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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 April 2009 (23.04.2009)

PCT

(10) International Publication Number
WO 2009/050704 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IL2008/001358

(22) International Filing Date: 12 October 2008 (12.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/974,833 16 October 2007 (16.10.2007) US

(71) Applicant *(for all designated States except US)*: **TRUSTED PARTNERS, INC.** [US/US]; 445 Park Ave., 9th Floor, New York, New York 10022 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SHATY, Shachar** [IL/IL]; 20 Habaron Hirsh, 75227 Rishon Le Zion (IL).

(74) Agents: **SANFORD, T. COLB & CO.** et al.; P.O. Box 2273, 76122 Rehovot (IL).

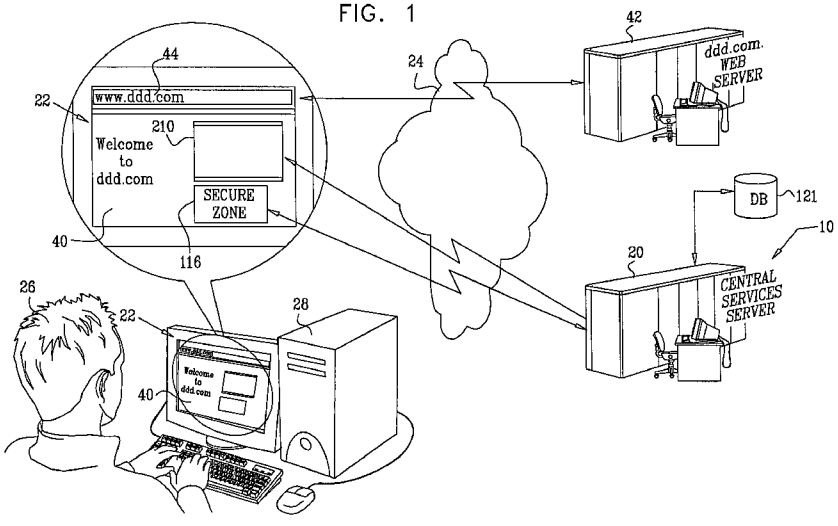
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

(54) Title: THIRD-PARTY-SECURED ZONES ON WEB PAGES

FIG. 1



(57) Abstract: A computer-implemented method is provided, including storing, in an authentication server system (10), a URL (44) identifying at least one web page (40), and providing a secure zone browser-side script to be placed on the web page (40). Upon opening of the web page (40) in a browser (22), the secure zone browser-side script triggers execution of a server-side script at the authentication server system (10). The server-side script creates, on the web page (40), an inline frame (116), which is controlled by the authentication server system (10) during a session that is associated with the inline frame (116). The authentication server system (10) retrieves a referrer address from the session, and compares the referrer address with the stored URL (44). Upon finding a match between the referrer address and the stored URL (44), the authentication server system (10) delivers web content to or via the inline frame (116). Other embodiments are also described.

WO 2009/050704 A2

THIRD-PARTY-SECURED ZONES ON WEB PAGES

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority from and is a continuation-in-part of US Application 11/974,833, filed October 16, 2007, entitled, "Third-party-secured zones on web pages," which is assigned to the assignee of the present application and is incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to web page content provided by third parties, and more specifically to third-party-secured web page communication.

BACKGROUND OF THE INVENTION

Web pages often display content provided by third-party servers. Various HTML elements are used to provide such content. For example, the HTML tag <IMG SRC...> often includes a fully-qualified uniform resource locator (URL) that causes the browser to retrieve and display a graphical image hosted by a third-party server, i.e., a server other than that which is hosting the main web page.

The serving of advertisements, such as banner ads, is one common application of such third-party provisioning of content. To display a web page including third-party-supplied advertising, a web browser first loads HTML content from the server hosting the web page. The HTML content typically includes an indication of the third-party location of the advertising, and, typically, an associated link to the advertiser's website. The browser typically executes a request to the third-party advertising host, which provides in return the media object(s) associated with the advertisement. The browser displays the media object(s) at the appropriate location on the web page.

A number of organizations issue online seals to websites that meet certain criteria, such as a certain level of reliability, maintenance of privacy of personal information, or adherence to business practices. Participating websites display a seal issued by the certification organization. For example, the Council of Better Business Bureau, Inc. operates the BBBOnLine® Reliability and Privacy Seal Programs. The BBBOnLine Reliability Seal confirms that a company is a member of its local Better Business Bureau,

has been reviewed to meet truth in advertisement guidelines, and follows good customer service practices. Similarly, the non-profit TRUSTe™ organization issues an electronic seal image to organizations that adhere to TRUSTe's established privacy principles and that agree to comply with the TRUSTe oversight and watchdog consumer dispute resolution process. VeriSign, Inc. (Mountain View, CA) provides the VeriSign Secured™ Seal to sites that are protected by a VeriSign SSL certificate.

In order to prevent fraudulent use of their seals, most organizations enable the online user to verify the authenticity of the seal. Minimally, clicking on the seal opens a web page served by the organization, which indicates whether the website displaying the seal has been authorized to do so. More sophisticated techniques for preventing fraudulent display of seals have been developed. For example, GeoTrust, Inc. (Needham, MA) provides seals that include a live time/date stamp, and/or the name of the company displaying the seal. For example, techniques for displaying and confirming the authenticity of a seal are described in US Patent 7,114,177 to Rosenberg et al., which is assigned to GeoTrust and is incorporated herein by reference, and in a white paper by Rosenberg et al., entitled "True SiteTM: Helping on-line companies create trusted brands so their site visitors feel confident enough to stay and pay," GeoTrust (November 2001), which is incorporated herein by reference. US Patent 6,658,394 to Khaishgi et al., which is incorporated herein by reference, also describes techniques for issuing electronic seals of certification to online entities.

SUMMARY OF THE INVENTION

In some embodiments of the present invention, a trusted third-party server creates a secure zone on a verified web page, and presents content in the zone to a user who is visiting the verified web page. The secure zone enables secure communication between the user's browser and the third-party server. The third-party server typically uses the zone for presenting web content, and/or for performing secure web-based applications, such as secure login or secure client-to-client transactions or communication. For some applications, the web content includes a verification seal. The third-party server is operated by a trusted third-party service provider, which verifies websites or portions thereof before allowing the use of the secure zone.

In some embodiments of the present invention, the secure zone comprises an inline frame, such as an HTML IFrame or an XFRAME, which the trusted third-party

server creates, controls, and populates with web content. Upon verifying at least one uniform resource locator (URL) of a website or a portion thereof, the third-party service provider issues a unique identification code to an entity, such as a corporate business entity, associated with the URL, and provides a zone script for placement on web pages identified by the URL. When a user opens a web page which includes the zone script, execution of the zone script triggers the execution of a program at the third-party server of the third-party provider. Upon authenticating that the URL has been verified, the program creates an inline frame on the web page, and delivers web content to or via the frame (for example, the program may present the web content in the frame). The program authenticates the URL by retrieving the referrer address (a URL) of the web page from a session between the inline frame and the third-party server, and checking whether this address is contained in a list of verified URLs maintained by the third-party provider. Optionally, the third-party server stores an identifier of the session for subsequent interaction between the user and the third-party server via the secure zone.

In some embodiments of the present invention, the entity's unique identification code is not passed to the user at any point during the creation of the secure zone, display of content in the zone, and subsequent secure communication between the user's browser and the third-party server. Furthermore, the code for placement on the web page typically contains no information specific to the entity or URL. The same code is thus generally placed on web pages identified by a plurality of different URLs controlled by different entities.

In some embodiments of the present invention, the third-party service provider comprises a seal issuer, which enables a web page identified by a verified URL to display a verification seal that is difficult to forge or misuse. Upon creating a secure zone on the web page, as described above, the third-party server presents, in or via the frame, a media object representing the seal. The seal server stores an identifier of the session between the frame and the seal server, for subsequent re-authentication of the user by the third-party server. In some embodiments of the present invention, a method is provided for providing a profile including authentication information and verified information regarding the entity (e.g., the corporate business entity) controlling the verified URL. When a user clicks on the seal, the seal server re-authenticates the user by checking whether the user is the same user previously associated with the session during which the seal was displayed in the inline frame. If so, the seal server opens a new window in the user's browser, and

presents the verified information regarding the entity associated with the URL, and information that enables the user to confirm the authenticity of the seal and the information displayed.

In some embodiments of the present invention, the third-party service provider provides a login service in the secure zone. Login information (e.g., username and password) entered by the user is transmitted directly to the third-party server. Upon successful verification of the login information, the third-party delivers, to or via the secure zone, web content available only to logged-in users.

In some embodiments of the present invention, the third-party service provider provides a secure communication service in the secure zone. A first user uses a first secure zone on a first web page to send information to a second user, who retrieves the information via a second secure zone typically on a second web page.

In some embodiments of the present invention, a web page displays a plurality of identifiers of entities (e.g., corporate business entities) in association with respective secure zones. The third-party service provider uses each of the secure zones for presenting web content specific to each respective entity. Each secure zone comprises an inline frame that specifies a unique identification code of the associated entity. The third-party service provider receives and uses the unique identification codes to authenticate each of the entities. Upon authentication, the central services server delivers web content to or via the secure zone.

There is therefore provided, in accordance with an embodiment of the present invention, a computer-implemented method including:

storing, in an authentication server system, a URL identifying at least one web page;

providing a secure zone browser-side script to be placed on the web page;

upon opening of the web page in a browser, triggering, by the secure zone browser-side script, execution of a server-side script at the authentication server system;

creating on the web page, by the server-side script, an inline frame, which is controlled by the authentication server system during a session that is associated with the inline frame;

retrieving, by the authentication server system, a referrer address from the session;

comparing, by the authentication server system, the referrer address with the

SUBSTITUTE SHEET (RULE 26)

stored URL; and

upon finding a match between the referrer address and the stored URL, delivering, by the authentication server system, web content to or via the inline frame.

In an embodiment of the present invention, the web content includes a seal media object, and delivering the web content includes presenting the seal media object in or via the inline frame.

For some applications, storing the URL includes storing the URL in association with verification information in the authentication server system, and further including:

upon finding the match between the referrer address and the stored URL, storing, by the authentication server system, an identifier of the session;

receiving an indication at the authentication server system that at least a portion of the seal media object has been activated by a user requesting the verification information;

responsively to the indication, authenticating, by the authentication server system, using the stored identifier of the session, that the seal media object has been activated in the session; and

responsively to the authenticating, presenting, by the authentication server system, the verification information to the user, in or via the inline frame.

