

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
14 November 2002 (14.11.2002)

PCT

(10) International Publication Number  
**WO 02/091706 A1**

(51) International Patent Classification<sup>7</sup>: **H04L 29/06**

(21) International Application Number: PCT/IL02/00349

(22) International Filing Date: 3 May 2002 (03.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/288,770 4 May 2001 (04.05.2001) US

(71) Applicant (for all designated States except US): **WHALE COMMUNICATIONS LTD.** [IL/IL]; Hamelacha St. 21, Afek Industrial Park, 48091 Rosh Ha'ayin (IL).

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

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **BARON, Elad** [IL/US]; 45 Fifth St., Cresskill, NJ 07626 (US).

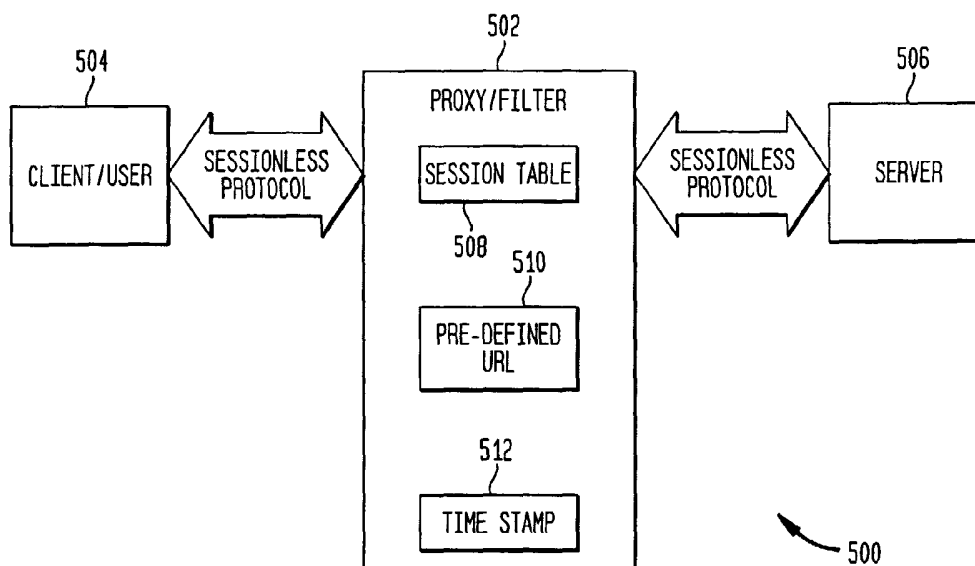
(74) Agents: **LUZZATTO, Kfir** et al.; P.O. Box 5352, 84152 Beer-Sheva (IL).

Published:

— with international search report

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

(54) Title: A METHOD AND SYSTEM FOR TERMINATING AN AUTHENTICATION SESSION UPON USER SIGN-OFF



(57) Abstract: An authentication component resides between a server and a client, or on a server, and monitors one or more transactions communicated between the server and the client. When the authentication component detects a transaction that contains a termination indication, the authentication session is terminated, forcing the client to re-authenticate the next time a transaction with the server is desired. The termination indication may have been provided by an application running on the server, or alternatively, the termination indication may be provided by the authentication component.

## **A METHOD AND SYSTEM FOR TERMINATING AN AUTHENTICATION SESSION UPON USER SIGN-OFF**

### **Cross Reference To Related Applications**

This application claims the benefit of U.S. Provisional Patent Application No. 60/288,770 filed on May 4, 2001, the entire disclosure of which is incorporated herein by reference.

### **Field of the Invention**

The present disclosure relates to a system and method for ensuring integrity of user sessions, and more particularly, to a system and method for terminating an authentication session immediately upon the authenticated user's manifestation of the user's intention to sign off from or terminate his interaction with the application.

### **Background of the Invention**

It is generally necessary for modern Web-based applications to maintain a "session". A "session" means a sequence of transactions, i.e., requests and responses sent back and forth between the Web-based application or Web server and the user. This need to maintain a session arises because Web-based applications use the HTTP protocol, which is by itself a stateless protocol, meaning that each request-response pair is independent of previous ones. This session will often be referred to as an "application session" herein.

In order to maintain an application session, some type of "token" or "ticket" must be passed by the Web browser each time a request is sent to the application in

- 2 -

order for the application to associate this request with the specific application session. Since the token remains the same in all subsequent client requests, the application identifies all such requests as part of the same application session. A "cookie" is the most commonly used type of token for this purpose, although other alternatives exist, including using a specific URL parameter as the token. In addition to serving as an application session identifier, this token sometimes contains some additional application session information.

In order to authenticate the user, a software component may be implemented which resides between the user and the Web server and authenticates the user at the beginning of each session. Authentication is often accomplished by challenging the user to provide some credentials unknown to other users. These credentials could be in the form of passwords, client certificates, or readouts from some physical devices that the user carries and can be verified at the server side. This authentication component can be implemented as a proxy, filter, or other agent well known to those skilled in the art. For example, a software component residing in front of the Web server and receiving requests on behalf of the server, and eventually passing the requests to the server and the responses from the server back to the client may be implemented. As an additional example, a software component residing on the Web server that interacts with the Web server in order to modify and/or control the request/response data-flow may be implemented.

Like the application as described above, the authentication component must also keep track of the user's session in order to preclude the need to re-authenticate the user every time a request is sent. Being in the middle of the data path between the user and the application, the authentication component could theoretically accomplish this by tracing the application session tracking process, for example, by verifying that the cookie described above continues to be passed to the application.

