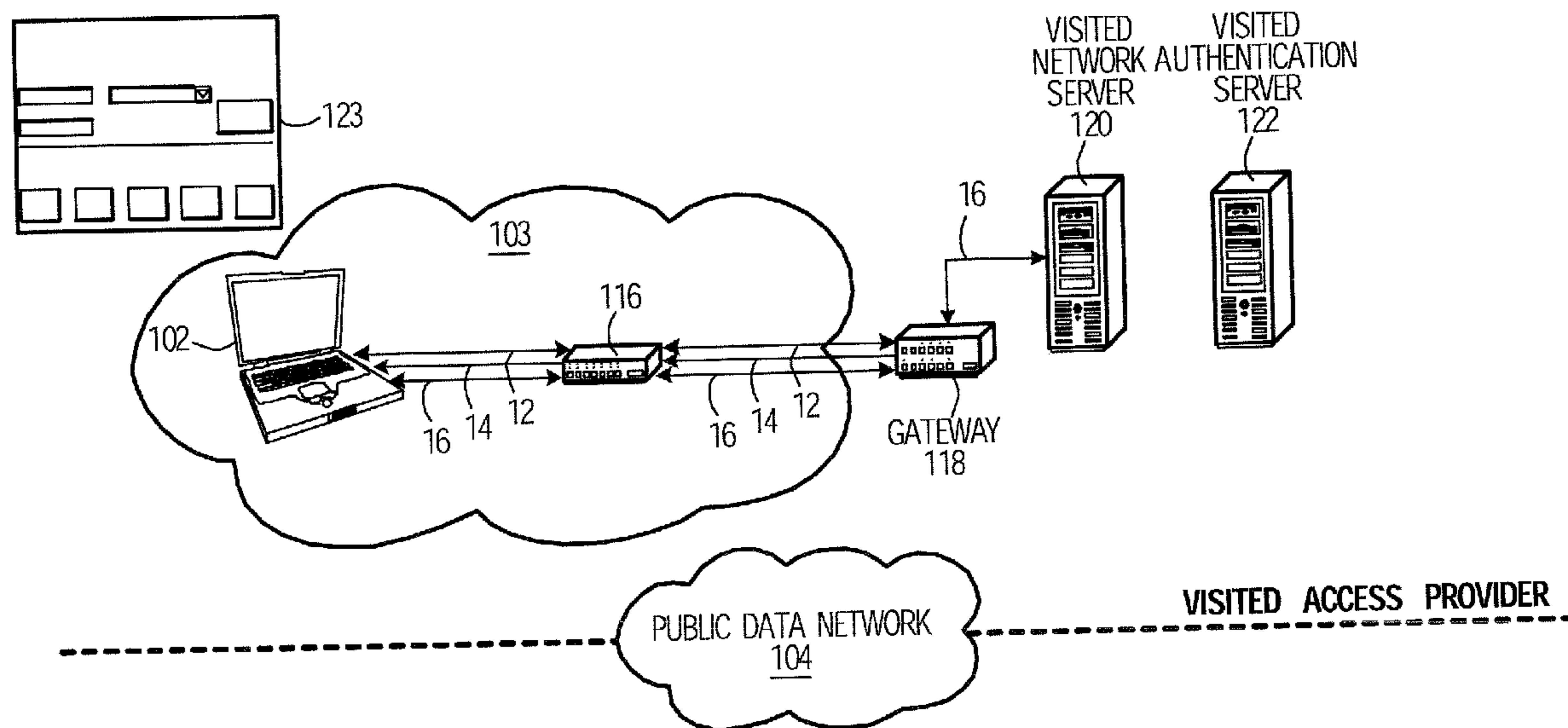
(72) Inventeurs/Inventors:  
NEDKOV, NICOLAS, CA;  
WONG, SPENCER, CA;  
SMITH, BRIAN NORMAN, CA

(73) Propriétaire/Owner:  
BCE INC., CA

(74) Agent: SMART & BIGGAR

(54) Titre : SYSTEMES ET METHODES DE CONTROLE D'ACCES A UN RESEAU PUBLIC DE DONNEES A PARTIR  
D'UN FOURNISSEUR D'ACCES VISITE

(54) Title: SYSTEMS AND METHODS FOR CONTROLLING ACCESS TO A PUBLIC DATA NETWORK FROM A  
VISITED ACCESS PROVIDER



(57) Abrégé/Abstract:

To allow a user to access a public data network from a region of service operated by a visited access provider, the visited provider is supplied with an identity of a credit provider. The user is redirected to the credit provider, resulting in establishment of a temporary connection with the credit provider. During this temporary connection, the user supplies original user credentials and, in return, receives substitute user credentials if the original user credentials are valid. The substitute user credentials are supplied to the visited provider, which proceeds to have the user authenticated by the credit provider on the basis of the substitute user credentials. In this way, the visited provider authenticates the user with the credit provider before allowing the user to access the public data network, but a secure exchange of the original user credentials between the user and the credit provider prevents unauthorized access to this information by the visited provider.

1    ***ABSTRACT OF THE DISCLOSURE***

2

3    To allow a user to access a public data network from a region of service operated by a  
4    visited access provider, the visited provider is supplied with an identity of a credit  
5    provider. The user is redirected to the credit provider, resulting in establishment of a  
6    temporary connection with the credit provider. During this temporary connection, the  
7    user supplies original user credentials and, in return, receives substitute user credentials  
8    if the original user credentials are valid. The substitute user credentials are supplied to  
9    the visited provider, which proceeds to have the user authenticated by the credit provider  
10   on the basis of the substitute user credentials. In this way, the visited provider  
11   authenticates the user with the credit provider before allowing the user to access the  
12   public data network, but a secure exchange of the original user credentials between the  
13   user and the credit provider prevents unauthorized access to this information by the  
14   visited provider.

15

1           **SYSTEMS AND METHODS FOR CONTROLLING ACCESS TO A**  
2           **PUBLIC DATA NETWORK FROM A VISITED ACCESS PROVIDER**

3  
4  
5       ***FIELD OF THE INVENTION***

6  
7       The present invention relates generally to telecommunications and, more specifically, to  
8       methods for controlling access to a public data network, such as the internet, from access  
9       points operated by different competitive entities.

10  
11       ***BACKGROUND OF THE INVENTION***

12  
13       The availability of ubiquitous, wireless internet access is a simple design goal in theory,  
14       yet its implementation in practice is replete with business considerations that need to be  
15       addressed with advanced technical solutions. In particular, the increased desire for  
16       people to access the internet from their own computers where data resides locally  
17       requires an entirely different approach from the simplistic “internet cafés” that have  
18       sprouted into existence globally in recent years. To this end, the industry has seen the  
19       emergence of various standards, including IEEE 802.11b, known to those in the industry  
20       as “Wi-Fi”. The reader is invited to consult <http://www.wi-fi.org> on the internet for  
21       further information on Wi-Fi as well as the Wi-Fi alliance, a nonprofit international  
22       association formed in 1999 to certify interoperability of wireless Local Area Network  
23       products based on IEEE 802.11 specification.

24  
25       Since the emergence of the IEEE 802.11b specification in 1999, an increasing number of  
26       vendors have used this standard in producing Wi-Fi compliant wireless LAN (WLAN)  
27       products. Pioneers of high speed internet access have built WLAN “hotspots”, which are  
28       basically zones of public internet access. Since it is difficult for a single service provider  
29       to build an infrastructure that offers global access to its subscribers, roaming between  
30       service providers is essential for delivering global access to customers. Roaming allows  
31       enterprises and service providers to enhance their employee connectivity and service  
32       offerings by expanding their footprint to include network access at Wi-Fi enabled  
33       hotspots.

1 In a roaming scenario, a wireless device (e.g. a laptop, PDA, etc.) moves to a hotspot not  
2 operated by its home access provider. It is here that registration of the device with the  
3 visited access provider and authorization of the access from the home access provider  
4 must take place. Conventional solutions require the user to supply their home login  
5 credentials to the visited access provider's authentication, authorization and accounting  
6 (AAA) server and this visited AAA server then validates the user's home login  
7 credentials by interacting with the home access provider.

8

9 Disadvantageously, a problem arises due to the visited AAA server having complete  
10 access to customer login information for customers utilizing a competitor as its access  
11 provider while roaming. This information can easily be abused. While clearly an issue  
12 amongst competing corporate entities providing internet access, this problem is expected  
13 to generate even greater concern as increasing numbers of smaller, independent  
14 enterprises begin to operate their own hotspots in the future, with few or no regulatory  
15 restrictions.

16

17 Against this background, there is a need to improve the security of the process by which  
18 a user having a business relationship with a home access provider obtains access to the  
19 Internet via a gateway operated by a visited access provider.

20

## 21 ***SUMMARY OF THE INVENTION***

22

23 A first broad aspect of the present invention seeks to provide a method of controlling  
24 access to a public data network from a visited access provider. The method comprises  
25 receiving from a client device a message indicative of a request to access the data  
26 network; supporting a temporary connection between the client device and a credit  
27 provider, the temporary connection comprising a transmission of substitute user  
28 credentials from the credit provider in response to transmission of original user  
29 credentials from the client device; receiving the substitute user credentials from the client  
30 device; communicating the substitute user credentials to the credit provider to  
31 authenticate the client device; responsive to successful authentication of the client device  
32 by the credit provider on the basis of the substitute user credentials, authorizing the client  
33 device to access the data network; and wherein the temporary connection is secured to

1 prevent the visited access provider from determining the original user credentials  
2 transmitted by the client device.

3

4 A second broad aspect of the present invention seeks to provide a network. The network  
5 comprises a network server entity adapted to receive from a client device a message  
6 indicative of a credit provider; and a gateway entity adapted to support a temporary  
7 connection between the client device and the credit provider via the network server  
8 entity, the temporary connection comprising a transmission of substitute user credentials  
9 from the credit provider in response to transmission of original user credentials from the  
10 client device, the temporary connection being secured to prevent the network server  
11 entity from determining the original user credentials transmitted by the client device.  
12 The network server entity is further adapted to receive the substitute user credentials  
13 from the client device. The network further comprises an authentication entity adapted  
14 to communicate the substitute user credentials to the credit provider to authenticate the  
15 client device. The network server entity is further adapted to authorize the client device  
16 to access the data network in response to successful authentication of the client device by  
17 the credit provider on the basis of the substitute user credentials.