In an embodiment of the present invention, the URL includes a first URL, the web page includes a first web page, storing the URL includes storing the first URL and a second URL identifying at least one second web page, and providing the secure zone browser-side script includes providing the same secure zone browser-side script to be placed on the first web page and on the second web page.

In an embodiment of the present invention, the inline frame includes an HTML IFrame, and creating the inline frame includes creating the HTML IFrame on the web page.

In an embodiment of the present invention, the method further includes, upon finding the match between the referrer address and the stored URL, storing, by the authentication server system, an identifier of the session. For some applications, the method further includes:

receiving an indication at the authentication server system of an interaction of a user with the web content delivered to or via the inline frame;

responsively to the indication, authenticating, by the authentication server system,

using the stored identifier of the session, that the interaction occurred in the session; and

responsively to the authenticating, performing, by the authentication server system, at least one step selected from the group consisting of: modifying at least a portion of the web content delivered to or via the inline frame, presenting information in the inline frame, and presenting information in a window of the browser opened via the inline frame.

The identifier of the session may include a random key, and storing the identifier of the session includes storing the random key in an object that represents the session. Alternatively or additionally, storing the identifier of the session includes retrieving a session ID from an object that represents the session. Further alternatively or additionally, storing the URL includes assigning an entity ID to an entity associated with the URL, and storing the identifier of the session includes storing the entity ID. Typically, the method does not include communicating the entity ID to the browser.

Alternatively or additionally, storing the identifier of the session includes retrieving and storing an IP address of the browser.

In an embodiment of the present invention, the web content includes login controls, and the method further includes: receiving at the authentication server system login information entered by a user using the login controls; authenticating the login information by the authentication server system; and delivering, by the authentication server system, restricted-access content to or via the inline frame.

In an embodiment of the present invention, the URL includes a first URL, the web page includes a first web page, and the inline frame includes a first inline frame, the web content includes first web content including transmission controls, storing the URL includes storing the first URL and a second URL, which identifies a second web page, creating further includes creating, on the second web page, a second inline frame, delivering the web content further includes delivering, to or via the second inline frame, second web content including receipt controls, and the method further includes sending, via the authentication server system, by a first user of the first website, using the transmission controls, information to a second user of the second website; and receiving the information by the second user, using the receipt controls.

For some applications, the web content includes streaming content, and delivering the web content includes leaving the inline frame open while delivering the streaming

SUBSTITUTE SHEET (RULE 26)

content.

There is further provided, in accordance with an embodiment of the present invention, apparatus including:

an interface for communicating with a browser over a network;

a memory, configured to store a URL identifying at least one web page having thereon a secure zone browser-side script; and

a processor, configured to execute a server-side script triggered by the secure zone browser-side script upon opening of the web page in the browser, which server-side script causes the processor to create on the web page an inline frame, which is controlled by the processor during a session that is associated with the inline frame, and the processor is configured to retrieve a referrer address from the session, compare the referrer address with the stored URL, and upon finding a match between the referrer address and the stored URL, deliver web content to or via the inline frame via the interface.

There is still further provided, in accordance with an embodiment of the present invention, a computer software product including a tangible computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to store a URL identifying at least one web page having thereon a secure zone browser-side script, and execute a server-side script triggered by the secure zone browser-side script upon opening of the web page in a browser, which server-side script causes the computer to create on the web page an inline frame, which is controlled by the computer during a session that is associated with the inline frame, and the instructions, when read by the computer, cause the computer to retrieve a referrer address from the session, compare the referrer address with the stored URL, and upon finding a match between the referrer address and the stored URL, deliver web content to or via the inline frame.

There is additionally provided, in accordance with an embodiment of the present invention, a computer-implemented method including:

storing, in an authentication server system, a plurality of unique identification codes assigned to respective entities;

providing a plurality of secure zone HTML code elements to be placed on a web page in association with respective identifiers of the entities, the HTML code elements

specifying respective ones of the unique identification codes for the respective associated identifiers of the entities, and the HTML code elements specifying creation of respective inline frames on the web page;

upon opening of the web page in a browser, triggering execution of a server-side program at the authentication server system, which program receives the unique identification codes specified by the code elements;

authenticating the received unique identification codes by comparing the received unique identification codes to the unique identification codes stored in the authentication server system; and

for each match found between one of the received unique identification codes and one of the stored unique identification codes, delivering, by the authentication server system, web content to or via the one of the inline frames associated with the one of the received unique identification codes.

In an embodiment, authenticating the received unique identification codes further includes storing, in the authentication server system, a URL identifying the web page, retrieving, by the authentication server system, a referrer address of the web page, and comparing, by the authentication server system, the referrer address with the stored URL, and delivering the web content includes delivering the web content only if the referrer address is identical to the stored URL.

In an embodiment, the web content includes a seal media object, and delivering the web content includes presenting the seal media object in or via the one of the inline frames.

In an embodiment, the method further includes storing by the authentication server system, for each match found, an identifier of a session that is associated with the associated one of the inline frames.

For some applications, the method further includes receiving an indication at the authentication server system of an interaction of a user with the web content delivered to or via the one of the inline frames; responsively to the indication, authenticating, by the authentication server system, using the stored identifier of the session, that the interaction occurred in the session; and, responsively to the authenticating, performing, by the authentication server system, at least one step selected from the group consisting of: modifying at least a portion of the web content delivered to or via the one of the inline frames, presenting information in the one of the inline frames, and presenting information

SUBSTITUTE SHEET (RULE 26)

in a window of the browser opened via the one of the inline frames.

For some applications, the web content includes login controls, and the method further includes receiving, at the authentication server system, login information entered by a user using the login controls; authenticating the login information by the authentication server system; and delivering, by the authentication server system, restricted-access web content to or via the one of the inline frames.

There is yet additionally provided, in accordance with an embodiment of the present invention, apparatus including:

an interface for communicating with a browser over a network;

a memory, configured to store a plurality of unique identification codes assigned to respective entities, and to store a URL identifying at least one web page having thereon a plurality of secure zone HTML code elements placed in association with respective identifiers of the entities, the HTML code elements specifying respective ones of the unique identification codes for the respective associated identifiers of the entities, and the HTML code elements specifying creation of respective inline frames on the web page; and

a processor, configured to execute, upon opening of a web page in the browser, a server-side program that receives the unique identification codes specified by the code elements, to authenticate the received unique identification codes by comparing the received unique identification codes to the unique identification codes stored in the memory, and, for each match found between one of the received unique identification codes and one of the stored unique identification codes, to deliver, via the interface, web content to or via the one of the inline frames associated with the one of the received unique identification codes.

In an embodiment, the processor is configured to further authenticate the received unique identification codes by retrieving a referrer address of the web page, and comparing the referrer address with the stored URL; and deliver the web content only if the referrer address is identical to the stored URL.

In an embodiment, the web content includes a seal media object, and the processor is configured to deliver the web content by presenting the seal media object in or via the one of the inline frames via the interface.

In an embodiment, the processor is configured to store, for each match found, an

SUBSTITUTE SHEET (RULE 26)

identifier of a session that is associated with the associated one of the inline frames. For some applications, the processor is configured to receive an indication of an interaction of a user with the web content delivered to or via the one of the inline frames; responsively to the indication, authenticate, using the stored identifier of the session, that the interaction occurred in the session; and, responsively to the authenticating, perform at least one action selected from the group consisting of: modifying at least a portion of the web content delivered to or via the one of the inline frames, presenting information in the one of the inline frames, and presenting information in a window of the browser opened via the one of the inline frames.

For some applications, the web content includes login controls, and the processor is configured to receive login information entered by a user using the login controls, authenticate the login information, and delivering restricted-access web content to or via the one of the inline frames.

There is also provided, in accordance with an embodiment of the present invention, a computer software product including a tangible computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to store a plurality of unique identification codes assigned to respective entities; to store a URL identifying at least one web page having thereon a plurality of secure zone HTML code elements placed in association with respective identifiers of the entities, the HTML code elements specifying respective ones of the unique identification codes for the respective associated identifiers of the entities, and the HTML code elements specifying creation of respective inline frames on the web page; to execute, upon opening of a web page in a browser, a server-side program that receives the unique identification codes specified by the code elements; to authenticate the received unique identification codes by comparing the received unique identification codes to the stored unique identification codes; and, for each match found between one of the received unique identification codes and one of the stored unique identification codes, to deliver web content to or via the one of the inline frames associated with the one of the received unique identification codes.

The present invention will be more fully understood from the following detailed description of embodiments thereof, taken together with the drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic, pictorial illustration showing a secure zone system, in accordance with an embodiment of the present invention;

Fig. 2 is a flow chart that schematically illustrates a method for displaying web content in a secure zone of a web page, in accordance with an embodiment of the present invention;

Fig. 3 is a schematic, pictorial illustration showing a verification seal system, in accordance with an embodiment of the present invention;

Fig. 4 is a flow chart that schematically illustrates a method for providing a profile including verified information, in accordance with an embodiment of the present invention;

Fig. 5 is a flow chart that schematically illustrates a method for secure login, in accordance with an embodiment of the present invention;

Fig. 6 is a flow chart that schematically illustrates a method for secure client-to-client transactions, in accordance with an embodiment of the present invention;

Fig. 7 is a schematic illustration of an exemplary screenshot of a web page that displays a plurality of identifiers of entities in association with respective secure zones, in accordance with an embodiment of the present invention; and

Fig. 8 is a flow chart that schematically illustrates a method for displaying identifiers of entities in association with respective secure zones, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Fig. 1 is a schematic, pictorial illustration showing a secure zone system 10, in accordance with an embodiment of the present invention. System 10 comprises a central services server 20, which comprises a Web server that communicates with a Web browser 22 over a wide area network (WAN) 24, such as the Internet. A user 26 operates the Web browser, which is typically implemented using conventional browser software running on a personal computer or workstation 28, as is known in the art.

Central services server 20 typically comprises at least one general-purpose computer workstation, having a processor, an interface with WAN 24, and, optionally, a user interface. Software for carrying out the process management functions of central

services server 20 may be provided to the server in electronic form, over a network, for example, or it may alternatively be furnished on tangible media, such as optical, magnetic or electronic memory media. Central services server 20 comprises web serving functionality, which is typically provided by a web server that runs on the same workstation that provides the other functionality of server 20 described herein, or runs on a separate server or workstation. The Web serving functionality of system 10 may be distributed over a plurality of Web servers, as is known in the art.