- 3 -

In reality, however, it usually accomplishes this via independent session tracking, using similar mechanisms. For example, a different cookie is issued by the authentication component, which is used either as a session identifier or as an encrypted authentication approval ticket (i.e., presenting this ticket along with a request approves the request). This is described in more detail in the following paragraph. As a result, re-authentication is necessary only when a new session with this authentication component is initiated. For the sake of clarity, this session will be referred to as an "authentication session" herein.

In the case of an authentication session maintained by means of a cookie or token used as a session identifier, the authentication component issues a cookie or other token to the client such as the Web browser upon the user's first request. The user's first request typically does not contain a valid token/cookie. The cookie or token issued by the authentication component contains a random number. The random number should be large enough to prevent "brute force" attacks, which attempt to find the value by guessing, from succeeding within a reasonable amount of time. The random number is used internally at the authentication component to identify an entry in a session table using a hashing algorithm. This session table contains all active sessions currently being maintained by the authentication component. In the case of an authentication session maintained by means of an encrypted authentication approval ticket, or encrypted token/cookie, whatever information would be stored in the session table described above is instead encrypted in the cookie that is sent back and forth between the browser and the authentication component together with each request and response. The authentication component uses a cryptographic key, which is unknown outside the scope of the authentication component, and it adds some fixed "salt" value to the information encrypted, which is used to verify a legitimate cookie upon decryption.

- 4 -

An issue exists with regards to termination of the authentication session. Once a user is authenticated at a terminal, it is assumed that all subsequent requests that that terminal issues come from that authenticated user. Accordingly, it is critical that when the user finishes his interaction with the application, the authentication session terminates, so that a new user at that terminal will not be mistakenly assumed to be already authenticated. This is particularly important when the user is logging in from public spaces such as Internet cafes, airports, etc. Since there is no standard method of logging off from a Web-based application, most authentication mechanisms utilize some form of a "time-out" mechanism, whereby if a user does not interact with the application for a certain amount of time, for example, 10 minutes, the authentication session expires. Alternatively, some authentication mechanisms implement a fixed time-out, which allows the session to stay alive for a certain amount of time, regardless of user activity. However, such mechanisms are inadequate in public spaces where a stranger can take control of the browser a moment after a legitimate user has ostensibly signed off. This problem is exacerbated where public Internet access facilities "lock down" their browsers (i.e., the browser cannot be closed), since in that case the user cannot even terminate the session by closing the browser (which would typically discard its cookies when closed).

Moreover, despite the fact that an application may contain some type of log-off button or URL which is intended to terminate the application session (not to be confused with the authentication session), such termination typically would have no effect on the authentication mechanism because existing authentication mechanisms are unaware of the application's log-off mechanism, and therefore the authentication mechanism would not terminate the authentication session. As a result, the next person using the same browser could be implicitly authenticated by the authentication component since a legitimate cookie would be sent to the

- 5 -

authentication component. This would allow a malicious user to interact with the supposedly protected application (even though engaging possibly in a new application session) without first authenticating his identity via the authentication component's authentication mechanism. Thus, while the application may have its own authentication feature (e.g., a user name and password) which would provide some level of protection against this malicious user, the superior authentication provided by the authentication component's authentication mechanism would be bypassed. In the case of an application that provides HTTP Basic Authentication, the potential to bypass the authentication component's authentication mechanism would leave the application particularly vulnerable, since there exists an inherent vulnerability in HTTP Basic Authentication resulting from the fact that the Web browser saves the user names and passwords of previous users who have accessed a site.

Therefore, it is highly desirable to have a system and method for allowing an immediate authentication session termination when the legitimate user signs off. In addition, it is also desirable that this system and method allow immediate session termination even if the application itself does not inherently support a sign-off feature.

### **Summary of the Invention**

A system and method, and/or a program storage device, for terminating an authentication session immediately following the user's manifestation of his intention to terminate his interaction with an application is provided. In one aspect, user's requests are monitored until a pre-defined URL is requested by the user. The authentication session after such URL is requested is then terminated.

- 6 -

This URL may be either a pre-existing URL in the application, or a URL presented by the authentication component for this purpose.

### **Brief Description of the Drawings**

Preferred embodiments will now be described, by way of example only, with reference to the accompanying drawings. Like reference numbers indicate identical or functionally similar elements.

Figure 1 is a flow diagram illustrating an example of initiating a typical authentication session in one embodiment;

Figure 2 is a flow diagram illustrating an example of monitoring for authentication termination requests in one embodiment;

Figure 3 is a flow diagram illustrating an example of terminating an authentication session in one embodiment when an application provides a session termination procedure;

Figure 4 is a flow diagram illustrating an example of terminating an authentication session in one embodiment when an application does not provide a session termination procedure; and

Figure 5 is a diagram illustrating various components in the system for terminating an authentication session.

### **Detailed Description of Preferred Embodiments**

Typically, a session table that is maintained at an authentication component contains all active sessions currently being maintained by the authentication component. If an entry in the session table is deleted, or marked "expired," the session is effectively broken, since a new request by the client does not carry a valid cookie (or other token). That is, the cookie content does not map anymore to an active entry in the session table, and therefore the new request would force a re-

- 7 -

authentication of the user. The authentication process itself involves getting some credentials from the user and verifying them against some expected values before proceeding to create a corresponding entry in the session table. This process of checking the user's credentials is described in U.S. Patent No. 5,097,505, U.S. Patent No. 5,168,520, and U.S. Patent No. 5,657,388.