18

19 A third broad aspect of the present invention seeks to provide a network. The network  
20 comprises server means for receiving from a client device a message indicative of a  
21 credit provider; means for supporting a temporary connection between the client device  
22 and the credit provider via the server means, the temporary connection comprising a  
23 transmission of substitute user credentials from the credit provider in response to  
24 transmission of original user credentials from the client device, the temporary connection  
25 being secured to prevent the server means from determining the original user credentials  
26 transmitted by the client device; means for receiving the substitute user credentials from  
27 the client device; means for communicating the substitute user credentials to the credit  
28 provider to authenticate the client device; and means for authorizing the client device to  
29 access the data network in response to successful authentication of the client device by  
30 the credit provider on the basis of the substitute user credentials.

31

32 A fourth broad aspect of the present invention seeks to provide a method of  
33 authenticating users having a business relationship with a credit provider. The method

1 comprises receiving original user credentials from a client device over a temporary  
2 connection that passes through a visited provider of access to a data network, the  
3 temporary connection being secured to prevent the visited provider of access from  
4 determining the original user credentials transmitted by the client device; sending  
5 substitute user credentials to the client device over the temporary connection, the  
6 substitute user credentials being associated with the original user credentials; receiving  
7 the substitute user credentials from the visited provider of access; authenticating the  
8 client device on the basis of the substitute user credentials; and responsive to successful  
9 authentication of the client device on the basis of the substitute user credentials,  
10 indicating to the visited provider of access to the data network that the client device has  
11 been successfully authenticated.

12

13

14 A fifth broad aspect of the present invention seeks to provide a credit provider having a  
15 business relationship with a plurality of users. The credit provider comprises a network  
16 server entity and an authentication entity. The network server entity is adapted to:  
17 receive original user credentials from a client device over a temporary connection that  
18 passes through a visited provider of network access, the temporary connection being  
19 secured to prevent the visited provider of network access from determining the original  
20 user credentials transmitted by the client device; and send substitute user credentials to  
21 the client device over the temporary connection, the substitute user credentials being  
22 associated with the original user credentials. The authentication entity is adapted to  
23 receive the substitute user credentials from the visited provider of network access;  
24 authenticate the client device on the basis of the substitute user credentials; and indicate  
25 to the visited provider of network access that the client device has been successfully  
26 authenticated in response to successful authentication of the client device on the basis of  
27 the substitute user credentials.

28

29 A sixth broad aspect of the present invention seeks to provide a credit provider having a  
30 business relationship with a plurality of users. The credit provider comprises means for  
31 receiving original user credentials from a client device over a temporary connection that  
32 passes through a visited provider of access to a data network, the temporary connection  
33 being secured to prevent the visited provider of access from determining the original user

1 credentials transmitted by the client device; means for sending substitute user credentials  
2 to the client device over the temporary connection, the substitute user credentials being  
3 associated with the original user credentials; means for receiving the substitute user  
4 credentials from the visited provider of access; means for authenticating the client device  
5 on the basis of the substitute user credentials; and means for responsive to successful  
6 authentication of the client device on the basis of the substitute user credentials,  
7 indicating to the visited provider of access to the data network that the client device has  
8 been successfully authenticated.

9  
10 A seventh broad aspect of the present invention seeks to provide a method of accessing a  
11 public data network from a region of service operated by a visited access provider. The  
12 method comprises supplying to the visited access provider an identity of a credit  
13 provider; establishing a temporary connection with the credit provider; receiving  
14 substitute user credentials from the credit provider during the temporary connection in  
15 response to supplying the credit provider with original user credentials provider during  
16 the temporary connection; and supplying the substitute user credentials to the visited  
17 access provider for authentication of the client device by the credit provider on the basis  
18 of the substitute user credentials; wherein the temporary connection is secured to prevent  
19 the visited access provider from determining the original user credentials supplied to the  
20 credit provider.

21  
22 An eighth broad aspect of the present invention seeks to provide and apparatus for  
23 accessing a data network from a region of service operated by a visited access provider.  
24 The apparatus comprises means for supplying to the visited access provider an identity of  
25 a credit provider; means for establishing a temporary connection with the credit provider;  
26 means for receiving substitute user credentials from the credit provider during the  
27 temporary connection in response to supplying the credit provider with original user  
28 credentials provider during the temporary connection; and means for supplying the  
29 substitute user credentials to the visited access provider for authentication of the client  
30 device by the credit provider on the basis of the substitute user credentials; wherein the  
31 temporary connection is secured to prevent the visited access provider from determining  
32 the original user credentials supplied to the credit provider.

33

1 A ninth broad aspect of the present invention seeks to provide a graphical user interface  
2 for guiding a user through a process of accessing a data network from a region of service  
3 operated by a visited access provider. The graphical user interface comprises a browser  
4 capable of interfacing with a user; and a control entity operative to: output via the  
5 browser content from the visited access provider; responsive to identification via the  
6 browser of a credit provider, output via the browser content from the credit provider, said  
7 content from the credit provider being inaccessible by the visited access provider; and  
8 responsive to identification via the browser of user credentials of a particular user having  
9 a business relationship with the credit provider, access content of user-selected locations  
10 on the data network.

11

12 A tenth broad aspect of the present invention seeks to provide a computer program  
13 product for use with a client device in accessing a data network from a region of service  
14 operated by a visited access provider, the computer program product comprising a  
15 computer usable medium having computer readable program code thereon. The  
16 computer readable program code includes program code for implementing a browser to  
17 interface with a user; program code for outputting via the browser content from the  
18 visited access provider; program code for outputting via the browser content from a  
19 credit provider in response to receiving via the browser an identification of the credit  
20 provider, said content from the credit provider being inaccessible by the visited access  
21 provider; and program code for accessing via the browser content of user-selected  
22 locations on the data network in response to receiving via the browser an identification  
23 of user credentials of a particular user having a business relationship with the credit  
24 provider.

25

26 These and other aspects and features of the present invention will now become apparent  
27 to those of ordinary skill in the art upon review of the following description of specific  
28 embodiments of the invention in conjunction with the accompanying drawings.

29

### 30 ***BRIEF DESCRIPTION OF THE DRAWINGS***

31

32 Figs. 1A through 1F show different steps in a process for authenticating a user of a  
33 visited provider of access to a public data network;

1

2

3 Fig. 2 is a diagram illustrating the flow of messages exchanged between different entities  
4 in Figs. 1A through 1F.

5

6 ***DETAILED DESCRIPTION OF THE EMBODIMENTS***

7

8 Fig. 1A shows a client device 102 that has entered a region 103 of service to a public  
9 data network 104. The public data network 104 could be the internet or, generally, any  
10 network accessible at multiple access points operated by different “access providers”. In  
11 specific circumstances, the client device 102 may be a laptop, PDA, handheld computing  
12 device, tablet PC, or any other wireless device. The client device 102 could also be a  
13 mobile telephone, provided it is equipped with a suitable network interface other than, or  
14 in addition to, a standard wireless interface. The user of the client device 102 is assumed  
15 to have a business relationship with a “home” access provider. In an example, the user  
16 may be a mobile telephone network subscriber, an internet access subscriber, a cable  
17 subscriber, local telephone service subscriber, power company subscriber, etc.

18

19 In the roaming scenario illustrated in Fig. 1A, access to the public data network 104 from  
20 within the region 103 is controlled by a visited provider of public data network access.  
21 Accordingly, such access provider may be termed a “visited” access provider. The  
22 visited access provider is shown as comprising a physical access module 116, a gateway

1 118, a visited network server 120 (e.g., a web server) and a visited authentication server  
2 122. A non-limiting example of an authentication server 122 is an identity system or  
3 database capable of handling the RADIUS protocol. An example is the LDAP database  
4 (or another server) that is capable of communicating in accordance with the RADIUS  
5 protocol. For simplicity, communication links between the physical access module 116,  
6 the gateway 118, the visited network server 120 and the visited authentication server 122  
7 have been omitted from the drawing.

8  
9 In a specific embodiment, the physical access module 116 may be implemented as a bi-  
10 directional radio frequency transceiver, adapted to exchange wireless signals with the  
11 client device 102. It is within the scope of the present invention to exchange wireless  
12 signals conforming with the IEEE 802.11 standards, although this is not a requirement of  
13 the present invention. Other types of signals that could be exchanged between the client  
14 device 102 and the physical access module 116 include free space optical signals, infra-  
15 red signals, electrical signals over a twisted pair or coaxial cable, optical signals over an  
16 optical waveguide, etc.

17  
18 The physical access module 116 is connected to the gateway 118, which interfaces with  
19 the public data network 104. The gateway 118 provides packet processing and other  
20 low-level processing features. For instance, the gateway 118 is capable of recognizing  
21 when a client device (e.g., client device 102) is attempting to access the public data  
22 network 104. The gateway 118 has the capability to respond by redirecting the client  
23 device towards the visited network server 120.

24  
25 In a specific embodiment, the visited network server 120 may be a web server, which  
26 provides the capability of exchanging interactive web content with a connection endpoint  
27 such as the client device 102. The visited network server 120 also has the ability to  
28 instruct the gateway 118 to release (i.e., enable) or abort a session between a client  
29 device (e.g., client device 102) across the public data network 104. The visited network  
30 server 120 also interacts with the visited authentication server 122 by providing to it user  
31 credentials received from various client devices.

32

1 The visited authentication server 122 is adapted to receive such credentials and to  
2 validate them by communicating with authentication servers associated with other access  
3 providers. The configuration of the visited authentication server 122 may be standard  
4 and it may abide by well-known protocols such as the RADIUS protocol. For more  
5 information on usage of the RADIUS protocol by the authentication server 122, the  
6 reader is invited to consult the Internet Engineering Task Force's (IETF) Request for  
7 Comments (RFC) 2865, RFC 2866 and RFCs subsequent thereto.