In an embodiment of the present invention, a third-party service provider operates system 10. The service provider verifies a plurality of uniform resource locators (URLs) (websites or portions of websites). For example, the service provider may verify a URL including a domain name of a website including a plurality of web pages, such as, for example, "www.ddd.com", or one or more URLs within a domain name, such as all web pages identified by URLs which begin with "www.ddd.com/store". The websites are typically operated by entities not otherwise legally affiliated with the third-party service provider. Typically, the verification includes verifying a relationship between an entity and the URL. To perform such verification, the third-party service provider typically verifies that the URL is associated with the entity, and/or information regarding the website and/or the operator of the website, such as the legal identity, credentials, policies, and/or business practices of the operator of the website. The third-party service provider typically stores the URL in association with verification information, such as information regarding the entity, e.g., a profile of the entity. The third-party service provider typically issues a unique identification code to the entity.

Reference is made to Fig. 2, which is a flow chart that schematically illustrates a method 100 for seamless authentication of a URL and presenting web content in a secure zone on a web page, in accordance with an embodiment of the present invention. As shown in Fig. 1, an operator of a website hosts at least one web page 40 of the website on at least one Web server 42. The web page has a URL 44, such as the exemplary domain name "www.ddd.com" shown in the figure. Web server 42 communicates with browser 22 over WAN 24. Method 100 enables the display of web content, typically HTML content, within web page 40 or another window in browser 22. The web content may comprise, for example, graphical content, text content, streaming media content, audio content, other media content, or other objects supported by HTML or browsers, such as user controls, Microsoft® ActiveX controls, and/or Java™ applets, which may provide

static or dynamic information, and/or enable interaction with the user. For some applications, the web content is delivered by a party external to both the operator of the website and the third-party service provider, such as advertisements or news. The information may be sent using protocols such as RSS or other online streaming protocols.

At a website verification step 102 during a setup portion 104 of method 100, the third-party service provider verifies at least one characteristic of URL 44, such as an association between the URL and an entity controlling the URL , such as described hereinabove. Upon verifying the URL, the third-party service provider issues a unique identification code to the entity controlling the URL (an "entity ID"), and stores the entity ID and information regarding the identify, in association with the URL, in one or more databases of system 10, at an issue and store entity ID step 106. The service provider provides a secure zone script for placement on web page 40, at a zone code issuance step 108. For some applications, the zone is visible on the web page, in which case the zone script is generally placed on web page 40 at a desired location for displaying the web content. For other applications, the zone is invisible, and may display content, for example, by causing the opening of an additional window in the browser.

During a display portion 110 of method 100, user 26 opens web page 40 in browser 22, at a display web page step 112. The opening of the web page in the browser causes the browser to execute the zone script included in the web page, at a zone script execution step 114. Execution of the zone script by the browser triggers the execution of a server-side script at central services server 20 (Fig. 1) of the third-party service provider. The zone script typically is written in a client-side scripting language, such as JavaScript or VBScript. For example, the zone code may include the following JavaScript code:

LISTING 1

```
<script language="JavaScript"
src="http://www.tpstaging.com/Jscripts/TpSecureZone.js"
type="text/javascript"></script>
```

The server-side script creates an inline frame 116 (Fig. 1), such as an HTML IFrame, at the location of the zone code on web page 40, at a frame creation step 118. An IFrame is an HTML element that enables the embedding of another HTML document inside a main document. IFrames are specified in HTML 4.01 Specification, W3C

Recommendation 24 December 1999, which is incorporated herein by reference. Alternatively, web page 40 itself includes an HTML element that creates the inline frame, which is populated by server-side code called by the zone script.

The use of an inline frame enables central services server 20 to set up a direct connection (which is typically secure) with web page 40, i.e., not via Web server 42 that is serving web page 40 outside of the frame. As a result, central services server 20 has direct and exclusive control over the section of web page 40 occupied by inline frame 116. Creation of the inline frame causes the web serving functionality of central services server 20 to create a session between the inline frame and central services server 20. For example, the web serving functionality may place a cookie on the computer in which the browser is running in order to maintain the session, as is known in the art. (Although browser- and server-side scripts are generally described in the present application, including in the claims, as executing various processes, it is to be understood that associated computer processors actually execute these various processes responsively to software instructions contained in the scripts.)

After creating the inline frame, the server-side script calls a server-side program running on central services server 20, which performs the remainder of the steps of display portion 110 of method 100. Alternatively, the server-side script itself performs all or a portion of these remaining steps.

The server-side script is written in a server-side scripting language, such as JavaScript or VBScript. The name and location of the server-side script is indicated by the zone code (in the exemplary code above, by the SRC attribute). The server-side script, for example, may include the following JavaScript code:

LISTING 2

```
document.write("<iframe id='Iframe1'
src='http://www.tpstaging.com/TpSecureZone.aspx'
width='130px' height='90px' frameborder='0'
scrolling='no' ></iframe>");
```

At a website authentication step 120, the server-side program authenticates that a web address of web page 40 (URL 44) is registered with central services server 20. The

SUBSTITUTE SHEET (RULE 26)

server-side program determines the URL by retrieving the referrer address from the session of the inline frame, for example using the HTTP_REFERER variable, and checks whether the web address was registered at step 106 above. It is noted that at no point during this authentication process is any client- or website-specific data transferred over the Internet in a decipherable way.

For some applications, after authenticating the web address, the server-side program stores an identifier of the session between the inline frame and the central services server. For some applications, the identifier comprises a session key, which comprises: (a) a random, unique value, (b) optionally, the entity ID, and, optionally, (c) the IP address of the browser 22 client (retrieved using the REMOTE_ADDR variable), and stores the key as a record in a data repository 121 (e.g., one or more tables, or a relational database) stored on or in communication with central services server 20, at a key creation and storage step 122.

For some applications, the server-side program also stores the session key in the session between the inline frame and the central services server. For example, the server-side program may use a Microsoft® Active Server Pages (ASP) Session Object for this purpose (e.g., using the statement "Session["Key"] = CreateRandomKey();"). For some applications, central services server 20 uses this stored key at step 202 of method 200, described hereinbelow with reference to Fig. 4. The use of the session key obviates any need to send the entity ID to browser 22 throughout the content serving processes described herein.

Alternatively, for some applications, rather than creating a random value for storage in the key at step 122 above, the server-side program retrieves the ASP Session ID automatically created when the session between the inline frame and the central services server was created, and includes this value in the key. For these applications, the server-side program does not necessarily store the key in the Session Object, because the Session Object already includes the ASP Session ID which is used later at step 202 of method 200 to confirm the identify of the session. For applications in which the server-side program uses a server-side scripting language other than ASP that supports sessions, the server-side program retrieves the session ID from these sessions.

At a web content presentation step 124, the server-side program delivers web content to inline frame 116 or via inline frame 116 (e.g., by opening a new window in the

browser via the inline frame), thereby concluding display portion 110 of method 100. The inline frame session typically, but not necessarily, remains open after delivering the content. For some applications, such as when the web content includes streaming content, the inline frame is left open for displaying the content.

Reference is made to Fig. 3, which is a schematic, pictorial illustration showing an authentication seal system 150, in accordance with an embodiment of the present invention. Authentication seal system 150 represents one implementation of secure zone system 10, described hereinabove with reference to Figs. 1 and 2. In addition to the elements of system 10, authentication seal system 150 comprises at least one seal repository server 152, which may run on a separate workstation, as shown in Fig. 1, or on the same workstation on which central services server 20 runs (configuration not shown). Each seal repository server 152 comprises at least one general-purpose computer workstation, having a processor and at least one interface. Seal repository server 152 is typically protected by a firewall. For some applications, system 150 comprises separate seal repository servers 152 for different geographic regions, such as different countries.

In an embodiment of the present invention, to display an authentication seal in the secure zone defined by inline frame 116, the third-party service provider and authentication seal system 150 use method 100, described hereinabove with reference to Fig. 2, modified as follows. Upon authenticating a website, or a portion thereof, at authentication step 102, the third-party service provider typically also stores additional certification information regarding the website and/or its operator, such as described hereinabove, in seal repository server 152, for display during a seal verification procedure, as described hereinbelow with reference to Fig. 4. For some applications, at key creation and storage step 122, the server-side program stores the session key in seal repository 152. At web content presentation step 124, the server-side program populates inline frame 116 with a seal media object 154.

Reference is made to Fig. 4, which is a flow chart that schematically illustrates a method 200 for providing a profile including verified information, in accordance with an embodiment of the present invention. Method 200 begins when a user requests information regarding the entity associated with the URL, by activating at least a portion of media object 154, typically by clicking on it, at a request information step 202. At a user re-authentication check step 204, central services server 20 checks whether the user

is the same user 26 previously associated with the inline frame session created by central services server 20 at step 118 of method 100, described with reference to Figs. 2 and 3 hereinabove.

For some applications, to perform this re-authentication check the central services server constructs an authentication key that comprises:

- the random value stored at step 122 of method 100 above, which is now retrieved by the central services server from the Session Object. If the information-requesting user is the same as user 26 to whom the seal was displayed at step 124 of method 100 above, the same inline frame session continues, so the same random value is retrieved that was earlier stored. If, on the other hand, the information-requesting user is any user other than user 26, or the session has timed out, the server is not able to retrieve the same random value, because the information-requesting user has a different session from the session created for user 26. Alternatively, for applications in which the server-side program does not create a random key at step 122 of method 100 of Fig. 2, the authentication key comprises the Session ID, rather than the random value;
- optionally, the entity ID; and
- optionally, the IP address of the browser 22 client (retrieved using the REMOTE_ADDR variable).

The central services server attempts to look up this authentication key in the data repository 121 in which the key was stored at step 122 of method 100 above (which, as mentioned, for some applications is stored in seal repository server 152). If there is no match in the database between this random value-IP combination and one of the keys stored earlier, re-authentication of the user fails, at a failed verification step 206. For example, the information-requesting user may be trying to spoof the user 26, or the session may have timed out. Typically, the central services server stores the IP address of the failed information-verifying user for later analysis.

Alternatively, for applications in which the key created at step 122 of method 100 includes the ASP Session ID instead of a random value, as described hereinabove, the authentication key includes the ASP Session ID of the current session, rather than the

SUBSTITUTE SHEET (RULE 26)

value retrieved from the Session Object.

On the other hand, if the same user 26 is confirmed to be requesting information at check step 204, the entity ID of the key is returned from the database. At a verification information display step 208, central services server 20, or seal repository server 152, using the entity ID, retrieves additional information regarding the entity and/or the URL from seal repository server 152, and displays this information to user 24. This information is typically displayed in a pop-up window 210 opened for this purpose over the same open session, either at step 208 or prior thereto, such at step 202, or, alternatively, by redirecting the window in which the zone is located.

In an embodiment of the present invention, the techniques of method 200, described hereinabove with reference to Fig. 4, are used for re-authenticating a user for applications other than presenting a seal, such as for other applications described herein.