Since an authentication component typically receives all HTTP requests from the client and passes them to the Web server, the authentication component can make decisions based on the content of these requests. In one embodiment, the authentication component monitors these requests, and when it detects a manifestation by the user of the user's intention to terminate his interaction with the application (a "termination indication"), the authentication component initiates a session termination sequence, which results in the deletion of the relevant entry from the session table, thereby rendering the authentication session expired. The termination indication may take the form a request for a specific URL, for example, which was pre-defined at authentication component configuration. Such URL shall be referred to as the "authentication session termination URL". If the application itself happens to provide the user with some type of log-off button or URL which is intended to terminate the application session (not to be confused with the authentication session), then this same URL may serve as the authentication session termination URL. This, as well as the scenario in which the application does not provide such a log-off mechanism, will be described in further detail in the following paragraphs.

In one aspect, an authentication component residing between the user and the application may take the form of a proxy implementation, a filter implementation, or another agent well known to those skilled in the art. Solely for the sake of explanation, in the following description the method and system is often

- 8 -

described in the context of a proxy implementation. Those skilled in the art of computer programming, however, will appreciate that the implementation need not be in the form of proxy only. A proxy generally authenticates a user upon the first attempt by the user to reach the application, from which point the proxy maintains an authentication session. A system and method provided terminates this session immediately following the user's ending an interaction with the application. The system and method provided may be used alone as an alternative to, or supplement the conventional methods described above that are based on inactivity or scheduled timeouts.

Figure 1 is a flow diagram illustrating an example of initiating a typical authentication session in one embodiment. At 102, a user tries to initiate a session by sending a request to an application. At 103, an authentication component, for example, proxy, inspects this request to determine whether it includes a valid cookie or token. If not, then the authentication component challenges the user to provide authentication credentials at 104. At 106, if the credentials are valid, then the authentication component creates a new cookie or other token for the user for this session. The authentication component may alternatively create a corresponding entry in the session table. At 107, the authentication component forwards the user request to the application, and at 108, monitors the application session until the application responds. At 109, when the application responds the authentication component attaches the cookie to the response and passes this to the user. Subsequent requests are similarly inspected to verify that they contain a valid token. Thus, the authentication component also forwards any subsequent user requests carrying a valid cookie/token to the application.

Figure 2 is a flow diagram illustrating an example of monitoring for authentication termination requests in one embodiment. Once a session has been

- 9 -

verified at 202, for example, as described with reference to Figure 1, the authentication component inspects every user request as shown at 203 to determine whether the request is for the authentication session termination URL as shown at 204. If it is not, at 205, the authentication component continues to pass the requests to the application. Once the authentication session termination URL is requested, however, the authentication component begins the session termination sequence.

This sequence may vary depending, *inter alia*, on whether the application itself provides for a log-off button or other URL which is intended to terminate the application session or otherwise is identified as the application session termination URL. Accordingly, at 207, depending on whether the authentication component was configured to use an existing application URL as a termination trigger, the processing then continues as will be described with reference to Figures 3 and 4.

In one embodiment, if an application itself provides a termination procedure such as a log-off URL, the application-provided URL may be configured at the proxy and used as an authentication session termination URL. Accordingly, at 208, the processing continues to Figure 3. Figure 3 is a flow diagram illustrating an example of terminating an authentication session in one embodiment when an application provides a session termination procedure. In one embodiment, if an application has an embedded "log-off" or other URL, the authentication component predetermines this URL as an authentication session termination URL. The authentication component then monitors the user requests for this predetermined URL. When the authentication component detects a request for the authentication session termination URL, the authentication component marks the authentication session as "termination pending" in the session table as shown at 301. At 302, the authentication component passes the URL request to the application. At 303, the

- 10 -

authentication component monitors the application session until the application responds with the page corresponding with such request, for example, its log-off page. At 304, the authentication component passes a log-off page either the application's log-off page received from the application or a log-off page generated by the authentication component which authentication component discards the application's log-off page to the user and then immediately terminates the authentication session by deleting the corresponding session entry from the session table at 305. New user requests are now forced to re-authenticate, for example, as per Figure 1.

In one embodiment, if the reply, for example, the application's log-off page, itself contemplates additional requests and responses, such as images, etc., then the session may be terminated either (i) immediately (ii) after a pre-defined set of requests and/or responses have been made (this set may be defined using lists of URLs, regular expressions, MIME types, file extensions, or any other content-based rules); (iii) after a pre-defined number of requests and/or responses have been made; or (iv) immediately after the first request is made that does not fit within a pre-defined set of requests (an "invalid request").

Alternatively, as soon as the authentication session termination URL is requested by the user, the authentication component, for example, a proxy, may terminate the session by deleting its entry from the session table, without first passing this URL request to the application. In one aspect, a proxy may terminate the session immediately after passing the URL request to the application, without waiting for the application to reply with its response.

Additional improvements to this process may include any or a combination of the following described features. For example, a timeout restriction feature may be

- 11 -

included. This feature would automatically break an authentication session after a pre-defined period of time after the request for the authentication session termination URL is submitted by the user. This timeout restriction would occur, for example, even if the application response, for example, the log-off page, does not come or not all of the additional allowed requests/responses arrive. This timeout restriction may be implemented in one embodiment by storing a time stamp value at the time when the session entry of "termination pending" is entered. Thereafter, the time stamp value may be monitored either periodically or on each following user request. When the pre-defined time period passes, a proxy may delete the session entry. The timeout restriction may also be implemented by triggering a scheduled interrupt which when activated, deletes the session entry if the entry is still active.

Additional features may include data traffic restrictions. For example, a proxy may disallow the passage of any new user requests while in "termination pending" mode, except requests and corresponding responses that are part of the application's response to the authentication session termination URL, such as images, etc. This may be achieved by monitoring subsequent requests and rejecting (i.e., not forwarding to the application) any request other than a pre-defined set of requests. This set may be defined using lists of URLs, regular expressions, MIME types, file extensions, or any other content-based rules. If the application's log-off page does not provide for any subsequent requests or responses, then a proxy may simply disallow the passage of any user requests once the log-off request has been made.