8

9 Fig. 1B shows portions of a "home" credit provider with which the user of client device  
10 102 has a business relationship. It is assumed that the home credit provider has access to  
11 the public data network 104, e.g., by way of a web server. In an embodiment, the home  
12 credit provider is an access provider which provides internet access to client devices 102  
13 within a specific geographic region, similarly to the visited access provider. This would  
14 be the case, for example, where the home credit provider is a wireless operator.  
15 However, in alternative embodiments, the home credit provider may be a utility (e.g.,  
16 power company, telephone company, gas company), a credit card company, a bank, a  
17 loan agency or any source of verifiable credit that the client device 102 can access via the  
18 public data network 104.

19

20 Generally speaking, the home credit provider comprises a home network server 106 and  
21 a home authentication server 108. For simplicity, communication links between the  
22 home network server 106 and the home authentication server 108 have been omitted  
23 from the drawing. Also for simplicity, gateways linking the home network server 106 to  
24 other access providers (e.g., via the public data network 104) are not shown.

25

26 In a specific example, the home network server 106 may be a web server, capable of  
27 interactively exchanging web content with a connection endpoint. The home network  
28 server 106 is connected to the home authentication server 108, which is responsible for  
29 authenticating users on the basis of received user credentials. In a specific embodiment,  
30 the home authentication server 108 maintains a database 110 of user credentials  
31 associated with each of a plurality of authorized users. For simplicity, the database 110  
32 may be referred to as a "database of authorized users". When user credentials are

1 supplied to the home authentication server 108, the home authentication server 108  
2 attempts to validate the received user credentials by verifying whether they appear in the  
3 database 110 of authorized users. If they do indeed appear in the database 110 of  
4 authorized users, the associated user with these user credentials is said to be successfully  
5 authenticated and if they do not appear in the database 110 of authorized users, no  
6 associated user is successfully authenticated and it is said that authentication has been  
7 unsuccessful.

8  
9 In accordance with an embodiment of the present invention, a functional component  
10 associated with the authentication server 108 is a home translation engine 112. The  
11 home translation engine 112 may be a physical or logical entity and it may be integral  
12 with or separate from the hardware or software of the authentication server 108 or the  
13 home network server 106. In a specific embodiment, the translation engine 112  
14 maintains a database 114 of "substitute" user credentials. The translation engine 112 has  
15 suitable circuitry, software and/or control logic for generating substitute user credentials  
16 associated with received original user credentials. Specifically, when supplied with  
17 original user credentials and prompted to generate substitute user credentials, the  
18 translation engine 112 can either generate arbitrary substitute user credentials or it may  
19 derive the substitute user credentials on the basis of the original user credentials by  
20 performing a particular algorithmic function. The substitute user credentials are then  
21 stored in the database 114. Another role of the translation engine 112 is to verify  
22 whether a given set of received substitute credentials appears in the database 114.

23  
24 The process of controlling access by the client device 102 to the public data network 104  
25 can best be described as a sequence of message streams with reference to Fig. 1A, Figs.  
26 1C-1F and Fig. 2. The message streams represent a logical flow of information. When  
27 the flow of information involves entities operated by the same access provider, this is  
28 illustrated by solid arrows; where the flow of information involves entities operated by  
29 different access providers, this is indicated by dashed arrows.

30  
31 To begin, the client device 102 sends a message stream 12 in an attempt to access the  
32 public data network 104. The message stream 12 is received at the gateway 118 through  
33 the physical access module 116. In a non-limiting example, the message stream 12 may

1 identify the location of a web page (e.g., by way of an IP address) that the user wishes to  
2 access. The IP address of the web page may be supplied in response to a DNS query  
3 following text entry of a web page in a web browser operating as a graphical user  
4 interface. Alternatively, in another non-limiting example, the browser operating on the  
5 client device 102 can be pre-programmed to attempt to access a default home page. In  
6 yet other instances, the browser could simply send a message to the gateway 118  
7 indicative that the client device 102 is attempting to access the public data network 104,  
8 without necessarily specifying any given web address. It should also be understood that  
9 graphical user interfaces other than web browsers are within the scope of the present  
10 invention.

11  
12 Upon recognizing the attempt of the client device 102 to access the public data network  
13 104, the gateway 118 sends a message stream 14 to the client device 102 redirecting it to  
14 the visited network server 120. In a non-limiting example embodiment, this can be done  
15 by way of an HTTP redirect which supplies an address of the visited network server 120.  
16 Thus, a new message stream 16 begins to be exchanged between the client device 102  
17 and the visited network server 120. In a specific embodiment, the visited network server  
18 120 is a web server. Thus, the message stream 16 causes a login web page 123 to be  
19 displayed on the client device 102 and interactive exchange of web content takes place  
20 between the two end points of the connection, namely the client device 102 and the  
21 visited web server 120. In a specific example embodiment of the login web page 123,  
22 there is provided an array of buttons representative of various candidate credit providers.  
23 If roaming is to successfully take place, the candidate credit providers should include the  
24 user's home credit provider. The user is prompted to select his or her home credit  
25 provider and this may be done in a variety of ways including but not limited to pushing  
26 one of the buttons using a mouse or stylus, the typing of a realm from a keyboard or the  
27 selection of a menu item with a digital pen. Other selection techniques will be known to  
28 those of ordinary skill in the art.

29  
30 At this point, the user is assumed to have identified a credit provider, hereinafter referred  
31 to as the user-selected credit provider. It is noted that the user-selected credit provider  
32 may not always be the home credit provider for the user in question, especially when the  
33 user's intentions are malicious. With reference now to Fig. 1C, the visited network

1 server 120, upon receipt of the user's identification of a credit provider, now directs the  
2 client device 102 to a network server 124 in the user-selected credit provider, thus  
3 establishing a connection between these two entities. In the specific embodiment where  
4 the network server 124 is a web server, the connection carries a message stream 18 that  
5 causes a web page 136 to be displayed on the client device 102, followed by interactive  
6 exchange of information between the two end points of the connection, namely the client  
7 device 102 and the web server 124 operated by the user-selected credit provider.

8  
9 The message stream 18 allows the user (by way of the client device 102) to supply  
10 original user credentials 134 to the network server 124 of the user-selected credit  
11 provider. For example, the original user credentials 134 may comprise a username, a  
12 realm and a password, although various other formats for the original user credentials  
13 will be known to those of ordinary skill in the art. In a specific case, the original user  
14 credentials may be entered on the web page 136 as "jsmith@network.com" with a  
15 corresponding password, where "jsmith" is known as the username and "network.com"  
16 is known as the realm. In another embodiment, the original user credentials 134  
17 comprise an account number (e.g., based on address, home telephone number, driver's  
18 license, etc.) and a password. In still other embodiments, the original user credentials  
19 134 comprise a bank account number and a personal identification number. In yet  
20 another embodiment, the original user credentials 134 comprise a credit card number and  
21 an expiry date or, alternatively, a cardholder name and a credit card number and  
22 optionally the expiry date.

23  
24 While in some embodiments, the original user credentials 134 are entered by the user, in  
25 other embodiments, the original user credentials 134 may be supplied to the network  
26 server 124 with little or no intervention from the user. For example, by enabling a  
27 memory feature in the browser, the original user credentials 134 may be submitted to the  
28 network server 124 upon mere confirmation by the user by a single action, such as the  
29 click of a mouse or the stroke of a key or the touch of a finger or stylus, etc. In other  
30 instances, the browser operating on the client device 102 may be programmed to enter  
31 predetermined original user credentials 134 without any input from the user.

32

1 It is noted that the connection between the client device 102 and the network server 124  
2 may physically pass through the physical access module 116, the gateway 118, the public  
3 data network 104 and, most typically, a gateway (not shown) operated by the user-  
4 selected credit provider. Advantageously, the client device 102 and the network server  
5 124 of the user-selected credit provider can cooperate to make the message stream 18  
6 secure and, in particular, impenetrable by the visited network server 120. In other words,  
7 the integrity of the original user credentials 134 supplied by the client device 102 to the  
8 network server 124 of the user-selected credit provider can be safeguarded. An example  
9 of a secure connection, not to be construed as a limiting example, is an SSL (secure  
10 socket layer) connection.

11

12 Reference is now made to Fig. 1D, which shows the steps in a procedure performed at  
13 the network server 124 of the user-selected credit provider upon receipt of the original  
14 user credentials 134. As previously mentioned, the access provider identified by the user  
15 may or may not be the home network server 106. Accordingly, to keep the discussion as  
16 general as possible, the network server 124 is shown as communicating with a generic  
17 authentication server 126 (not necessarily the home authentication server 108), which in  
18 turn is associated with a generic translation engine 128 (not necessarily the home  
19 translation engine 112). The authentication server has access to a database 130 of  
20 authorized users (not necessarily the database 110 of authorized users) and the translation  
21 engine 128 has access to a database 132 (not necessarily database 114). The network  
22 server 124, authentication server 126, translation engine 128, database 130 of authorized  
23 users and database 132 mirror similar entities in the home credit provider and, in fact,  
24 will correspond to those entities when the user-selected credit provider is the home credit  
25 provider for the user in question.

26

27 A first step in the procedure is for the network server 124 to establish a message stream  
28 20 with the authentication server 126 in order to communicate the original user  
29 credentials 134 in an initial authentication phase. Upon receipt of the original user  
30 credentials 134, the authentication server 126 consults its database 130 of authorized  
31 users in an attempt to locate the original user credentials 134. If, indeed, the original  
32 user credentials 134 are found in the database 130 of authorized users, then the  
33 authentication server 126 will deem the authentication to have been successful. At this

1 point, the authentication server 126 provides the original user credentials to the  
2 translation engine 128 and commands it to generate substitute user credentials. This  
3 command is represented by message stream 22. The translation engine 128 responds by  
4 generating a set of substitute user credentials 138 and storing them in the database 132  
5 for future reference as will be seen from the discussion to follow. Message stream 24  
6 represents the return of the substitute user credentials 138 to the network server 124.