Reference is made to Fig. 5, which is a flow chart that schematically illustrates a method 300 for secure login, in accordance with an embodiment of the present invention. Method 300 enables user 26 viewing web page 40 to securely log into a service or system offered by the third-party service provider, via the secure zone provided by inline frame 116. The method begins at content presentation step 124 of method 100 of Fig. 2, after the earlier steps of method 100 have been completed, such that inline frame 116 has been created on web page 40. At step 124 of method 100, the server-side program populates inline frame 116 with login controls, such as text boxes for entering a username and password, and other login-related information, such as login instructions. When the user submits the login information, the information is sent to central services server 20 for authentication, at a send information step 302. Server 20 checks whether the login information is correct, at an authentication check step 304. If the server finds that the login information is correct, the user is logged in, and the server delivers restricted-access web content to the user, to or via the inline frame, typically by redirecting the current active browser window, opening a new window in the browser, or populating the inline frame, at a restricted-access window presentation step 306. If the login information is found to be incorrect, login fails, at a login failure step 308. For some applications, during the login process, such as when the user submits the login information, the third-party server re-authenticates the user, using the re-authentication techniques described hereinabove with reference to step 204 of method 200 of Fig. 4.

Reference is made to Fig. 6, which is a flow chart that schematically illustrates a method 400 for secure client-to-client transactions, in accordance with an embodiment of the present invention. Method 400 enables a first user 26 viewing web page 40 to securely transmit information to at least one second user 26, via the third-party service provider. Method 400 includes a transmit phase 402, followed by an accept phase 404. Transmit phase 402 optionally begins at a login step 406, at which first user 26 performs a secure login via inline frame 116, using method 300 described hereinabove with reference to Fig. 5. Alternatively, the transmit phase begins without secure login, after inline frame 116 has been created, as described hereinabove with reference to steps 102 through 122 of method 100 of Fig. 2.

At a transaction controls presentation step 408, the server-side program populates inline frame 116, or another window generated via the inline frame, with transaction controls that, for example, allow the first user to enter a message and/or select files for transmission. The transaction controls also enable the first user to enter a destination address, such as an alphanumeric user ID, and to give a send instruction. Using the controls in the inline frame, the user enters information (e.g., a message and/or one or more files), and sends the information, at a send information step 410. For some applications, during information sending process, such as when the user submits an indication to send the information, the third-party server re-authenticates the user, using the re-authentication techniques described hereinabove with reference to step 204 of method 200 of Fig. 4. Server 20 stores the transmitted information, at an information storage step 412. The server also sets a notification for the recipient, at a set notification step 414.

Accept phase 404 optionally begins at a login step 416, at which a second user 26 performs a secure login via inline frame 116, using method 300 described hereinabove with reference to Fig. 5. Alternatively, the accept phase begins without secure login, after inline frame 116 has been created, as described hereinabove with reference to steps 102 through 122 of method 100 of Fig. 2.

At a notification step 418, the server-side program populates inline frame 116, or another window generated via the inline frame, with a notification that the transmitted information has been sent. The second user selects the information for retrieval, such as viewing and/or downloading from server 20, at a receipt step 420. For some applications,

during the information retrieval process, such as when the user submits a request for retrieval, the third-party server re-authenticates the user, using the re-authentication techniques described hereinabove with reference to step 204 of method 200 of Fig. 4.

For some applications, transmission of information is performed on an entity level, i.e., information is sent from a first entity (e.g., "www.ddd.com") to a second entity (e.g., "www.eee.com"), each of which has a unique ID. Typically, any user logged into the first entity can send information, and any user logged into the second, receiving entity can view and/or download the transmitted information.

For other applications, transmission of information is performed on a user level, i.e., information is sent from a first user to a second user, each of which has a unique user ID. Each user can log into any web page participating in the information transmission service offered by the third-party service provider.

For some applications, method 400 is used to enable client-to-client transactions beyond information exchange, such as trading or other business transactions. For these applications, the information communicated using the method relates to such transactions.

Fig. 7 is a schematic illustration of an exemplary screenshot of a web page 500 that displays a plurality of identifiers 502 of entities in association with respective secure zones 504, in accordance with an embodiment of the present invention. For some applications, identifiers 502 comprise human-readable names of the entities (e.g., corporate business entities). Alternatively or additionally, the identifiers comprise hypertext URLs 506 that are associated with the entities. Generally, web page 500 is served by a web server whose operator is unaffiliated with the entities and unaffiliated with central services server 20. For some applications, central services server 20 uses each of secure zones 504 for presenting web content specific to each respective entity. Alternatively, the same content is presented in all or a portion of the secure zones. The third-party service provider operating central services server 20 issues a unique identification code to each of the entities. Alternatively, only a portion of the entities are issued identification codes, and secure zones 504 are displayed only for the entities having identification codes.

For some applications, web page 500 displays search results, which include respective hypertext URLs 506, each of which is associated with a respective one of the entities, for example, the entity that operates the web site or page associated with the

URL. For other applications, web page 500 displays a list of identifiers of the entities (such as human-readable names of the entities), for example, to provide an online directory of the entities.

In some of the embodiments described hereinabove with reference to Figs. 1-6, the same secure zone browser-side script is provided on a plurality of web pages. In these embodiments, central services server 20 identifies each of the web pages by retrieving its unique URL from the referrer address.

In contrast, in the present embodiment, a plurality of secure zones 504 are displayed on web page 500, which is identified by a single URL that is not directly associated with the entities displayed on web page 500. Central services server 20 thus cannot use the referrer address of web page 500 to identify the unique identification code of the entity associated with each secure zone. Instead, secure zones 504 are created by respective HTML code elements that specify the respective unique identification codes of the respective associated entities. Central services server 20 receives and uses the unique identification codes to authenticate that each of the entities is registered with the central services server. Upon authentication, the central services server delivers web content to or via the secure zone, such as described hereinabove with reference to step 124 of method 100 of Fig. 2. For some applications, the content is unique and/or customized for each entity, while for other applications, the same content is provided for a plurality of entities (e.g., a seal media object). For some applications, the central services server stores an identifier of a session between the secure zone and the central services server, as described hereinabove with reference to step 122 of method 100 of Fig. 2. The central services server may use this identifier for a re-authentication check before providing a profile including verified information, as described hereinabove with reference to Fig. 4. The web content delivered to or via the secure zone may include any of the applications described hereinabove, such as with reference to Figs. 3, 4, 5, and/or 6, for example, a seal media object, or transactions controls (e.g., for secure login).

For some applications, each of the HTML code elements comprises an inline frame 510, such as an HTML IFrame, which specifies as its content source a URL provided by central services server 20, and passes a parameter containing the unique identification code to central services server 20. The following exemplary HTML code element is for an entity having an identification code with the value "123," which is

identified by the parameter "IdValue":

LISTING 3

```
<iframe
src="http://www.tpsmartseal.com/listings.aspx?listType=200&ListArea=10&IdType=2&I
dValue=123"
frameborder="0" width="20" height="20">
</iframe>
```

As explained above, this HTML code element appears a plurality of times on the search results web page, each time specifying a different identification code. The HTML code element triggers execution of a server-side script, which receives the unique identification code, and, responsively thereto, generates appropriate HTML code for presentation in the user's browser.

Reference is made to Fig. 8, which is a flow chart that schematically illustrates a method 600 for displaying identifiers of entities in association with respective secure zones, in accordance with an embodiment of the present invention. Method 600 begins at a setup step 601, at which a third-party service provider verifies and registers the entities, typically using the techniques described hereinabove with reference to setup portion 104 of method 100 of Fig. 2, *mutatis mutandis*. At a web page generation step 602, a web server generates a web page that displays a plurality of identifiers of entities (e.g., human-readable names of the entities), and, in association with each of the entity identifiers, an HTML code element, such as an HTML IFrame, which includes as a parameter a unique identification code for the entity. A user's web browser receives and displays the web page, at a display web page step 604. The browser loads the source URL specified by the HTML code elements, at a load source URL step 606. Loading the URL triggers execution of a server-side program, typically a script, by central services server 20. Typically, the plurality of HTML code elements specify the same source URL.

The server-side program separately authenticates each entity, using the unique identification code specified by each HTML code element, at an authentication step 608. To perform this authentication, the server-side program typically authenticates that the unique identification code is registered with central services server 20. Optionally, the server-side program further authenticates the entity by authenticating that a web address

(such as one or more URLs) of the web page is registered with central services server 20. The server-side program determines the URL of the web page by retrieving the referrer address from the session of the inline frame, for example using the HTTP_REFERER variable, and checks whether the web address was registered. For some applications, server-side program checks whether the unique identification code was associated with the URL during registration.

For some applications, after authenticating the web address, the server-side program stores an identifier of the session between the inline frame and the central services server, at a key creation step 610. Typically, the server-side program uses techniques described hereinabove with reference to step 122 of method 100 of Fig. 2. At a web content presentation step 612, the server-side program delivers web content to or via each of the authenticated secure zones (e.g., by opening a new window in the browser via the inline frame). The inline frame session typically, but not necessarily, remains open after delivering the content. For some applications, such as when the web content includes streaming content, the inline frame is left open for displaying the content.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove, as well as variations and modifications thereof that are not in the prior art, which would occur to persons skilled in the art upon reading the foregoing description.

CLAIMS

1. A computer-implemented method comprising:

storing, in an authentication server system, a URL identifying at least one web page;

providing a secure zone browser-side script to be placed on the web page;

upon opening of the web page in a browser, triggering, by the secure zone browser-side script, execution of a server-side script at the authentication server system;

creating on the web page, by the server-side script, an inline frame, which is controlled by the authentication server system during a session that is associated with the inline frame;

retrieving, by the authentication server system, a referrer address from the session;

comparing, by the authentication server system, the referrer address with the stored URL; and

upon finding a match between the referrer address and the stored URL, delivering, by the authentication server system, web content to or via the inline frame.

2. The method according to claim 1, wherein the web content includes a seal media object, and wherein delivering the web content comprises presenting the seal media object in or via the inline frame.

3. The method according to claim 2, wherein storing the URL comprises storing the URL in association with verification information, in the authentication server system, and further comprising:

upon finding the match between the referrer address and the stored URL, storing, by the authentication server system, an identifier of the session;

receiving an indication at the authentication server system that at least a portion of the seal media object has been activated by a user requesting the verification information;

responsively to the indication, authenticating, by the authentication server system, using the stored identifier of the session, that the seal media object has been activated in the session; and

responsively to the authenticating, presenting, by the authentication server system, the verification information to the user, in or via the inline frame.