Yet another feature may include data traffic restrictions with proxy-generated responses. With this feature, when a proxy detects that the user has requested the authentication session termination URL, the proxy generates and serves its own log-off page or similar response to the user and does not pass (but

- 12 -

rather discards) any application-generated response to the user. The proxy may still pass the authentication session termination URL to the application. The proxy-generated log-off page may include additional images and options. The proxy then acts as the server with respect to this log-off page and requests and responses related thereto. Thus, once the log-off request has been made by the user, the proxy may disallow the passage of any new requests from the user to the application; however, it continues to respond to requests that are part of the proxy-generated log-off page, such as images, etc., by serving the pages that correspond to those requests.

Alternatively, or in addition, once the log-off request has been made by the user, the proxy can be pre-configured to act as a client, emulating the user, with respect to the application by engaging in certain requests and responses with the application (without necessarily passing any responses to the user). At the same time or alternatively, the proxy may act as a server with respect to the user, providing responses to the user that may or may not be identical to those provided by the application.

As an alternative to using the cookie or other token to identify an entry in a session table as described above, the method can be similarly implemented in the case of an authentication session maintained by use of an encrypted token/cookie. In that case, the termination of the authentication session would be accomplished not by deleting an entry from a session table but by one of the following methods: (i) the proxy instructs the browser to stop sending the cookie; or (ii) the proxy enters the cookie content into a table that contains all disallowed cookies, such that any cookie whose content maps to such table is thus identified as an invalid cookie, thereby forcing a re-authentication of the user whose request included that cookie.

- 13 -

Figure 4 is a flow diagram illustrating an example of terminating an authentication session in one embodiment when an application does not provide a session termination procedure. Where the application does not have any embedded "log-off" or similar URL, the authentication component, having detected a request for the authentication session termination URL, does not pass this request to the application but instead serves its own pre-configured log-off page to the user as shown at 401. At 402, the authentication component then immediately terminates the authentication session by, for example, deleting the corresponding session entry from the session table. New user requests are now forced to re-authenticate, for example, as per Figures 1 and 2.

In one embodiment, a proxy may monitor all of the responses coming from the Web server to the browser during the application session. Before passing each HTTP response to the browser, the proxy may add, for example, a "button" to the HTML portion of the response. The button, which would appear to the user as a "log-off" or similar button, may be added either only to pre-defined specific pages, or to all HTML pages. Alternatively, the proxy can make use of "frames" and, for example, append a frame to the first HTML page requested by the user, and include this button or similar mechanism within such frame. This button contains, for example, a reference, or link, to the authentication session termination URL. Once the user clicks on this link, a request with that URL is transmitted. The proxy receives the URL before it reaches the server.

Alternatively, a proxy may not add any button to the server's responses, but the proxy may still monitor the user's requests for a specific pre-defined URL. A user is, for example, given the pre-defined URL to use for terminating a session. The user, for example, may type the URL manually. Regardless of how the user requests this authentication session termination URL, i.e., by clicking a link or by

- 14 -

typing it, or in some other manner, the proxy detects this URL request before the request reaches the server and sends back a pre-defined response page, in the form of a log-off page, to the user. It then breaks the authentication session immediately. The proxy does not pass this URL request to the application as in the previous case, since the application is not aware of this URL. As described above, the application is not aware of this URL since such URL was either added by the proxy to the response after the response left the application, or such URL was manually requested by the user.

Additionally, a data traffic restriction together with a proxy-generated response, as described above, may be implemented. If the proxy-generated log-off page includes additional images and options, then the session may be terminated either (i) immediately after the log-off page is served to the user; (ii) after a pre-defined period of time after the request for the authentication session termination URL is submitted by the user; (iii) after a pre-defined set of requests and/or responses have been made, which set may be equivalent to, or may be a subset of, the entire set of possible requests and responses contemplated by the proxy-generated log-off page; or (iv) after a pre-defined number of requests and/or responses have been made, which number may equal, or may be lower than, the entire number of possible requests and responses contemplated by the proxy-generated log-off page.

Figure 5 is a diagram illustrating components of the authentication session termination system in one embodiment. An authentication component, for example, a proxy or filter, resides between a client 504 and a server 506. The authentication component may include a session table 508 for storing sessions in progress for each client. The session table may also include a pre-defined URL 510 that indicates that a session should be terminated. The session table may also include a

- 15 -

timestamp 512. As will be appreciated by those skilled in the art of computer programming, the data in the session table, pre-defined URL, and time stamp may be organized as row and columns of a table, as separate tables with links into one another, as a data structure or linked list format, or any other data storage method known. The authentication component 502 may reside with the server 506 or as a part of client system 504 or run between the server 506 and the client 504. The authentication component 502 monitors requests and responses communicated between the client 504 and the server 506, and when a pre-defined URL is detected, the authentication component proceeds to terminate the session, for example, according to embodiments described with reference to Figures 1-4.

Although the description of the system and method herein has been presented in the context of a proxy implementation solely for the sake of explanation, other components such as filters may be used to implement the system and method disclosed, including claimed improvements, alternatives and modifications thereto. In addition, although the system and method for terminating an authentication session is described herein with respect to the World Wide Web and HTTP transactions, those skilled in the technological art will appreciate that the present system and method may also be used in any other transactions and protocols where beginning and end of sessions are not maintained by client or server systems. Moreover, while the present invention has been described with reference to several embodiments thereof, those skilled in the art will recognize various changes that may be made without departing from the spirit and scope of the claimed invention. Accordingly, this invention is not limited to what is shown in the drawings and described in the specification but only as indicated in the appended claims.