7  
8 It is to be noted that the substitute user credentials 138 may or may not be in a format  
9 resembling the original user credentials 134. For example, the substitute user credentials  
10 138 may also comprise a different username, the same realm as the original user  
11 credentials and a different password. In another example, the substitute user credentials  
12 138 may comprise an alphanumeric string that is derived from the username and  
13 password of the original user credentials 134, as well as an indication of the user-selected  
14 credit provider, but no password. In a further example, the substitute user credentials  
15 138 may include an alphanumeric string and a realm indicative of the fact that the  
16 credentials are substitute in nature. This may be useful for corporate entities having  
17 subscribers from multiple realms and wishing to enable seamless roaming to users from  
18 all such realms by providing a common realm used for the specific purposes of  
19 authenticating subscribers. In yet another example, the substitute user credentials 138  
20 may include an alphanumeric string, an indication of the user-selected credit provider  
21 and an indication as to whether authentication was performed or whether it was  
22 successful. In still another example, the substitute user credentials 138 may take on a  
23 random value that is uncorrelated with the original user credentials 134, in addition to an  
24 indication of the user-selected credit provider. In many cases, it will be desirable to  
25 ensure that the original user credentials 134 are indecipherable from the substitute user  
26 credentials 138.

27  
28 Reference is now made to Fig. 1E, which represents the occurrence of events after the  
29 network server 124 receives the substitute credentials 138 from the translation engine  
30 128. The network server 124 operated by the user-selected credit provider sends to the  
31 client device 102 the substitute user credentials 138 as part of a message stream 26,  
32 which is in fact carried along the same connection as the message stream 18. In a  
33 specific non-limiting example, the substitute user credentials 138 may be forwarded as a

1 cookie or as URL parameters. (It is noted that for authorized users, the network server  
2 124 of the user-selected credit provider will correspond to the home network server 106).

3

4 As represented by message stream 28, the client device 102 then forwards the substitute  
5 user credentials 138 to the visited network server 120. It should be noted that the  
6 substitute user credentials 138 may or may not be made visible to the user of the client  
7 device 102 prior to their transmission to the visited network server 120. In other words,  
8 it is within the scope of the invention for the substitute user credentials 138 to be  
9 forwarded automatically to the visited network server 120 upon receipt from the network  
10 server 124 in a transparent fashion, i.e., without requiring user input. This can be  
11 achieved using standard parameter passing between web pages 123 and 136. The  
12 transparent transmission of the substitute user credentials 138 to the visited network  
13 server 120 increases convenience from the user's point of view since no additional data  
14 entry by the user is required.

15

16 Upon receipt of the substitute user credentials 138 at the visited network server 120, an  
17 authentication procedure is initiated. In one implementation, the visited network server  
18 120 provides a message stream 30 to the visited authentication server 122, where the  
19 message stream 30 contains the substitute user credentials 138. By way of non-limiting  
20 example embodiment, the message stream 30 may take the form of a RADIUS  
21 authentication request. Other standards-based and proprietary messages are within the  
22 scope of the present invention. In an alternative implementation, the message stream 30  
23 actually passes through the gateway 118 on its way from the visited network server 120  
24 to the visited authentication server 122. In this alternative implementation, the gateway  
25 118 is responsible for originating a RADIUS authentication request (or other standards-  
26 based or proprietary message) to the visited authentication server 122.

27

28 In response, the visited authentication server 122 initiates an authentication request with  
29 the authentication server 126 of the user-selected credit provider. The authentication  
30 server 122 knows that it needs to access the authentication server 126 based on a  
31 parameter of the substitute user credentials 138, such as the realm. It is assumed that the  
32 visited access provider and the user-selected credit provider have an already existing  
33 roaming relationship, including authentication server peering. In an example, this would

1 allow the visited access provider to bill the home credit provider for the use of its  
2 network. This translates into roaming charges on the user's bill. The initiation of the  
3 authentication request with the authentication server 126 is represented by a message  
4 stream 32.

5  
6 Upon receipt of the substitute user credentials at the authentication server 126, the  
7 authentication server 126 recognizes that the credentials being passed to it are substitute  
8 in nature. Myriad ways exist in order to allow the authentication server 126 to recognize  
9 that the credentials it has received are substitute in nature. For example, as indicated  
10 above, the realm forming part of the substitute user credentials 138 may identify the  
11 substitute nature of the credentials. Specifically, in the illustrated example, the realm  
12 "aaa.network.com" can provide a clear indication to the authentication server 128 in the  
13 "network.com" realm that the credentials being received are substitute user credentials.

14  
15 In an example implementation, upon receipt of the substitute user credentials 138, the  
16 authentication server 126 forwards these to the translation engine 128 in the form of  
17 message stream 24. The translation engine 128 searches for the substitute user  
18 credentials 138 in its database 132 of previously authenticated users. In this  
19 embodiment, the substitute user credentials 138 are assumed to have been previously  
20 generated as a result of successful authentication of the user on the basis of the original  
21 user credentials. Therefore, the database 132 is guaranteed to contain the substitute user  
22 credentials 138 and thus a match is guaranteed to be found. This allows the visited  
23 authentication server 122 and the authentication server 126 to agree on the financial and  
24 other terms pertaining to the roaming operation. The authentication server 126  
25 subsequently issues a message stream 36 which provides the visited authentication server  
26 122 with an indication that the authentication has been successful. Assuming such to be  
27 the case, the message stream 36 may take the form of a RADIUS authentication accept  
28 message, for example.

29  
30 Reference is now made to Fig. 1F, which assumes that successful authentication of the  
31 client device 102 on the basis of the substitute user credentials 138 has taken place. A  
32 message stream 38 represents the visited authentication server 122 informing the  
33 gateway 118, either directly or via the network server 120 (depending on the particular

1 implementation) that the client device 102 can be allowed to access the public data  
2 network 104. In a specific embodiment, this can be effected by way of a  
3 standards0based (XML, etc.) or proprietary "Session Release" command, resulting in a  
4 connection 40 between the client device 102 and desired locations in the public data  
5 network 104. The visited authentication server 122 now monitors the status of the user's  
6 connection 40 and is informed of its termination by the gateway 118. In a specific  
7 example, the gateway 118 transmits to the visited authentication server 122 accounting  
8 messages 42 (e.g., RADIUS messages such as Start, Interim and Stop), which are then  
9 processed by the visited authentication server 122 and communicated, as appropriate, to  
10 the authentication server 126 (which is actually the home authentication server 108, since  
11 authentication was successful).

12  
13 From the above, it will be appreciated the connection between the client device 102 and  
14 the network server 124 of the user-selected credit provider allow the client device 102 to  
15 communicate its original user credentials securely with the user-selected credit provider,  
16 typically the home credit provider. Thus, the nature of the connection that supports the  
17 message streams 18, 26 is temporary, and its duration or flow characteristics (e.g.,  
18 number of bytes of information exchanged) may be monitored by the gateway 118 and/or  
19 the visited network server 120. If the duration or traffic flow exceeds certain pre-set  
20 parameters, the gateway 118 or the visited network server 120 may terminate the  
21 connection. Such an action may be taken in order to prevent abuse of the temporary  
22 connection by the end user 102 in conspiracy with the home credit provider to escape  
23 roaming charges.

24  
25 Also, the above has mostly considered the case where authentication of the client device  
26 102 by the authentication server 126 in the user-selected credit provider was successful,  
27 which implies that the user-selected credit provider is the home credit provider.  
28 However, unsuccessful authentication is possible, e.g., in those cases where the user-  
29 selected credit provider is not the home credit provider. Unsuccessful authentication is  
30 detected by the authentication server 126. In response, the authentication server 126 may  
31 deny access immediately or may allow the client device 102 one or more additional  
32 chances to enter a new set of original user credentials 134 before truly denying access.

33

1 Those skilled in the art will appreciate that variations of the above sequence of events  
2 may be made without departing from the scope of the present invention. For example, in  
3 one specific variant, upon receipt of the original user credentials 134 via message stream  
4 18, the network server 124 does not forward the original user credentials 124 to the  
5 authentication server 126 for authentication. Rather, the network server 124 provides the  
6 original user credentials 134 directly to the translation engine 128, bypassing the  
7 authentication server 126 altogether. This causes the translation engine 128 to generate  
8 the substitute user credentials 138 without regard to whether the original user credentials  
9 134 are valid or not. Under this variant, the substitute user credentials 138 are stored in  
10 the database 132 in association with the original user credentials 134, for later  
11 authentication of the client device 102. It is noted that under this variant, message  
12 streams 20 and 22 are eliminated and message stream 24 (between the network server  
13 124 and the translation engine 128) becomes bi-directional.

14  
15 Upon receipt of the substitute user credentials 138 via message stream 32, the  
16 authentication server 126 forwards these to the translation engine 128, which searches  
17 for the substitute user credentials 138 in the database. Recall that the substitute user  
18 credentials 138 are assumed to have been previously generated regardless of whether  
19 authentication of the user on the basis of the original user credentials would have been  
20 successful or unsuccessful. Therefore, the database 132 is guaranteed to contain the  
21 substitute user credentials 138 and, moreover, a corresponding set of original user  
22 credentials 134 will be found. By consulting the database 132, the translation engine 128  
23 thus obtains the original user credentials 134 associated with the substitute user  
24 credentials 138. The translation engine 128 then provides, via message stream 34, the  
25 original user credentials 134 to the authentication server 126 for authentication. At this  
26 stage, the authentication server 126, for the first time, validates the original user  
27 credentials 134 by consulting the database 130 of authorized users. Assuming that  
28 authentication is successful, the visited authentication server 122 and the authentication  
29 server 126 agree on the financial and other terms pertaining to the roaming operation. If  
30 the authentication is unsuccessful, the authentication server 126 may deny access  
31 immediately or may allow the client device 102 one or more additional chances to enter a  
32 new set of original user credentials 134 before truly denying access.