4. The method according to claim 1, wherein the URL includes a first URL, wherein the web page includes a first web page, wherein storing the URL comprises storing the

first URL and a second URL identifying at least one second web page, and wherein providing the secure zone browser-side script comprises providing the same secure zone browser-side script to be placed on the first web page and on the second web page.

5. The method according to claim 1, wherein the inline frame includes an HTML IFrame, and wherein creating the inline frame comprises creating the HTML IFrame on the web page.

6. The method according to claim 1, further comprising, upon finding the match between the referrer address and the stored URL, storing, by the authentication server system, an identifier of the session.

7. The method according to claim 6, further comprising:

receiving an indication at the authentication server system of an interaction of a user with the web content delivered to or via the inline frame;

responsively to the indication, authenticating, by the authentication server system, using the stored identifier of the session, that the interaction occurred in the session; and

responsively to the authenticating, performing, by the authentication server system, at least one step selected from the group consisting of: modifying at least a portion of the web content delivered to or via the inline frame, presenting information in the inline frame, and presenting information in a window of the browser opened via the inline frame.

8. The method according to claim 6, wherein the identifier of the session includes a random key, and wherein storing the identifier of the session comprises storing the random key in an object that represents the session.

9. The method according to claim 6, wherein storing the identifier of the session comprises retrieving a session ID from an object that represents the session.

10. The method according to claim 6, wherein storing the URL comprises assigning an entity ID to an entity associated with the URL, and wherein storing the identifier of the session comprises storing the entity ID.

11. The method according to claim 10, wherein the method does not comprise communicating the entity ID to the browser.

12. The method according to claim 6, wherein storing the identifier of the session comprises retrieving and storing an IP address of the browser.

13. The method according to claim 1, wherein the web content includes login controls, and further comprising:

receiving at the authentication server system login information entered by a user using the login controls;

authenticating the login information by the authentication server system; and

delivering, by the authentication server system, restricted-access web content to or via the inline frame.

14. The method according to claim 1,

wherein the URL includes a first URL, the web page includes a first web page, and the inline frame includes a first inline frame,

wherein the web content includes first web content comprising transmission controls,

wherein storing the URL comprises storing the first URL and a second URL, which identifies a second web page,

wherein creating further comprises creating, on the second web page, a second inline frame,

wherein delivering the web content further comprises delivering, to or via the second inline frame, second web content comprising receipt controls, and further comprising:

sending, via the authentication server system, by a first user of the first website, using the transmission controls, information to a second user of the second website; and

receiving the information by the second user, using the receipt controls.

15. The method according to claim 1, wherein the web content includes streaming content, and wherein delivering the web content comprises leaving the inline frame open while delivering the streaming content.

16. Apparatus comprising:

an interface for communicating with a browser over a network;

a memory, configured to store a URL identifying at least one web page having thereon a secure zone browser-side script; and

a processor, configured to execute a server-side script triggered by the secure zone browser-side script upon opening of the web page in the browser, which server-side script causes the processor to create on the web page an inline frame, which is controlled by the

processor during a session that is associated with the inline frame, wherein the processor is configured to retrieve a referrer address from the session, compare the referrer address with the stored URL, and upon finding a match between the referrer address and the stored URL, deliver web content to or via the inline frame via the interface.

17. The apparatus according to claim 16, wherein the web content includes a seal media object, and wherein the processor is configured to present the seal media object in or via the inline frame.

18. The apparatus according to claim 17, wherein the memory is configured to store the URL in association with verification information, and wherein the processor is configured to: upon finding the match between the referrer address and the stored URL, store an identifier of the session in the memory; receive an indication that at least a portion of the seal media object has been activated by a user requesting the verification information; responsively to the indication, authenticate, using the stored identifier of the session, that the seal media object has been activated in the session; and responsively to authenticating, present the verification information to the user, in or via the inline frame.

19. The apparatus according to claim 16, wherein the URL includes a first URL, wherein the web page includes a first web page, and wherein the memory is configured to store the first URL, and to store a second URL identifying at least a second web page having thereon the same secure zone browser-side script as is on the first web page.

20. The apparatus according to claim 16, wherein the processor is configured to, upon finding the match between the referrer address and the stored URL, store an identifier of the session in the memory.

21. The apparatus according to claim 20, wherein the processor is configured to: receive an indication of an interaction of a user with the web content delivered to or via the inline frame; responsively to the indication, authenticate, using the stored identifier of the session, that the interaction occurred in the session; and responsively to the authenticating, perform at least one action selected from the group consisting of: modifying at least a portion the web content delivered to or via the inline frame, presenting information in the inline frame, and presenting information in a window of the browser opened via the inline frame.

22. The apparatus according to claim 16, wherein the URL includes a first URL, the

SUBSTITUTE SHEET (RULE 26)

web page includes a first web page, and the inline frame includes a first inline frame, wherein the web content includes first web content comprising transmission controls, wherein the memory is configured to store a second URL identifying at least one second web page having thereon the secure zone browser-side script, and wherein the processor is configured to: create, on the second web page, a second inline frame; deliver, to or via the second inline frame, second web content comprising receipt controls; receive information sent by a first user of the first website, responsively to use by the first user of the transmission controls; and transmit the information to a second user of the second website, responsively to use by the second user of the receipt controls.

23. A computer software product comprising a tangible computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to store a URL identifying at least one web page having thereon a secure zone browser-side script, and execute a server-side script triggered by the secure zone browser-side script upon opening of the web page in a browser, which server-side script causes the computer to create on the web page an inline frame, which is controlled by the computer during a session that is associated with the inline frame, and wherein the instructions, when read by the computer, cause the computer to retrieve a referrer address from the session, compare the referrer address with the stored URL, and upon finding a match between the referrer address and the stored URL, deliver web content to or via the inline frame.

24. The computer software product according to claim 23, wherein the web content includes a seal media object, and wherein the instructions, when read by the computer, cause the computer to present the seal media object in or via the inline frame.

25. The computer software product according to claim 24, wherein the instructions, when read by the computer, cause the computer to store the URL in association with verification information; upon finding the match between the referrer address and the stored URL, store an identifier of the session; receive an indication that at least a portion of the seal media object has been activated by a user requesting the verification information; responsively to the indication, authenticate, using the stored identifier, that the seal media object has been activated in the session; and responsively to authenticating, present the verification information to the user, in or via the inline frame.

26. A computer-implemented method comprising:

storing, in an authentication server system, a plurality of unique identification codes assigned to respective entities;

providing a plurality of secure zone HTML code elements to be placed on a web page in association with respective identifiers of the entities, the HTML code elements specifying respective ones of the unique identification codes for the respective associated identifiers of the entities, and the HTML code elements specifying creation of respective inline frames on the web page;

upon opening of the web page in a browser, triggering execution of a server-side program at the authentication server system, which program receives the unique identification codes specified by the code elements;

authenticating the received unique identification codes by comparing the received unique identification codes to the unique identification codes stored in the authentication server system; and

for each match found between one of the received unique identification codes and one of the stored unique identification codes, delivering, by the authentication server system, web content to or via the one of the inline frames associated with the one of the received unique identification codes.

27. The method according to claim 26,

wherein authenticating the received unique identification codes further comprises:

storing, in the authentication server system, a URL identifying the web page;

retrieving, by the authentication server system, a referrer address of the web page;

comparing, by the authentication server system, the referrer address with the stored URL, and

wherein delivering the web content comprises delivering the web content only if the referrer address is identical to the stored URL.

28. The method according to claim 26, wherein the web content includes a seal media object, and wherein delivering the web content comprises presenting the seal media object in or via the one of the inline frames.

29. The method according to claim 26, further comprising storing by the

authentication server system, for each match found, an identifier of a session that is associated with the associated one of the inline frames.

30. The method according to claim 29, further comprising:

receiving an indication at the authentication server system of an interaction of a user with the web content delivered to or via the one of the inline frames;

responsively to the indication, authenticating, by the authentication server system, using the stored identifier of the session, that the interaction occurred in the session; and

responsively to the authenticating, performing, by the authentication server system, at least one step selected from the group consisting of: modifying at least a portion of the web content delivered to or via the one of the inline frames, presenting information in the one of the inline frames, and presenting information in a window of the browser opened via the one of the inline frames.

31. The method according to claim 26, wherein the web content includes login controls, and further comprising:

receiving, at the authentication server system, login information entered by a user using the login controls;

authenticating the login information by the authentication server system; and

delivering, by the authentication server system, restricted-access web content to or via the one of the inline frames.

32. Apparatus comprising:

an interface for communicating with a browser over a network;

a memory, configured to store a plurality of unique identification codes assigned to respective entities, and to store a URL identifying at least one web page having thereon a plurality of secure zone HTML code elements placed in association with respective identifiers of the entities, the HTML code elements specifying respective ones of the unique identification codes for the respective associated identifiers of the entities, and the HTML code elements specifying creation of respective inline frames on the web page; and

a processor, configured to execute, upon opening of a web page in the browser, a server-side program that receives the unique identification codes specified by the code elements, to authenticate the received unique identification codes by comparing the received unique identification codes to the unique identification codes stored in the

SUBSTITUTE SHEET (RULE 26)

memory, and, for each match found between one of the received unique identification codes and one of the stored unique identification codes, to deliver, via the interface, web content to or via the one of the inline frames associated with the one of the received unique identification codes.

33. The apparatus according to claim 32, wherein the processor is configured to:

further authenticate the received unique identification codes by retrieving a referrer address of the web page, and comparing the referrer address with the stored URL, and

deliver the web content only if the referrer address is identical to the stored URL.

34. The apparatus according to claim 32, wherein the web content includes a seal media object, and wherein the processor is configured to deliver the web content by presenting the seal media object in or via the one of the inline frames via the interface.

35. The apparatus according to claim 32, wherein the processor is configured to store, for each match found, an identifier of a session that is associated with the associated one of the inline frames.

36. The apparatus according to claim 35, wherein the processor is configured to receive an indication of an interaction of a user with the web content delivered to or via the one of the inline frames; responsively to the indication, authenticate, using the stored identifier of the session, that the interaction occurred in the session; and, responsively to the authenticating, perform at least one action selected from the group consisting of: modifying at least a portion of the web content delivered to or via the one of the inline frames, presenting information in the one of the inline frames, and presenting information in a window of the browser opened via the one of the inline frames.

37. The apparatus according to claim 32, wherein the web content includes login controls, and wherein the processor is configured to receive login information entered by a user using the login controls, authenticate the login information, and delivering restricted-access web content to or via the one of the inline frames.