CLAIMS:

1. A method for terminating an authentication session following a user's indication that the user intends to terminate user's interaction with an application independent of the application comprising:

monitoring a request for a termination indication from a user in one or more transactions between a user and an application; and

terminating an authentication session in response to receiving the termination indication.

2. The method of claim 1, wherein the termination indication includes a predefined URL.

3. The method of claim 1, further including entering a session entry in an authentication session table when an authentication session begins.

4. The method of claim 1, wherein the terminating includes deleting a session entry from an authentication session table.

5. The method of claim 1, wherein the terminating includes marking a session entry in an authentication session table as expired.

6. The method of claim 1, wherein the terminating includes denoting an encrypted token associated with the authentication session as invalid.

7. The method of claim 1, wherein the terminating includes entering a session cookie associated with the authentication session into a table of disallowed cookies.

- 17 -

8. The method of claim 1, wherein the terminating includes detecting a predetermined parameter appended to the request.

9. The method of claim 1, further including entering a session entry, corresponding to a URL parameter, in an authentication session table when an authentication session begins.

10. The method of claim 1, wherein the termination indication has a pre-existing function in the application.

11. The method of claim 1, wherein the termination indication includes one or more pre-existing logoff URLs provided by the application.

12. The method of claim 1, wherein the terminating includes terminating the authentication session after communicating one or more transactions between the user and the application.

13. The method of claim 1, wherein the terminating includes:  
marking an authentication session as termination pending in a session table;  
communicating the transaction having the termination indication to the application;  
continuing to monitor the transactions until the application replies with a response to the termination indication; and  
terminating the authentication session.

14. The method of claim 13, wherein only predetermined transactions are permitted during the terminating.

- 18 -

15. The method of claim 13, wherein the terminating includes deleting an entry associated with the authentication session from the session table.

16. The method of claim 13, wherein the terminating includes marking a session entry in an authentication session table as expired.

17. The method of claim 13, wherein the terminating includes denoting an encrypted token associated with the authentication session as invalid.

18. The method of claim 13, wherein the terminating includes entering a session cookie associated with the authentication session into a table of disallowed cookies.

19. The method of claim 1, wherein the terminating includes terminating the authentication session after a predetermined period of time has passed after receiving the termination indication.

20. The method of claim 19, wherein the terminating includes allowing only a predetermined set of transactions to be communicated between the user and the application during the predetermined period of time.

21. The method of claim 19, wherein the terminating includes, after receiving the termination indication, terminating the authentication session upon the earlier of the expiration of the predetermined period of time or an invalid request is received from the user.

- 19 -

22. The method of claim 1, wherein the terminating includes terminating the authentication session after the first request is received from the user that is not among a predefined set of allowed requests or is one of a predefined set of disallowed requests.

23. The method of claim 1, further including:  
after receiving the termination indication, denoting the authentication session as termination pending;

allowing prior to terminating the authentication session one or more predefined transactions between the user and the application; and  
terminating the authentication session.

24. The method of claim 1, wherein the terminating includes:  
denoting the authentication session as termination pending; and

allowing one or more pre-defined URL requests and responses to and from the user and the application.

25. The method of claim 24, wherein the one or more pre-defined URL requests and responses include one or more requests and responses used for an application's logoff sequence.

26. The method of claim 1, further including presenting a logoff indication to the user in response to receiving the termination indication.

27. The method of claim 1, further including:

presenting in response to receiving the termination indication a logoff page to the user that includes additional options for the user;

- 20 -

intercepting one or more transactions from the user after presenting said logoff page; and

responding to the one or more transactions before terminating the authentication session.

28. The method of claim 26, further including discarding one or more application-generated responses to the user in response to receiving the termination indication.

29. The method of claim 27, further including allowing only selected, pre-defined requests from the user to the application after the presenting and before terminating.

30. The method of claim 1, further including disallowing a request from the user to the application after receiving the termination indication.

31. The method of claim 1, further including:  
monitoring one or more transactions from the application;  
adding a predefined data segment to the one or more transactions received from the application; and

transmitting to the user the one or more transactions having the added predefined data segment to present to the user an option to send the termination indication.

32. The method of claim 31, wherein the data segment includes a reference to an HTML log-off image that the user can select when the user intends to terminate the session.

- 21 -

33. The method of claim 32, wherein the HTML log-off image is presented in an HTML frame that remains in the browser display area throughout the session.

34. The method of claim 1, further including communicating the termination indication to the application after terminating an authentication session.

35. The method of claim 1, further including:

intercepting and not transmitting to the application one or more subsequent requests from the user to the application after receiving the termination indication; and

replying to one or more of the subsequent requests.

36. The method of claim 1, further including:

intercepting and not transmitting to the user one or more subsequent transactions from the application to the user after receiving the termination indication; and

sending one or more subsequent transactions to the application to emulate the user.

37. The method of claim 1, further including:

intercepting one or more subsequent user requests after receiving the termination indication;

sending, to emulate the user, one or more pre-defined subsequent requests to the application that are determined by but not necessarily identical to the one or more subsequent user requests; and

replying to one or more of the one or more subsequent user requests.

38. A system for terminating an authentication session, comprising:

- 22 -

a session entry table having one or more entries of valid sessions, and

an authentication component residing between a client and a server running an application, said authentication component monitoring transactions between the client and the server and in response to receiving a termination indication of a session initiating a termination sequence.

39. The system of claim 38, wherein the termination sequence includes deleting an entry associated with the session in the session entry table.