33

1 Those skilled in the art will also appreciate that the authentication server 126 and the  
2 translation engine 128 may be separate entities, each with access to their own separate,  
3 respective databases 130, 132. On the other hand, the authentication server 126 and the  
4 translation engine 128 may constitute a single entity, with a single database that includes  
5 both original and substitute user credentials for each authorized user. Treating the  
6 authentication server 126 and the translation engine 128 as separate entities may be  
7 advantageous in a business environment where the authentication server 126 belongs to a  
8 corporate entity different from the translation engine 128. Specifically, consider the case  
9 where multiple access providers rely on a common, trustworthy, third-party  
10 "clearinghouse". Under such a business model, the clearinghouse provides original-to-  
11 substitute and substitute-to-original user credential translation services for various access  
12 providers. Whenever a given credit provider receives original user credentials, these are  
13 sent to the clearinghouse for translation into substitute user credentials, possibly by  
14 selection from amongst a pool of substitute (i.e., temporary) credentials. Conversely,  
15 when a given credit provider needs to authenticate a user on the basis of substitute user  
16 credentials, these are sent to the clearinghouse, which returns the original user  
17 credentials, if they exist.

18

19 Moreover, those skilled in the art will appreciate that a credit provider may, at the same  
20 time, act as a home credit provider with respect to a first user, a visited access provider  
21 with respect to a second user, and a user-selected credit provider with respect to a third  
22 user. Thus, when the credit provider also acts as an access provider, it will be  
23 understood that the designation of a particular access provider as "home", "visited" or  
24 "user-selected" will change, depending on the user in question being authenticated.  
25 Thus, the term "home", "visited" or "user-selected" is not intended to designate a  
26 particular "type" of access provider, rather a role of the access provider in relation to the  
27 user whose credentials are being authenticated.

28

29 Those skilled in the art will further appreciate that the gateway 118, the visited network  
30 server 120 and the visited authentication server 122 represent logically separate  
31 functions, but not necessarily separate physical devices, i.e., any combination of these  
32 logical functions could be performed by a single physical device. Likewise, the network  
33 server 124, the authentication server 126 and the translation engine 128 represent

1 logically separate functions, but not necessarily separate physical devices, i.e., any  
2 combination of these logical functions could be performed by a single physical device.  
3 Similarly, the home network server 106, the home authentication server and the home  
4 translation engine 112 represent logically separate functions, but not necessarily separate  
5 physical devices, i.e., any combination of these logical functions could be performed by  
6 a single physical device.

7  
8 Also, it should be appreciated that the HTTP (hypertext transfer protocol) redirection  
9 mechanism described herein above is not to be construed as a limitation of the present  
10 invention. Other ways of redirecting the client device 102 to a different location than the  
11 one initially sought are within the scope of the invention and may be based on protocols  
12 such as FTP (file transfer protocol), IP sec, SMTP (simple mail transfer protocol), etc.

13  
14 Those skilled in the art will also appreciate that in some embodiments, the functionality  
15 of the network servers 106, 120, 124, authentication servers 108, 122, 126, gateway 118  
16 and translation engines 112, 128 may be implemented as pre-programmed hardware or  
17 firmware elements (e.g., application specific integrated circuits (ASICs), electrically  
18 erasable programmable read-only memories (EEPROMs), etc.), or other related  
19 components. In other embodiments, the above entities may be implemented as an  
20 arithmetic and logic unit (ALU) having access to a code memory (not shown) which  
21 stores program instructions for the operation of the ALU. The program instructions  
22 could be stored on a medium which is fixed, tangible and readable directly by the entity  
23 in question, (e.g., removable diskette, CD-ROM, ROM, or fixed disk), or the program  
24 instructions could be stored remotely but transmittable to the entity in question via a  
25 modem or other interface device (e.g., a communications adapter) connected to a  
26 network over a transmission medium. The transmission medium may be either a  
27 tangible medium (e.g., optical or analog communications lines) or a medium  
28 implemented using wireless techniques (e.g., microwave, infrared or other transmission  
29 schemes).

30  
31 While specific embodiments of the present invention have been described and illustrated,  
32 it will be apparent to those skilled in the art that numerous modifications and variations

- 1 can be made without departing from the scope of the invention as defined in the
- 2 appended claims.
- 3

1    **WHAT IS CLAIMED IS:**

2

3    1. A method of controlling access to a data network from a visited access provider,  
4       comprising

5       - receiving from a client device a message indicative of a request to access the data  
6       network;

7       - supporting a temporary connection between the client device and a credit  
8       provider, the temporary connection comprising a transmission of substitute user  
9       credentials from the credit provider in response to transmission of original user  
10      credentials from the client device;

11      - receiving the substitute user credentials from the client device;

12      - communicating the substitute user credentials to the credit provider to  
13      authenticate the client device;

14      - responsive to successful authentication of the client device by the credit provider  
15      on the basis of the substitute user credentials, authorizing the client device to  
16      access the data network;

17      - wherein the temporary connection is secured to prevent the visited access  
18      provider from determining the original user credentials transmitted by the client  
19      device.

20

21    2. The method defined in claim 1, wherein receiving from the client device the message  
22      indicative of the request to access the data network comprises receiving an identity of  
23      a Web page attempted to be accessed by a browser on the client device.

24

25    3. The method defined in claim 1, further comprising, prior to supporting:

26      - identifying to the client device at least one candidate credit provider including  
27      said credit provider.

28

29    4. The method defined in claim 3, wherein supporting is performed responsive to  
30      receipt from the client device of data indicative of a selected one of the at least one  
31      candidate credit provider.

32

- 1 5. The method defined in claim 1, wherein supporting is performed responsive to  
2 receipt from the client device of data indicative of the credit provider.  
3
- 4 6. The method defined in claim 5, further comprising:  
5 - causing the client device to establish the temporary connection with the credit  
6 provider.  
7
- 8 7. The method defined in claim 5, further comprising:  
9 - causing the client device to establish the temporary connection with the credit  
10 provider over the data network.  
11
- 12 8. The method defined in claim 7, wherein causing the client device to establish the  
13 temporary connection with the credit provider over the data network comprises  
14 redirecting the client device to an Internet Protocol (IP) address associated with the  
15 credit provider.  
16
- 17 9. The method defined in claim 7, further comprising:  
18 - terminating the temporary connection after transmission of a pre-determined  
19 amount of data over the temporary connection.  
20
- 21 10. The method defined in claim 7, further comprising:  
22 - terminating the temporary connection after a pre-determined duration.  
23
- 24 11. The method defined in claim 7, further comprising:  
25 - responsive to unsuccessful authentication of the client device by the credit  
26 provider on the basis of the substitute credentials, communicating to the client  
27 device an indication of the unsuccessful authentication.  
28
- 29 12. The method defined in claim 11, wherein the original user credentials comprise a  
30 user name, a realm and a password.  
31
- 32 13. The method defined in claim 11, wherein the original user credentials comprise a  
33 user name and a credit card number.

1

2 14. The method defined in claim 11, wherein the original user credentials comprise an  
3 account number and a personal identification number.

4

5 15. The method defined in claim 11, wherein the substitute user credentials comprise a  
6 user name and a realm.

7

8 16. The method defined in claim 15, wherein the original user credentials are  
9 characterized by being indecipherable from the substitute user credentials.

10

11 17. A network, comprising:

- 12 - a network server entity adapted to receive from a client device a message  
13 indicative of a credit provider;
- 14 - a gateway entity adapted to support a temporary connection between the client  
15 device and the credit provider via the network server entity, the temporary  
16 connection comprising a transmission of substitute user credentials from the  
17 credit provider in response to transmission of original user credentials from the  
18 client device, the temporary connection being secured to prevent the network  
19 server entity from determining the original user credentials transmitted by the  
20 client device;
- 21 - the network server entity being further adapted to receive the substitute user  
22 credentials from the client device;
- 23 - an authentication entity adapted to communicate the substitute user credentials to  
24 the credit provider to authenticate the client device;
- 25 - the network server entity being further adapted to authorize the client device to  
26 access the data network in response to successful authentication of the client  
27 device by the credit provider on the basis of the substitute user credentials.

28

29 18. The network defined in claim 17, wherein the network server entity is a web server.

30

31 19. A network, comprising:

- 32 - server means for receiving from a client device a message indicative of a credit  
33 provider;

- 1       - means for supporting a temporary connection between the client device and the
- 2       credit provider via the server means, the temporary connection comprising a
- 3       transmission of substitute user credentials from the credit provider in response to
- 4       transmission of original user credentials from the client device, the temporary
- 5       connection being secured to prevent the server means from determining the
- 6       original user credentials transmitted by the client device;
- 7       - means for receiving the substitute user credentials from the client device;
- 8       - means for communicating the substitute user credentials to the credit provider to
- 9       authenticate the client device;
- 10      - means for authorizing the client device to access the data network in response to
- 11      successful authentication of the client device by the credit provider on the basis
- 12      of the substitute user credentials.

13

14   20. A method of authenticating users having a business relationship with a credit

15   provider, comprising:

- 16      - receiving original user credentials from a client device over a temporary
- 17      connection that passes through a visited provider of access to a data network, the
- 18      temporary connection being secured to prevent the visited provider of access
- 19      from determining the original user credentials transmitted by the client device;
- 20      - sending substitute user credentials to the client device over the temporary
- 21      connection, the substitute user credentials being associated with the original user
- 22      credentials;
- 23      - receiving the substitute user credentials from the visited provider of access;
- 24      - authenticating the client device on the basis of the substitute user credentials;
- 25      - responsive to successful authentication of the client device on the basis of the
- 26      substitute user credentials, indicating to the visited provider of access to the data
- 27      network that the client device has been successfully authenticated.

28

29   21. The method defined in claim **20**, wherein receiving the original user credentials from

30   the client device is effected over the data network.

31

32   22. The method defined in claim **21**, wherein receiving the original user credentials is

33   effected via the visited provider of access to the data network.