38. A computer software product comprising a tangible computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to store a plurality of unique identification codes assigned to respective entities; to store a URL identifying at least one web page having thereon a

SUBSTITUTE SHEET (RULE 26)

plurality of secure zone HTML code elements placed in association with respective identifiers of the entities, the HTML code elements specifying respective ones of the unique identification codes for the respective associated identifiers of the entities, and the HTML code elements specifying creation of respective inline frames on the web page; to execute, upon opening of a web page in a browser, a server-side program that receives the unique identification codes specified by the code elements; to authenticate the received unique identification codes by comparing the received unique identification codes to the stored unique identification codes; and, for each match found between one of the received unique identification codes and one of the stored unique identification codes, to deliver web content to or via the one of the inline frames associated with the one of the received unique identification codes.

39. The computer software product according to claim 38, wherein the instructions, when read by the computer, cause the computer to:

further authenticate the received unique identification codes by retrieving a referrer address of the web page, and comparing the referrer address with the stored URL, and

deliver the web content only if the referrer address is identical to the stored URL.

40. The computer software product according to claim 38, wherein the web content includes a seal media object, and wherein the instructions, when read by the computer, cause the computer to deliver the web content by presenting the seal media object in or via the one of the inline frames.

41. The computer software product according to claim 38, wherein the instructions, when read by the computer, cause the computer to store, for each match found, an identifier of a session that is associated with the associated one of the inline frames.

42. The computer software product according to claim 41, wherein the instructions, when read by the computer, cause the computer to receive an indication of an interaction of a user with the web content delivered to or via the one of the inline frames; responsively to the indication, authenticate, using the stored identifier of the session, that the interaction occurred in the session; and, responsively to the authenticating, perform at least one action selected from the group consisting of: modifying at least a portion of the web content delivered to or via the one of the inline frames, presenting information in the one of the inline frames, and presenting information in a window of the browser opened

SUBSTITUTE SHEET (RULE 26)

via the one of the inline frames.

43. The computer software product according to claim 38, wherein the web content includes login controls, and wherein the instructions, when read by the computer, cause the computer to receive login information entered by a user using the login controls, authenticate the login information, and delivering restricted-access web content to or via the one of the inline frames.

SUBSTITUTE SHEET (RULE 26)

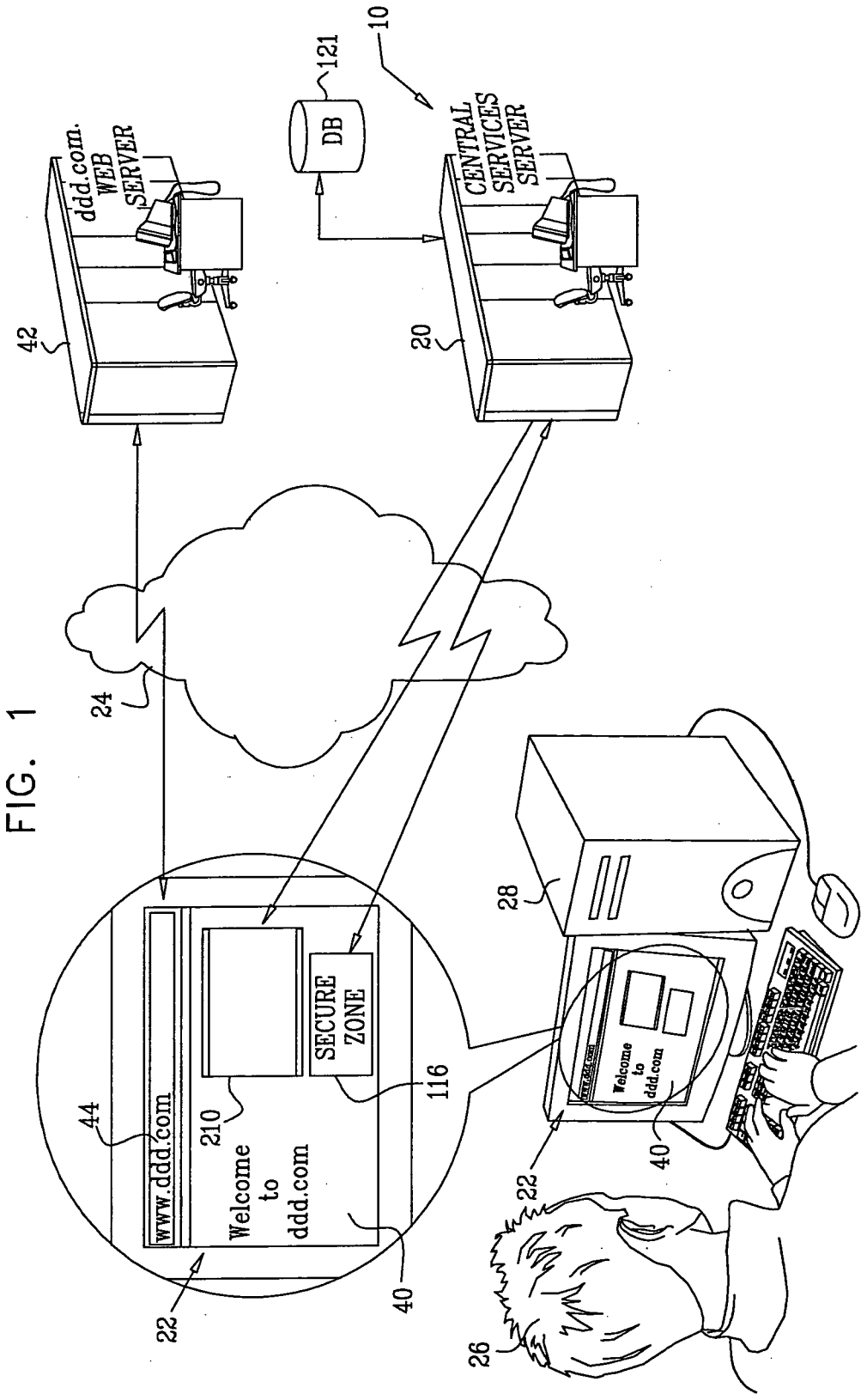

10
121
DB
ddd.com.
WEB
SERVER
CENTRAL
SERVICES
SERVER
42
20
24
28
www.ddd.com
SECURE
ZONE
44
210
116
Welcome
to
ddd.com
40
22
26

FIG. 1

FIG. 2

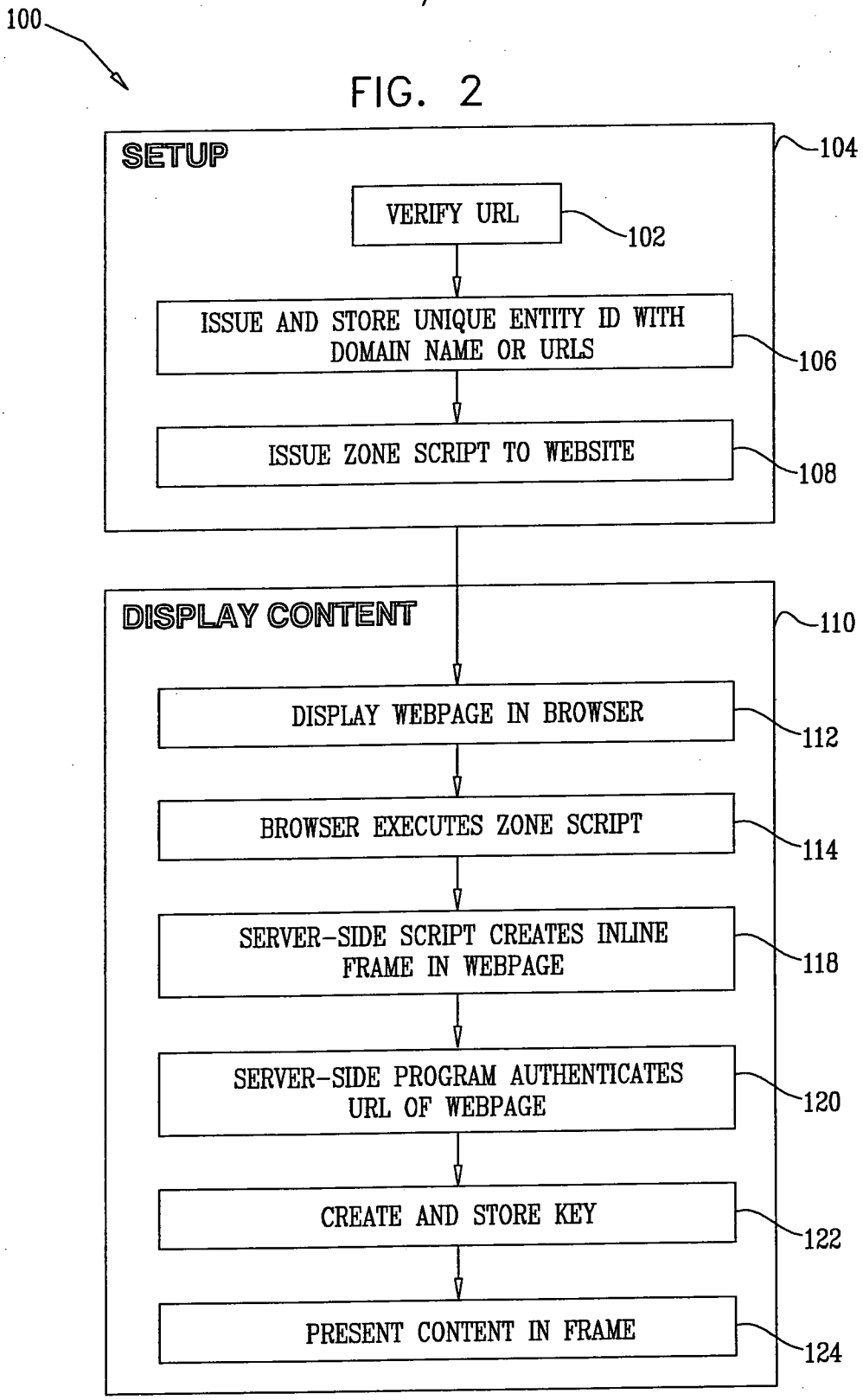
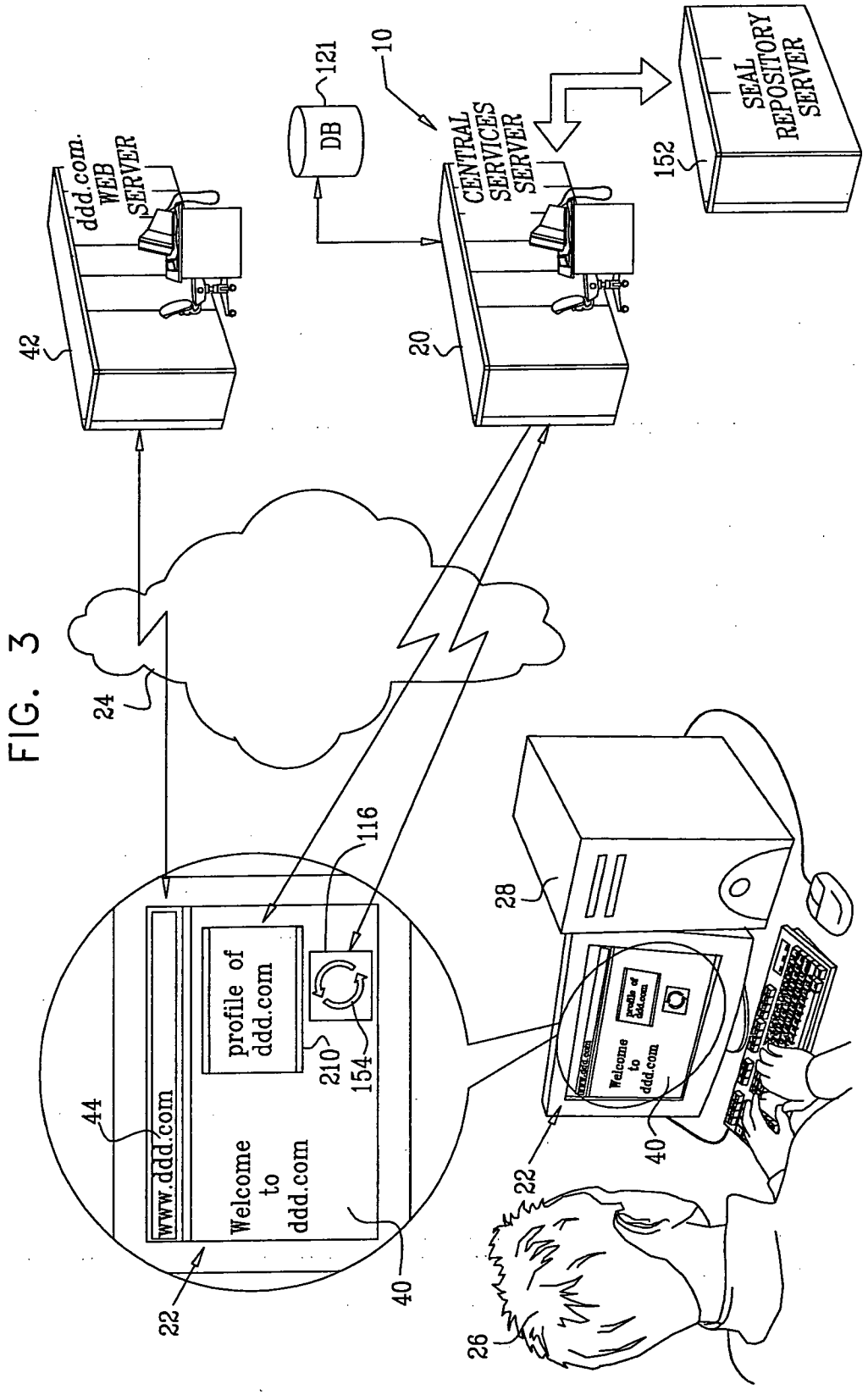