40. The system of claim 38, wherein the authentication module is a proxy.

41. The system of claim 38, wherein the authentication module is a filter.

42. The system of claim 38, wherein the one or more entries include one or more cookies.

43. The system of claim 38, wherein the one or more entries include one or more encrypted tokens.

44. The system of claim 38, wherein the one or more entries include one or more URL parameters.

45. The system of claim 38, wherein the termination indication includes a log-off URL.

46. A method for terminating an authentication session, comprising:  
validating a client transaction to begin a session between a client and an application;

- 23 -

entering a valid session entry in a session table;  
monitoring one or more transactions between the client and the application during the session;  
detecting a predefined termination indication in the one or more transactions;  
deleting the valid session entry in the session table.

47. The method of claim 46, further including:  
waiting for a predetermined period of time to pass before the deleting.

48. The method of claim 46, wherein the deleting the session entry includes marking the session entry as invalid.

49. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps of terminating an authentication session, comprising:

validating a client transaction to begin a session between a client and an application;

entering a valid session entry in a session table;

monitoring one or more transactions between the client and the application during the session;

detecting a predefined termination indication in the one or more transactions;

deleting the valid session entry in the session table.

50. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps of terminating and authentication session, comprising:

monitoring a request for a termination indication from a user in one or more transactions between a user and an application; and

- 24 -

terminating an authentication session in response to receiving the termination indication.

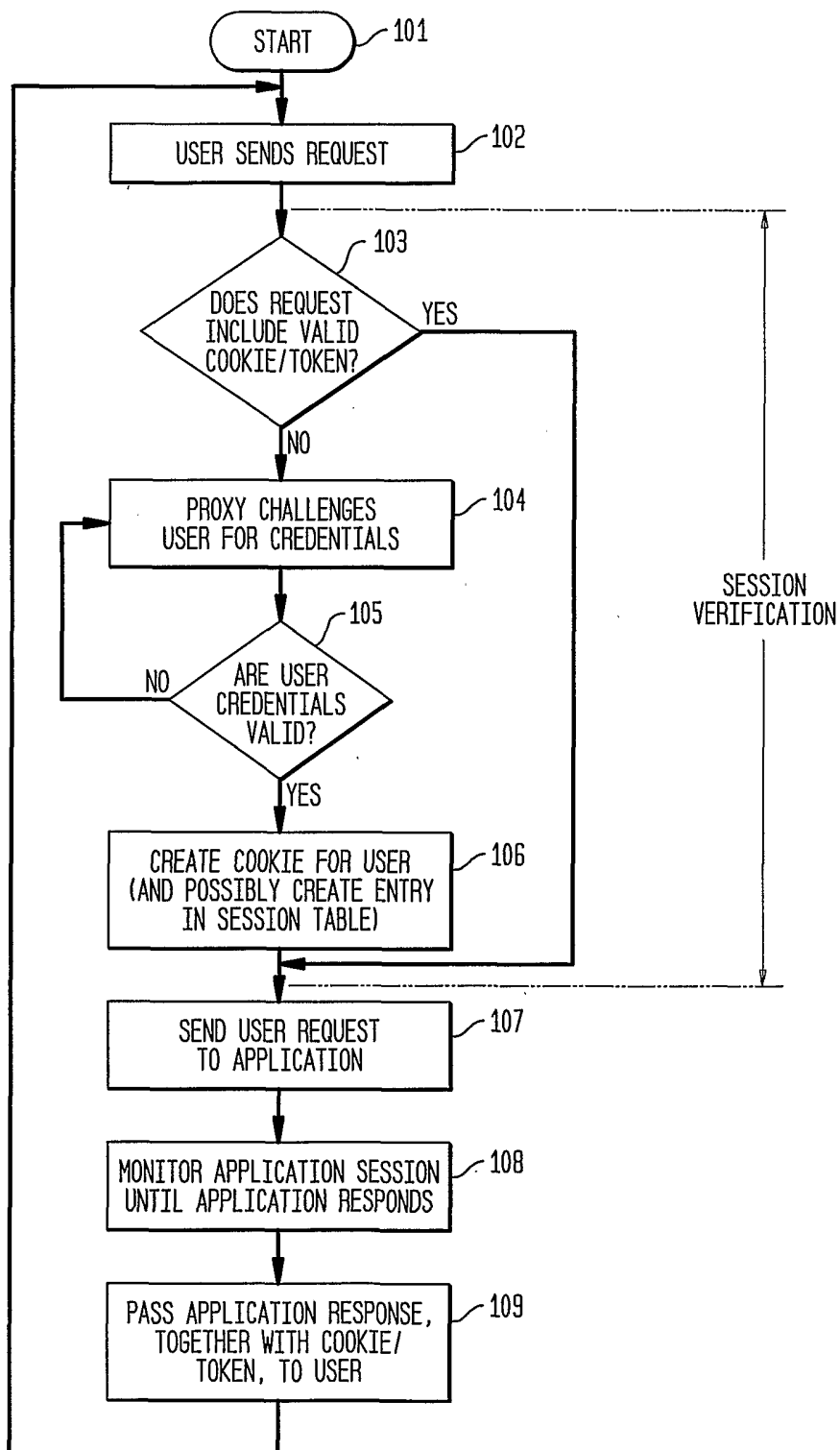
51. The program storage device of claim 50, wherein the terminating includes:

marking an authentication session as termination pending in a session table;  
communicating the transaction having the termination indication to the application;

continuing to monitor the transactions until the application replies with a response to the termination indication; and