- 1
- 2 23. The method defined in claim **20**, further comprising, between receiving the original
- 3 user credentials and sending the substitute user credentials:
- 4 - generating the substitute credentials.
- 5
- 6 24. The method defined in claim **23**, further comprising:
- 7 - storing the substitute user credentials in a database in association with the
- 8 original user credentials.
- 9
- 10 25. The method defined in claim **24**, wherein authenticating the client device on the basis
- 11 of the substitute user credentials comprises accessing the database, wherein the client
- 12 device is said to be successfully authenticated on the basis of the substitute user
- 13 credentials if the substitute user credentials are contained in the database.
- 14
- 15 26. The method defined in claim **25**, further comprising, between receiving the original
- 16 user credentials and sending the substitute user credentials:
- 17 - authenticating the client device on the basis of the original user credentials.
- 18
- 19 27. The method defined in claim **26**, wherein authenticating the client device on the basis
- 20 of the original user credentials comprises accessing a database of authorized users,
- 21 wherein the client device is said to be successfully authenticated on the basis of the
- 22 original user credentials if the original user credentials are contained in the database
- 23 of authorized users.
- 24
- 25 28. The method defined in claim **27**, wherein generating the substitute credentials is
- 26 performed in response to successful authentication of the client device on the basis of
- 27 the original user credentials.
- 28
- 29 29. The method defined in claim **23**, wherein the original user credentials comprise a
- 30 user name, a realm and a password.
- 31
- 32 30. The method defined in claim **23**, wherein the original user credentials comprise a
- 33 user name and a credit card number.

1

2 31. The method defined in claim 23, wherein the original user credentials comprise an  
3 account number and a personal identification number.

4

5 32. The method defined in claim 23, wherein generating the substitute user credentials  
6 comprises deriving the substitute credentials from the original user credentials.

7

8 33. The method defined in claim 23, wherein the substitute user credentials comprise  
9 data indicative of the substitute nature of the substitute user credentials.

10

11 34. The method defined in claim 29, wherein the substitute user credentials comprise  
12 data indicative of a realm different from the realm indicated by the original user  
13 credentials.

14

15 35. A credit provider having a business relationship with a plurality of users, comprising:

- 16 - a network server entity adapted to:
- 17 - receive original user credentials from a client device over a temporary  
18 connection that passes through a visited provider of network access, the  
19 temporary connection being secured to prevent the visited provider of  
20 network access from determining the original user credentials transmitted by  
21 the client device;
- 22 - send substitute user credentials to the client device over the temporary  
23 connection, the substitute user credentials being associated with the original  
24 user credentials;
- 25 - an authentication entity adapted to:
- 26 - receive the substitute user credentials from the visited provider of network  
27 access;
- 28 - authenticate the client device on the basis of the substitute user credentials;
- 29 - indicate to the visited provider of network access that the client device has  
30 been successfully authenticated in response to successful authentication of the  
31 client device on the basis of the substitute user credentials.

32

33 36. A credit provider having a business relationship with a plurality of users, comprising:

- 1       - means for receiving original user credentials from a client device over a
- 2       temporary connection that passes through a visited provider of access to a data
- 3       network, the temporary connection being secured to prevent the visited provider
- 4       of access from determining the original user credentials transmitted by the client
- 5       device;
- 6       - means for sending substitute user credentials to the client device over the
- 7       temporary connection, the substitute user credentials being associated with the
- 8       original user credentials;
- 9       - means for receiving the substitute user credentials from the visited provider of
- 10      access;
- 11      - means for authenticating the client device on the basis of the substitute user
- 12      credentials;
- 13      - means for responsive to successful authentication of the client device on the basis
- 14      of the substitute user credentials, indicating to the visited provider of access to
- 15      the data network that the client device has been successfully authenticated.

16

17   37. A method of accessing a data network from a region of service operated by a visited  
18   access provider, comprising

- 19      - supplying to the visited access provider an identity of a credit provider;
- 20      - establishing a temporary connection with the credit provider;
- 21      - receiving substitute user credentials from the credit provider during the
- 22      temporary connection in response to supplying the credit provider with original
- 23      user credentials provider during the temporary connection;
- 24      - supplying the substitute user credentials to the visited access provider for
- 25      authentication of the client device by the credit provider on the basis of the
- 26      substitute user credentials;
- 27      - wherein the temporary connection is secured to prevent the visited access
- 28      provider from determining the original user credentials supplied to the credit
- 29      provider.

30

31   38. A method defined in claim 37, wherein supplying the substitute user credentials to  
32   the visited access provider is performed automatically in response to receiving the  
33   substitute user credentials from the credit provider.

1

2 39. A method defined in claim 37, wherein supplying the substitute user credentials to  
3 the visited access provider is performed without requiring user input after receiving  
4 the substitute user credentials from the credit provider.

5

6 40. The method defined in claim 37, further comprising:

7 - accessing the data network via the visited access provider in response to  
8 successful authentication of the client device on the basis of the substitute user  
9 credentials.

10

11 41. The method defined in claim 40, further comprising, prior to supplying to the visited  
12 access provider the identity of the credit provider:

13 - receiving from the visited network provider an identity of at least one candidate  
14 credit provider including the credit provider.

15

16 42. The method defined in claim 41, further comprising:

17 - selecting the credit provider from among the at least one candidate credit provider  
18 identified whose identity is received from the visited network provider.

19

20 43. The method defined in claim 40, wherein the temporary connection is established  
21 over the data network.

22

23 44. The method defined in claim 43, wherein the temporary connection is established via  
24 the visited access provider.

25

26 45. The method defined in claim 44, wherein data sent to a home network during the  
27 temporary connection is encrypted at the client device and decrypted at the credit  
28 provider.

29

30 46. The method defined in claim 45, wherein data sent from the home network during the  
31 temporary connection is encrypted at the credit provider and decrypted at the client  
32 device.

33

1 47. The method defined in claim 37, wherein the temporary connection is a secure socket  
2 layer connection.

3

4 48. The method defined in claim 37, wherein establishing the temporary connection with  
5 the credit provider comprises receiving an Internet Protocol address of the credit  
6 provider from the visited access provider and accessing the Internet Protocol address  
7 via the Internet.

8

9 49. Apparatus for accessing a data network from a region of service operated by a visited  
10 access provider, comprising

- 11 - means for supplying to the visited access provider an identity of a credit provider;
- 12 - means for establishing a temporary connection with the credit provider;
- 13 - means for receiving substitute user credentials from the credit provider during the
- 14 temporary connection in response to supplying the credit provider with original
- 15 user credentials provider during the temporary connection;
- 16 - means for supplying the substitute user credentials to the visited access provider
- 17 for authentication of the client device by the credit provider on the basis of the
- 18 substitute user credentials;
- 19 - wherein the temporary connection is secured to prevent the visited access
- 20 provider from determining the original user credentials supplied to the credit
- 21 provider.

22

23 50. A graphical user interface for guiding a user through a process of accessing a data  
24 network from a region of service operated by a visited access provider, comprising:

- 25 - a browser capable of interfacing with a user;
- 26 - a control entity operative to:
  - 27 - output via the browser content from the visited access provider;
  - 28 - responsive to identification via the browser of a credit provider, output via the
  - 29 browser content from the credit provider, said content from the credit
  - 30 provider being inaccessible by the visited access provider;
  - 31 - responsive to identification via the browser of user credentials of a particular
  - 32 user having a business relationship with the credit provider, access content of
  - 33 user-selected locations on the data network.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32

51. The graphical user interface defined in claim 50, wherein the content from the visited access provider includes a text entry area for identification of the credit provider.
52. The graphical user interface defined in claim 50, wherein the content from the visited access provider includes a choice of at least one candidate credit provider allowing selective identification of the credit provider.
53. The graphical user interface defined in claim 50, wherein the content from the credit provider includes a text entry area for identification of the user credentials.
54. The graphical user interface defined in claim 51, wherein the content from the credit provider includes a text entry area for identification of the user credentials.
55. The graphical user interface defined in claim 52, wherein the content from the credit provider includes a text entry area for identification of the user credentials.
56. A computer program product for use with a client device in accessing a data network from a region of service operated by a visited access provider, the computer program product comprising a computer usable medium having computer readable program code thereon, the computer readable program code including:
- program code for implementing a browser to interface with a user;
  - program code for outputting via the browser content from the visited access provider;
  - program code for outputting via the browser content from a credit provider in response to receiving via the browser an identification of the credit provider, said content from the credit provider being inaccessible by the visited access provider;
  - program code for accessing via the browser content of user-selected locations on the data network in response to receiving via the browser an identification of user credentials of a particular user having a business relationship with the credit provider.