100
SETUP
104
VERIFY URL
102
ISSUE AND STORE UNIQUE ENTITY ID WITH DOMAIN NAME OR URLS
106
ISSUE ZONE SCRIPT TO WEBSITE
108
DISPLAY CONTENT
110
DISPLAY WEBPAGE IN BROWSER
112
BROWSER EXECUTES ZONE SCRIPT
114
SERVER-SIDE SCRIPT CREATES INLINE FRAME IN WEBPAGE
118
SERVER-SIDE PROGRAM AUTHENTICATES URL OF WEBPAGE
120
CREATE AND STORE KEY
122
PRESENT CONTENT IN FRAME
124

FIG. 3


ddd.com WEB SERVER
42
DB
121
10
CENTRAL SERVICES SERVER
20
SEAL REPOSITORY SERVER
152
24
116
28
www.ddd.com
profile of ddd.com
210
154
Welcome to ddd.com
44
22
40
26

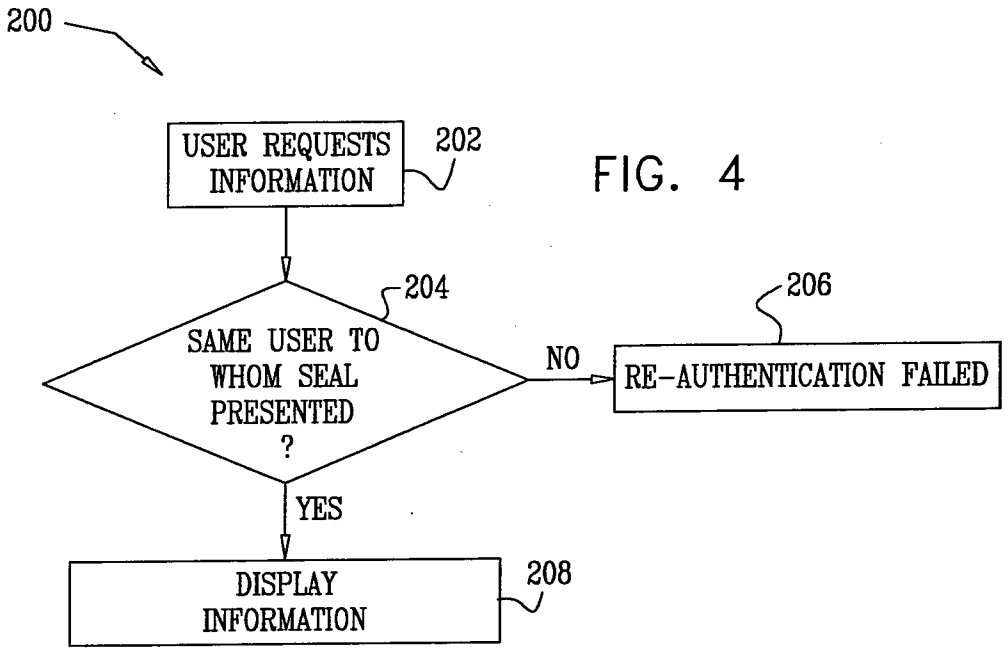

200
USER REQUESTS INFORMATION
202
204
SAME USER TO WHOM SEAL PRESENTED ?
NO
206
RE-AUTHENTICATION FAILED
YES
DISPLAY INFORMATION
208

FIG. 4

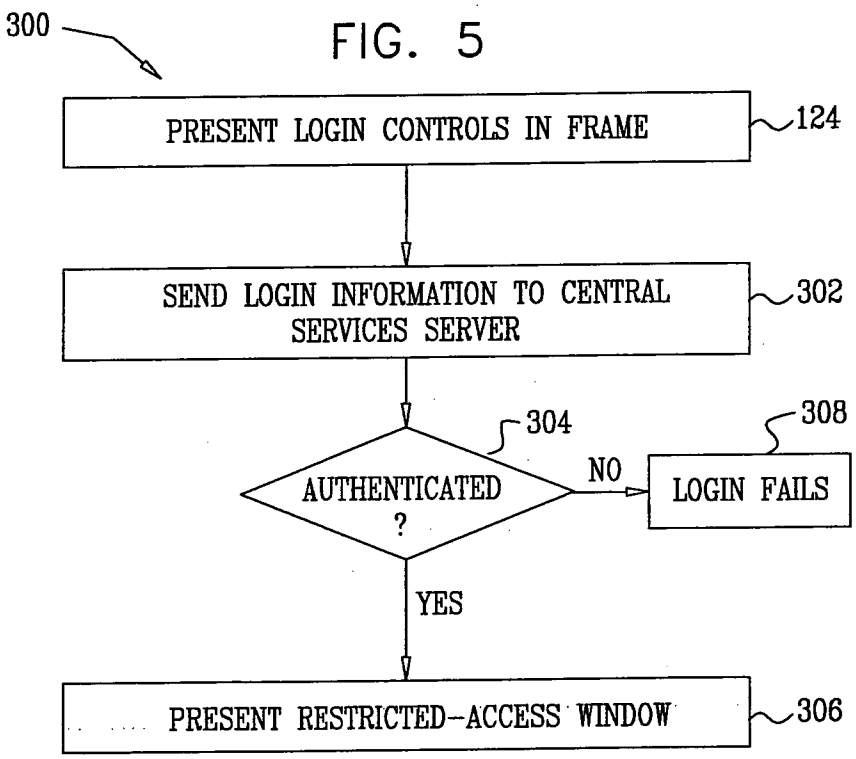
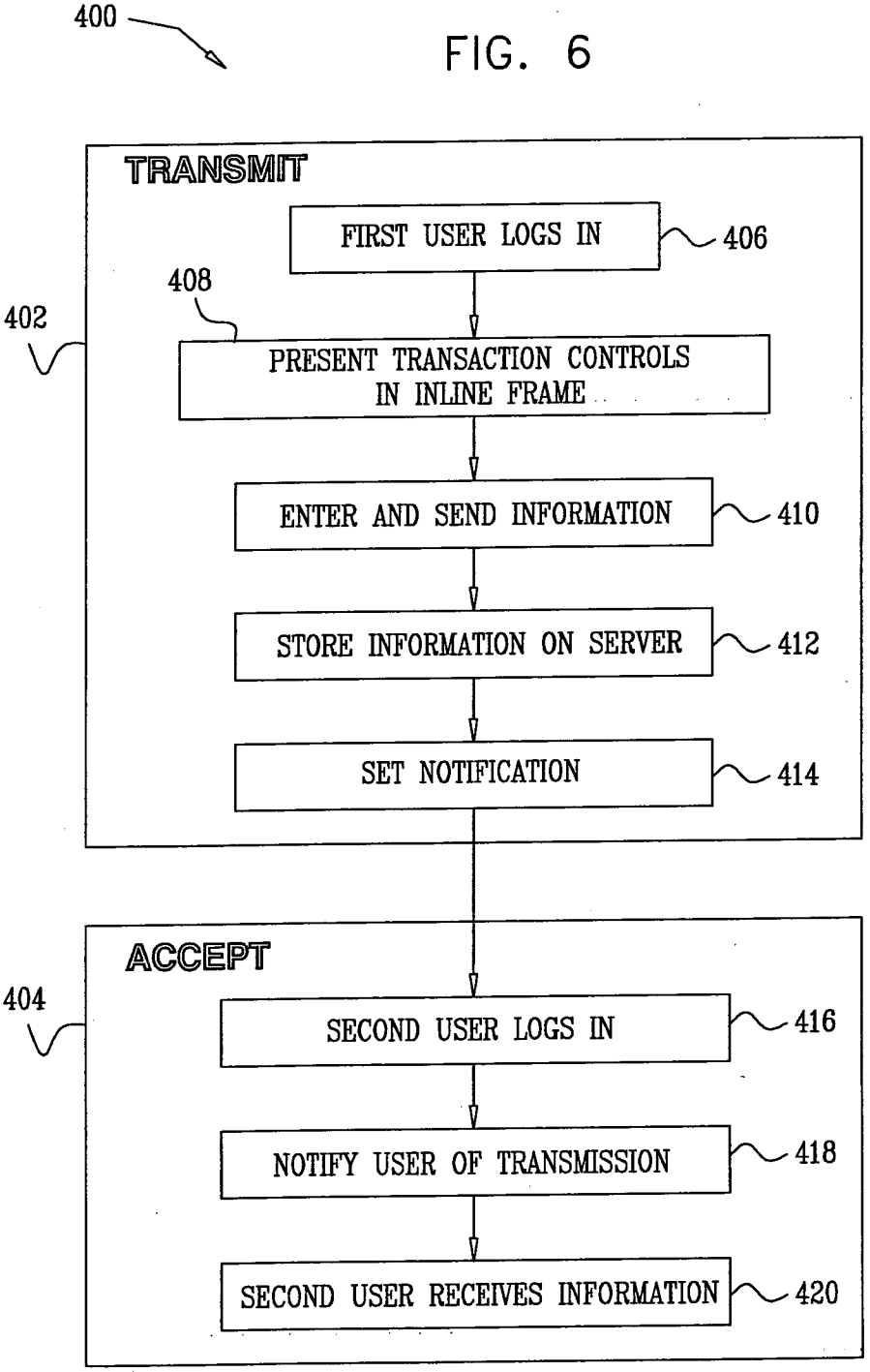