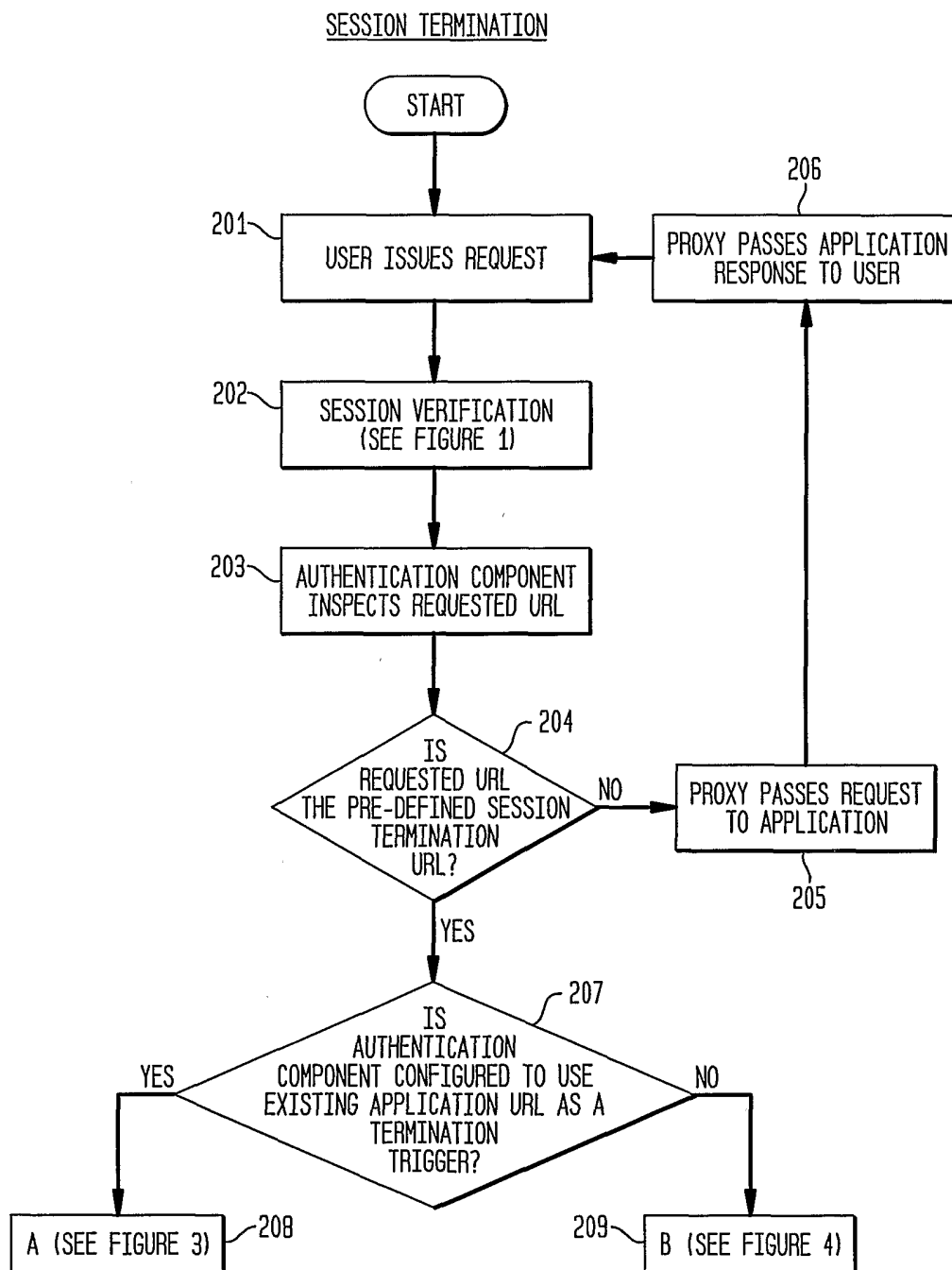
terminating the authentication session.