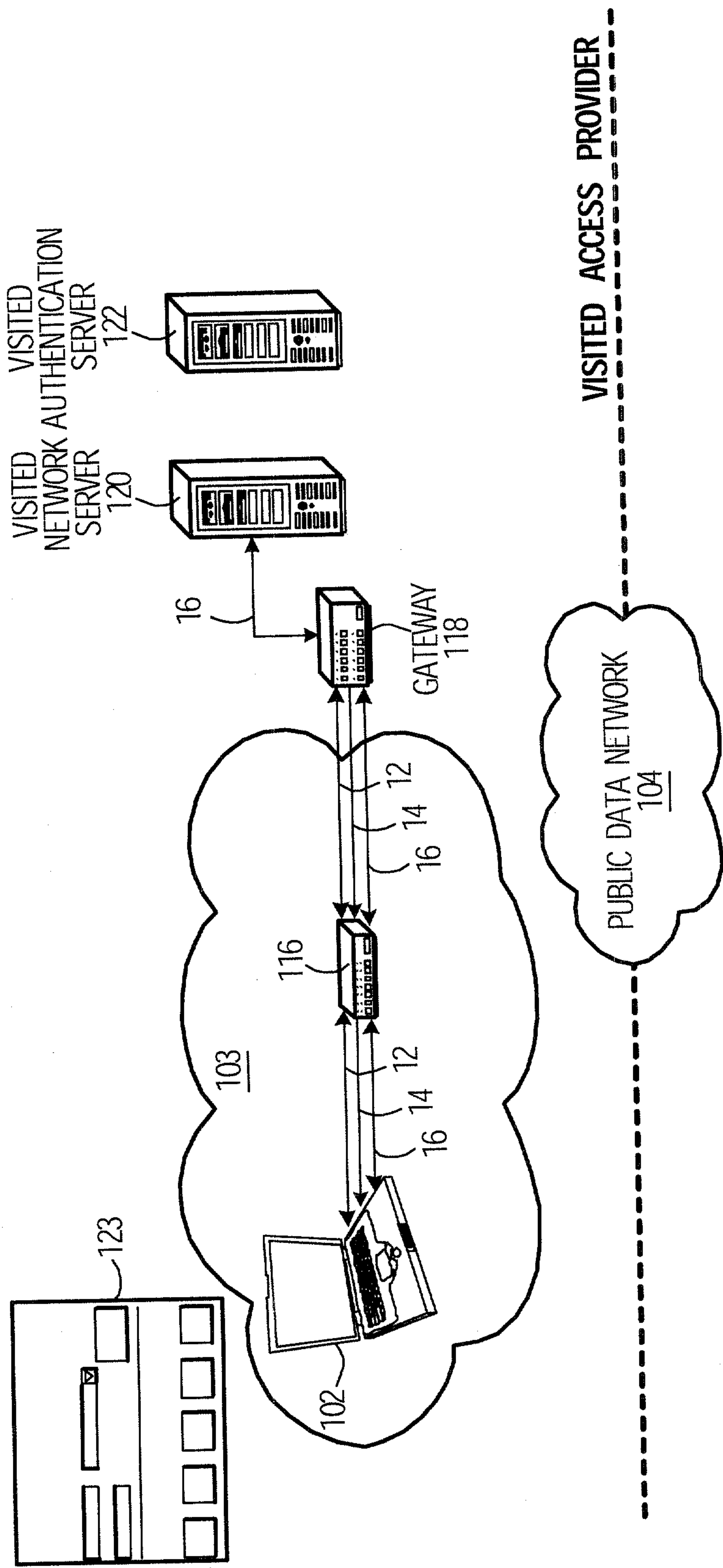


FIG. 1A

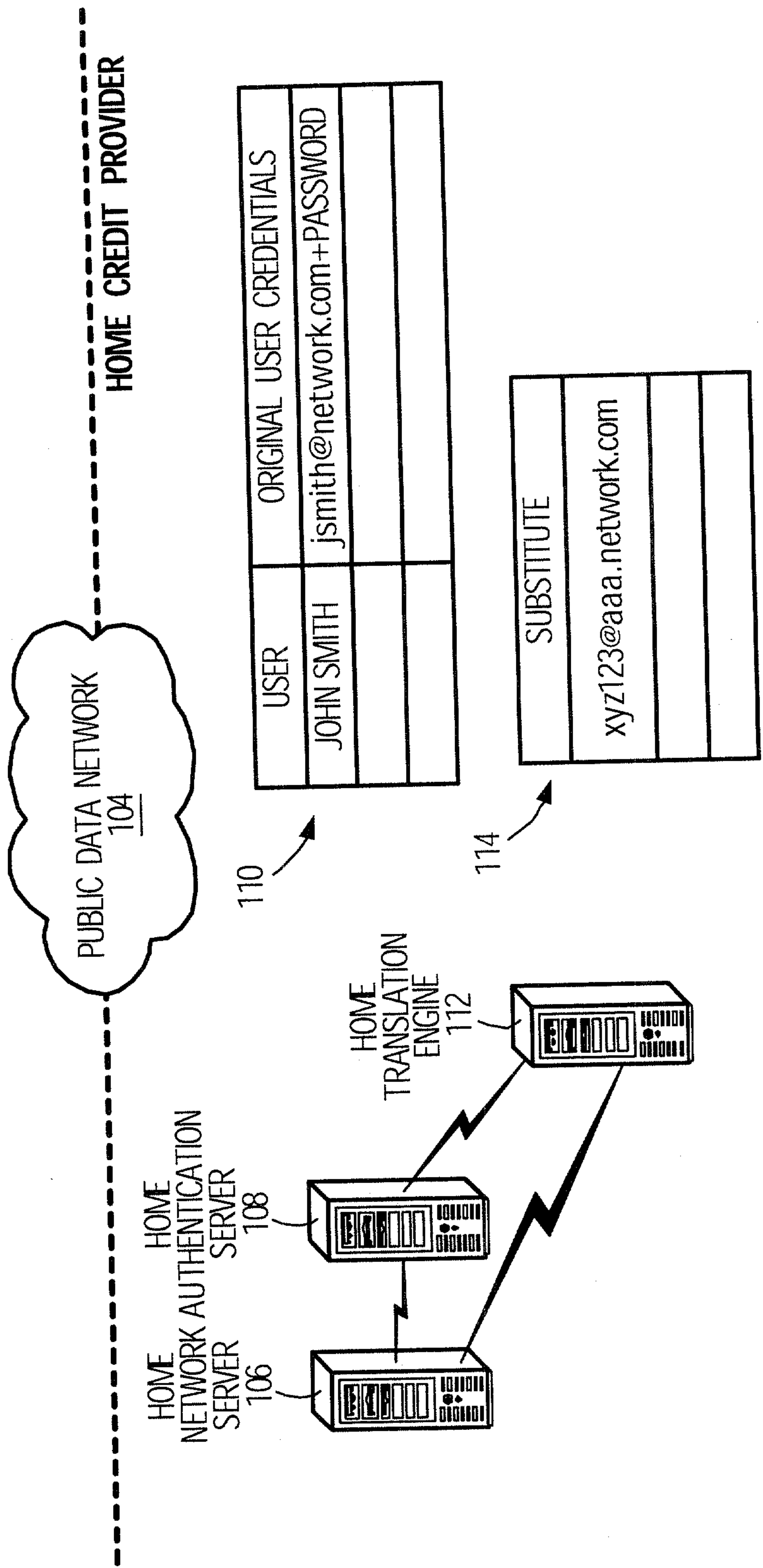


FIG. 1B

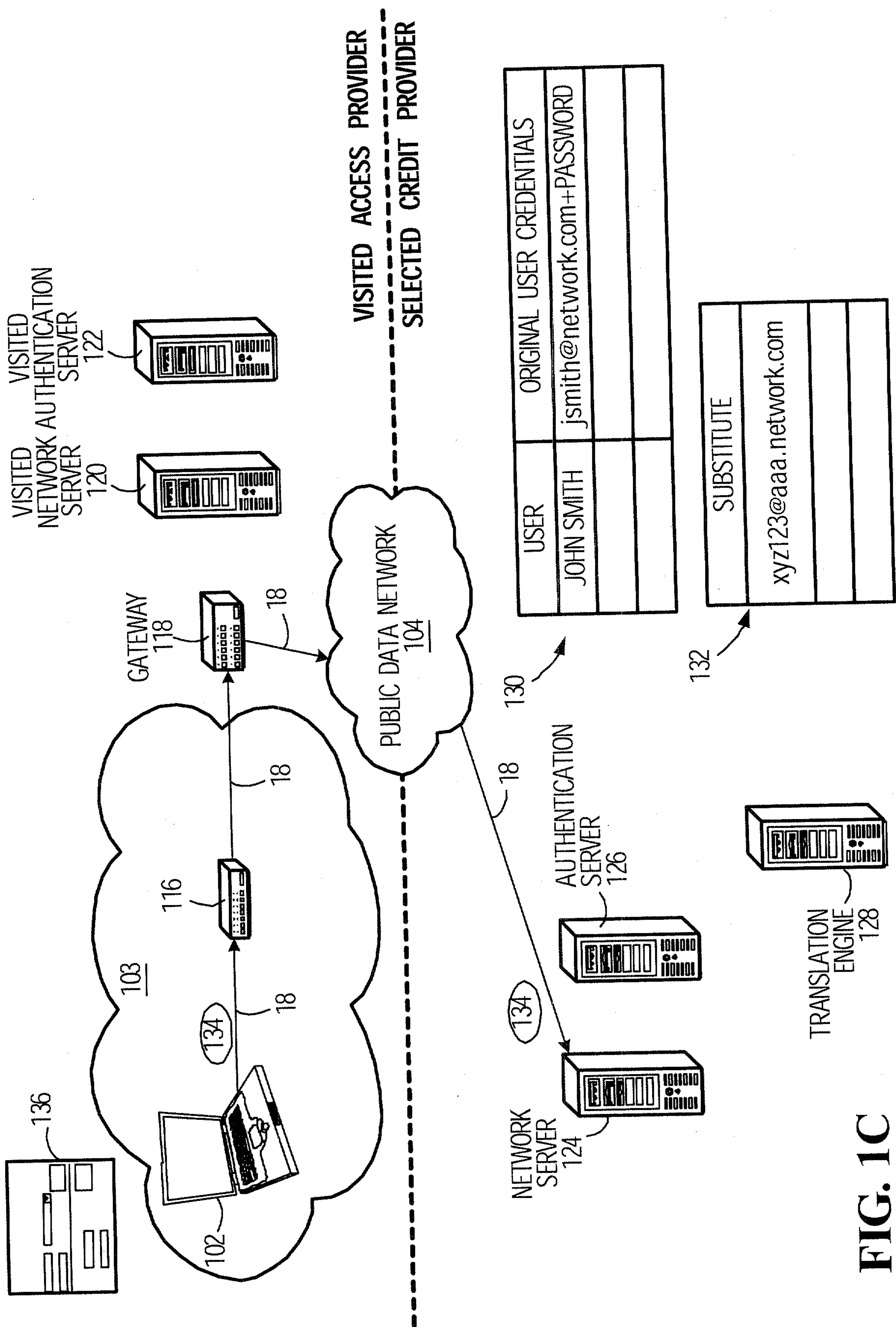


FIG. 1C