300
PRESENT LOGIN CONTROLS IN FRAME
124
SEND LOGIN INFORMATION TO CENTRAL SERVICES SERVER
302
304
AUTHENTICATED ?
NO
308
LOGIN FAILS
YES
PRESENT RESTRICTED-ACCESS WINDOW
306

FIG. 5

FIG. 6


400
TRANSMIT
FIRST USER LOGS IN
406
408
402
PRESENT TRANSACTION CONTROLS IN INLINE FRAME
ENTER AND SEND INFORMATION
410
STORE INFORMATION ON SERVER
412
SET NOTIFICATION
414
ACCEPT
404
SECOND USER LOGS IN
416
NOTIFY USER OF TRANSMISSION
418
SECOND USER RECEIVES INFORMATION
420

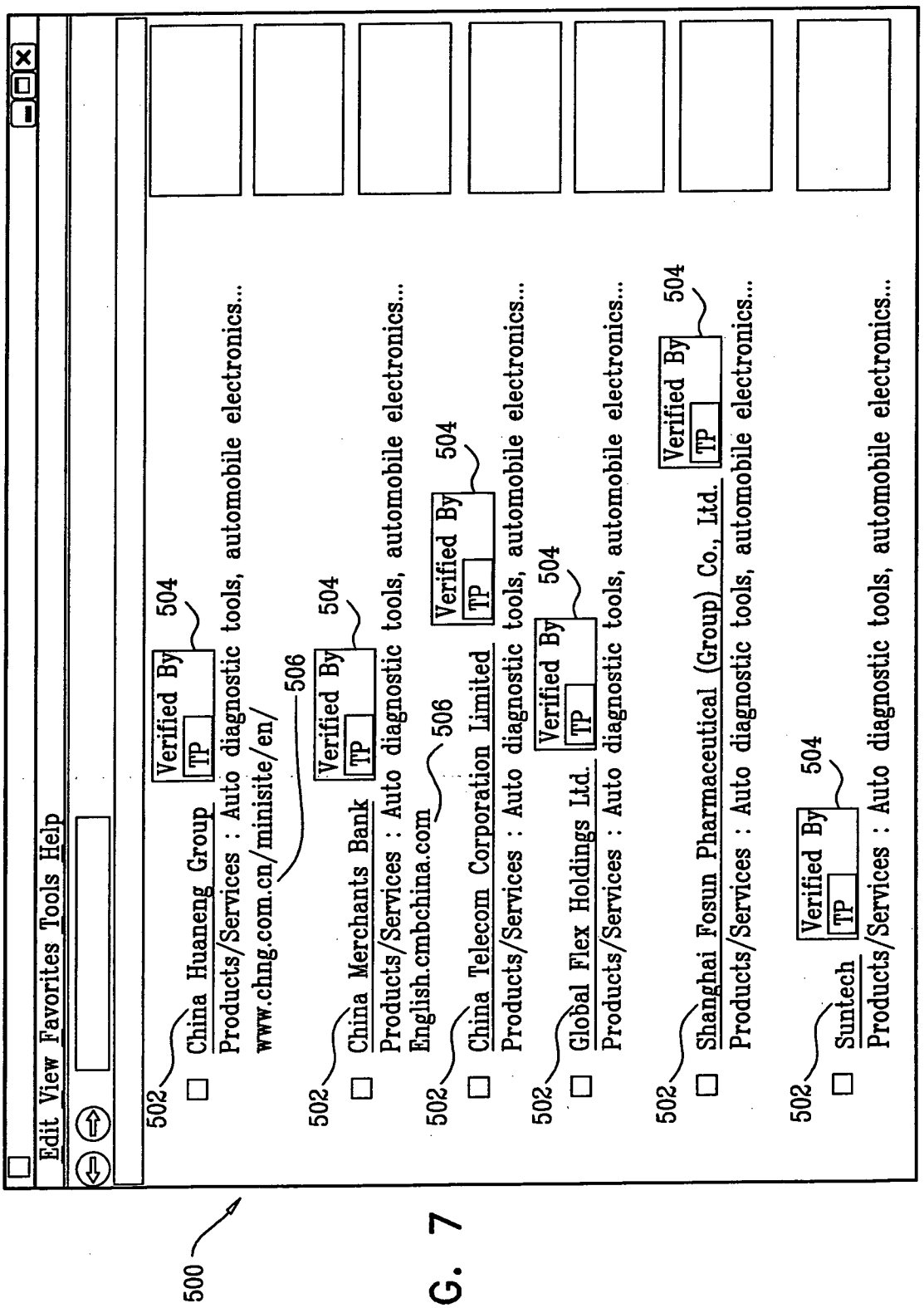

500
Edit View Favorites Tools Help
502
China Huaneng Group
Verified By TP
504
Products/Services : Auto diagnostic tools, automobile electronics...
www.chng.com.cn/minisite/en/
506
502
China Merchants Bank
Verified By TP
504
Products/Services : Auto diagnostic tools, automobile electronics...
English.cmbchina.com
506
502
China Telecom Corporation Limited
Verified By TP
504
Products/Services : Auto diagnostic tools, automobile electronics...
502
Global Flex Holdings Ltd.
Verified By TP
504
Products/Services : Auto diagnostic tools, automobile electronics...
502
Shanghai Fosun Pharmaceutical (Group) Co., Ltd.
Verified By TP
504
Products/Services : Auto diagnostic tools, automobile electronics...
502
Suntech
Verified By TP
504
Products/Services : Auto diagnostic tools, automobile electronics...

FIG. 7

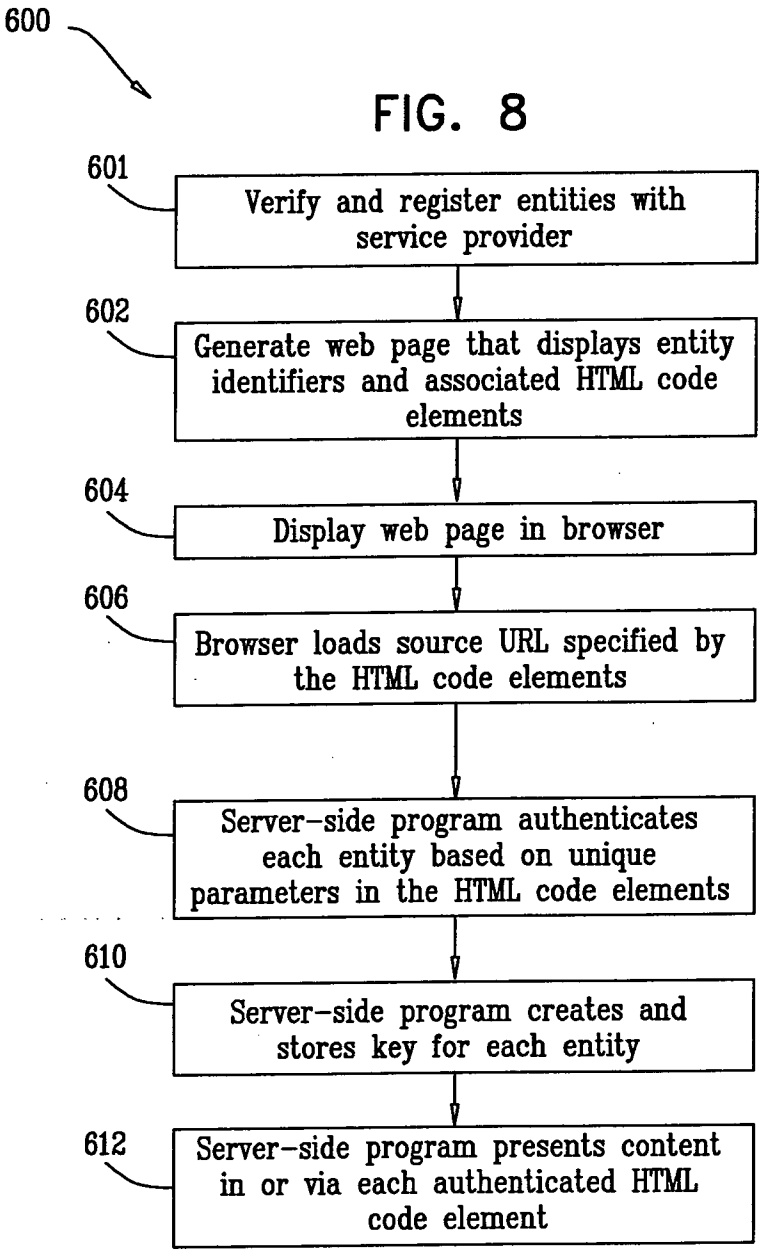

600
601
Verify and register entities with service provider
602
Generate web page that displays entity identifiers and associated HTML code elements
604
Display web page in browser
606
Browser loads source URL specified by the HTML code elements
608
Server-side program authenticates each entity based on unique parameters in the HTML code elements
610
Server-side program creates and stores key for each entity
612
Server-side program presents content in or via each authenticated HTML code element

FIG. 8