1/4

**FIG. 1** INITIATION OF SESSION/SESSION VERIFICATION

2/4

FIG. 2



3/4

FIG. 3

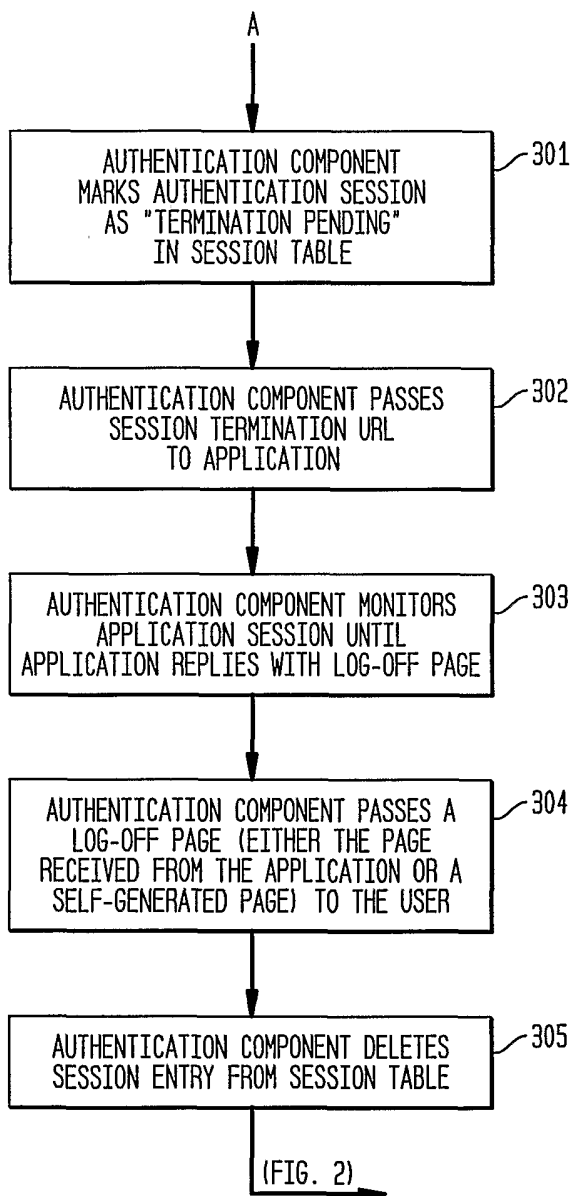
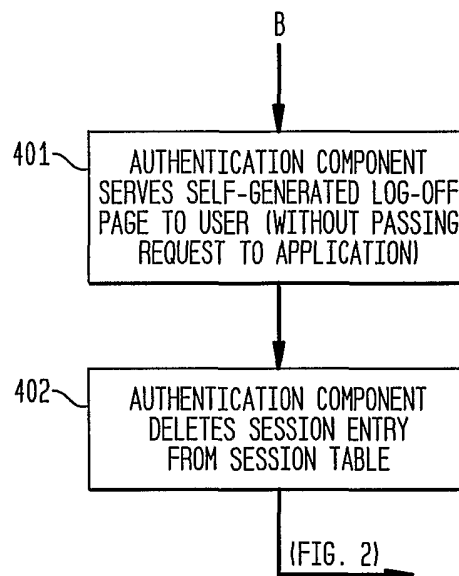
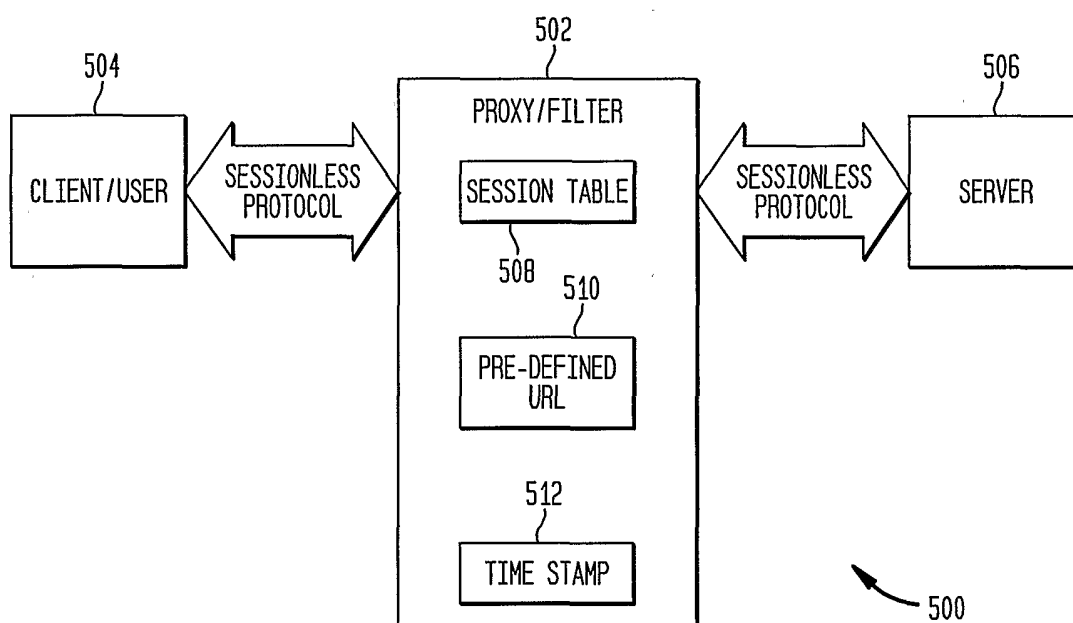


FIG. 4



4/4

FIG. 5



## INTERNATIONAL SEARCH REPORT

International Application No  
PCT/IL 02/00349

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 H04L

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

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

EPO-Internal, WPI Data, PAJ

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 226 752 B1 (GUPTA ABHAY ET AL) 1 May 2001 (2001-05-01) abstract column 11, line 10 -column 12, line 12 column 13, line 41 -column 14, line 50 ---	1-51
X	US 5 884 312 A (DUSTAN ROBERT FREDERICK ET AL) 16 March 1999 (1999-03-16) column 2, line 16 - line 31 column 3, line 15 - line 25 column 3, line 62 -column 4, line 13 column 12, line 23 - line 35 column 13, line 60 -column 14, line 11 column 14, line 51 -column 15, line 15 column 19, line 23 - line 64 --- -/--	1-51

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \* & \* document member of the same patent family

Date of the actual completion of the international search

26 July 2002

Date of mailing of the international search report

06/08/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Lebas, Y

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/IL 02/00349

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 161 182 A (NADOOSHAN MEHRDAD JAMEI) 12 December 2000 (2000-12-12) abstract column 2, line 29 -column 3, line 25 column 7, line 31 -column 8, line 35 -----	1-51
A	US 6 205 479 B1 (VITALE BENJAMIN F ET AL) 20 March 2001 (2001-03-20) abstract column 3, line 62 -column 4, line 12 column 5, line 12 -column 5, line 45 column 6, line 32 - line 45 -----	1-51

## INTERNATIONAL SEARCH REPORT

International Application No  
PCT/IL 02/00349

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 6226752	B1	01-05-2001	AU 4986200 A EP 1177654 A1 WO 0069110 A1 US 2001037469 A1	21-11-2000 06-02-2002 16-11-2000 01-11-2001
US 5884312	A	16-03-1999	AU 6182698 A WO 9838776 A1	18-09-1998 03-09-1998
US 6161182	A	12-12-2000	NONE	
US 6205479	B1	20-03-2001	AU 3557399 A CA 2328379 A1 EP 1076859 A1 WO 9953408 A1 US 2001007996 A1	01-11-1999 21-10-1999 21-02-2001 21-10-1999 12-07-2001