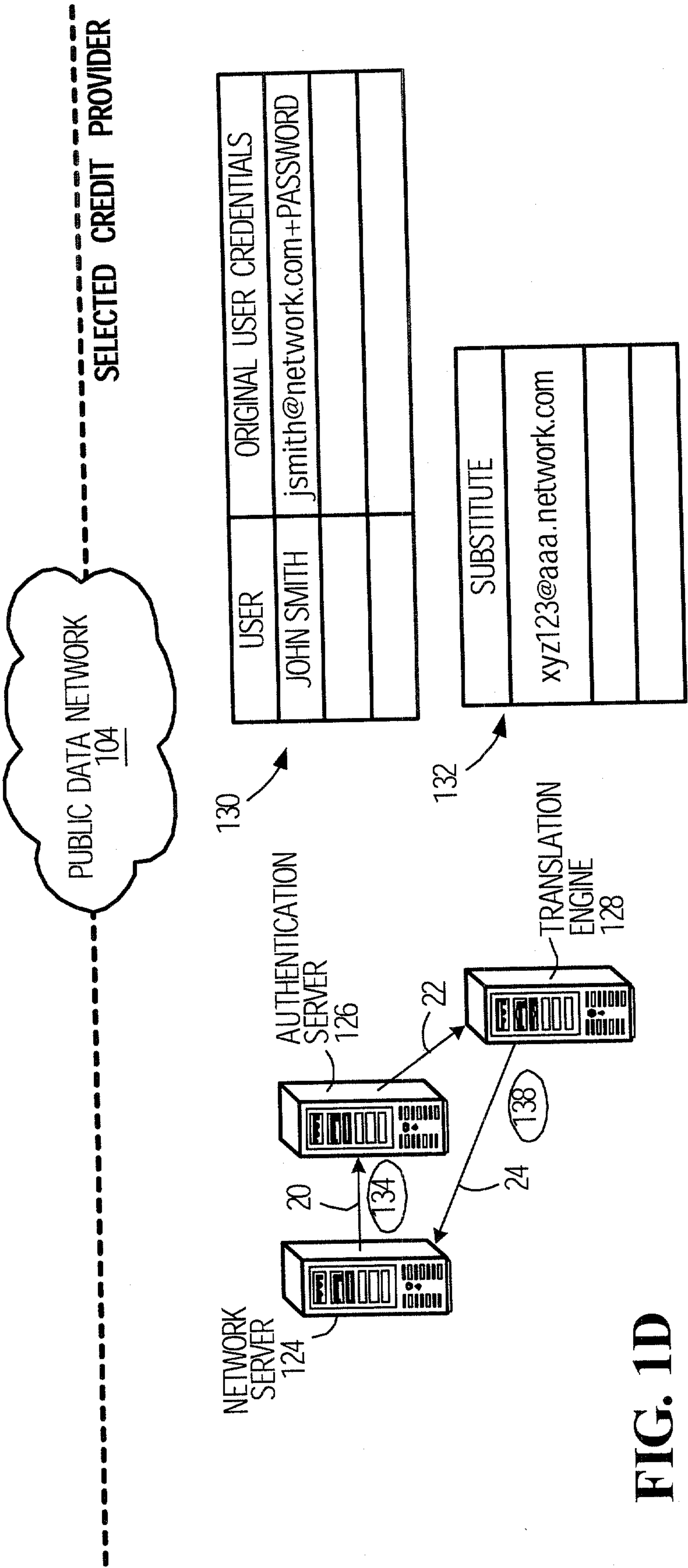


FIG. 1D

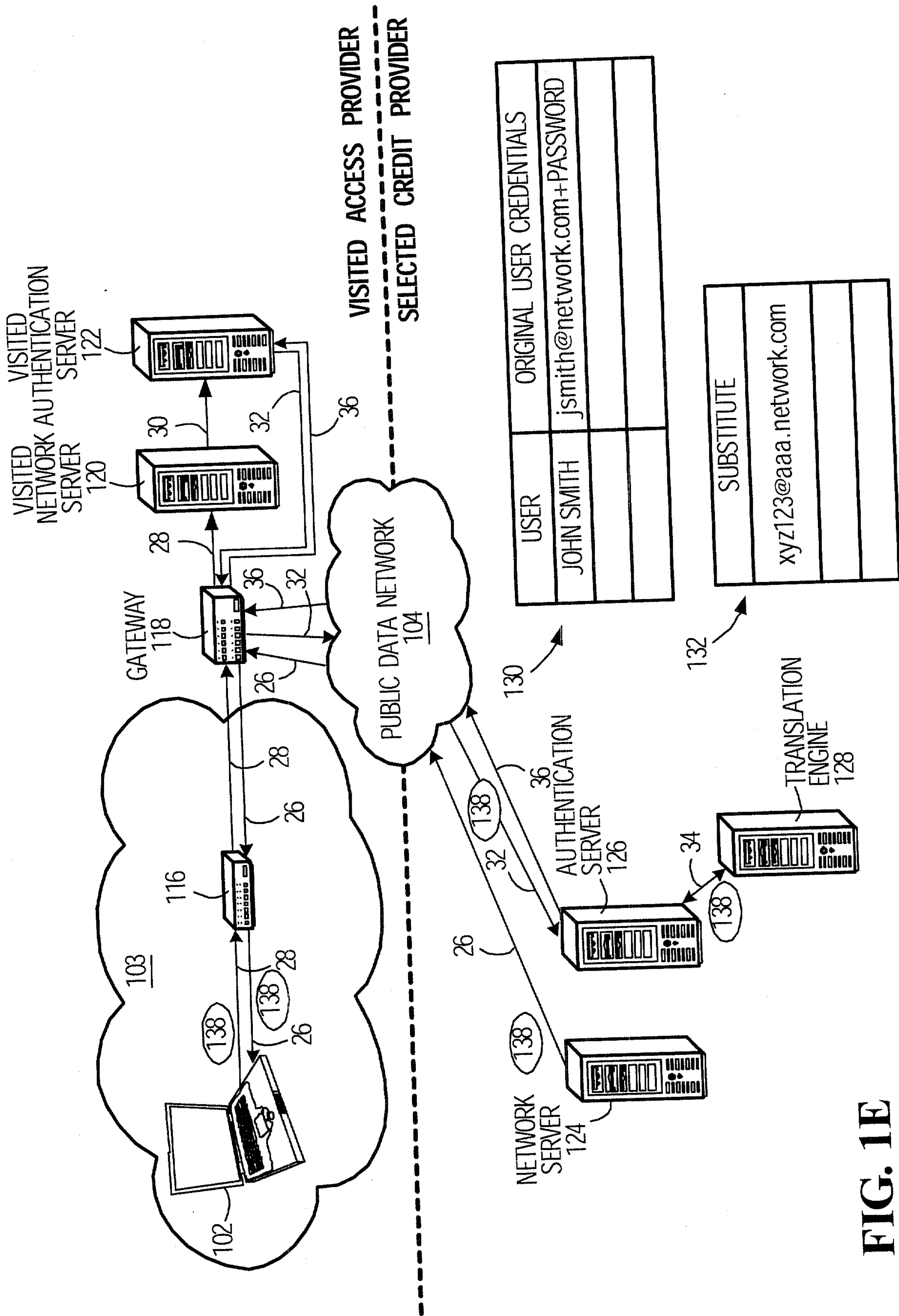


FIG. 1E

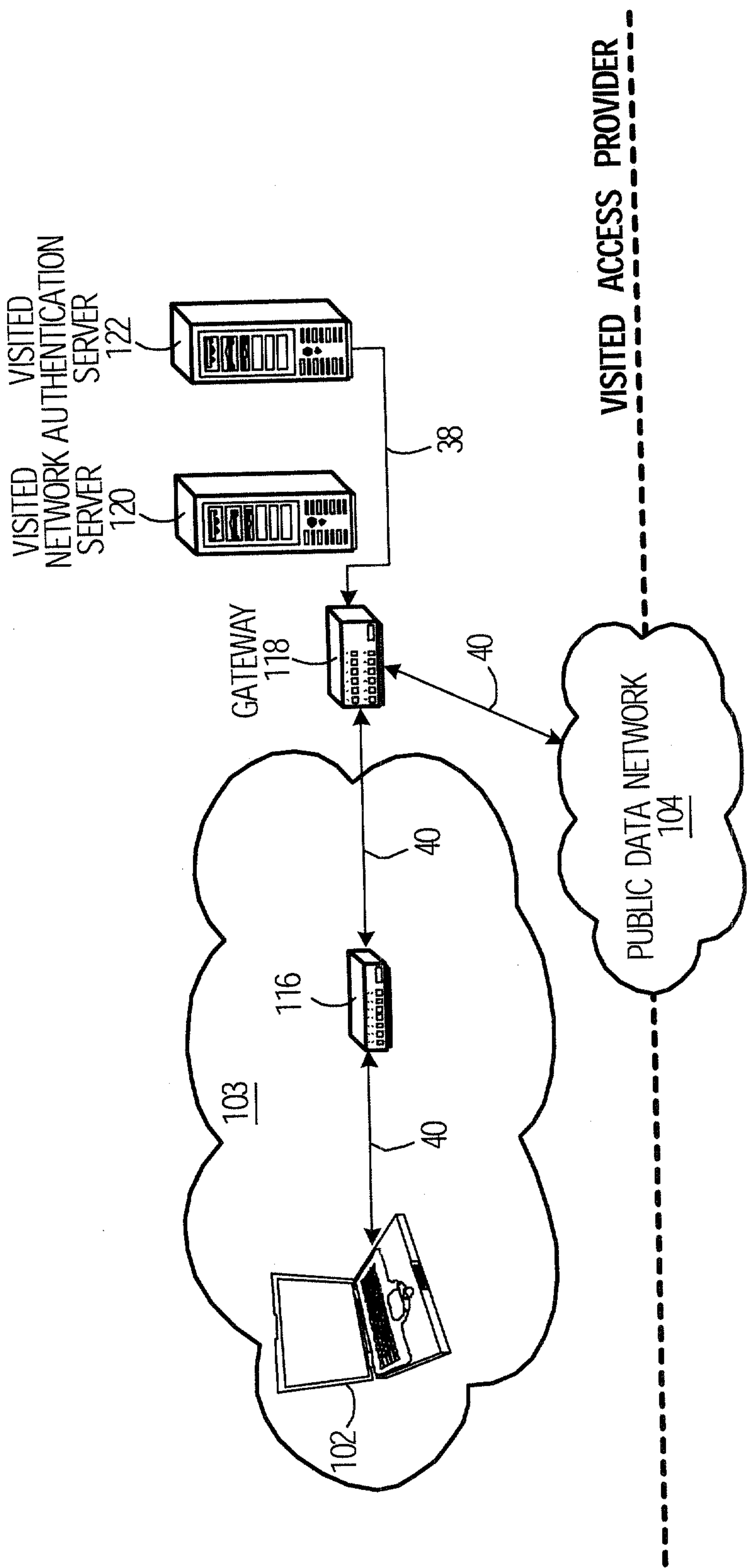


FIG. 1F

