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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 April 2013 (11.04.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/052693 A1

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

(21) **International Application Number**:
PCT/US2012/058789

(22) **International Filing Date**:
4 October 2012 (04.10.2012)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
13/252,931 4 October 2011 (04.10.2011) US

(71) **Applicant**: **QUALCOMM INCORPORATED** [US/US]; Attn: International Ip Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) **Inventors**: **FLANAGAN, Jessica M.**; 5775 Morehouse Drive, San Diego, California 92121 (US). **BROWN, Craig M.**; 5775 Morehouse Drive, San Diego, California 92121 (US). **PADDON, Michael W.**; 5775 Morehouse Drive, San Diego, California 92121 (US).

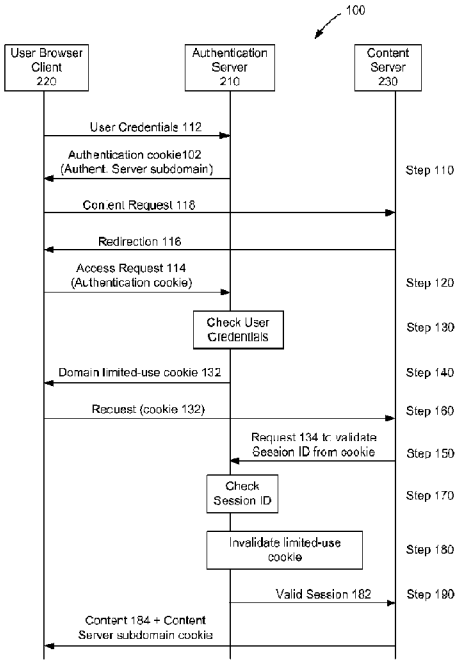
(74) **Agent**: **KIM, Won Tae**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) **Title**: METHOD AND APPARATUS FOR PROTECTING A SINGLE SIGN-ON DOMAIN FROM CREDENTIAL LEAKAGE



(57) **Abstract**: Disclosed is a method for protecting a single sign-on domain from credential leakage. In the method, an authentication server (210) provides an authentication cookie (102) to a browser client (220). The cookie has an authentication credential for the domain, and is associated with an authentication subdomain of the domain. The server (10) receives the cookie from the browser client (114). Upon authentication of the user authentication credential in the received cookie, the server (210) responds to the access request by forwarding, to the browser client, a limited-use cookie for the domain (132). The server (210) receives a request (134) from the content server (230) to validate a session identifier of the limited-use cookie received from the browser client. Upon validation, the server (210) provides a valid session message (182) to the content server (230) for enabling the content server to forward requested content (184) to the client.

WO 2013/052693 A1

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD AND APPARATUS FOR PROTECTING A SINGLE SIGN-ON DOMAIN FROM CREDENTIAL LEAKAGE

BACKGROUND

Field

[0001] The present invention relates generally to protecting a single sign-on domain from credential leakage.

Background

[0002] Single sign-on techniques allows an authorized user to access protected subdomain websites under a shared domain based on one sign-on transaction with one of the protected subdomain websites. In a typical single sign-on technique, a user accessing a protected subdomain website is authenticated and connected to a website that provides a session cookie to the user's browser. The session cookie allows the user to have access, in addition to the subdomain website, to all websites under the domain.

[0003] However, every host of a subdomain website, and every script running on every host must be trusted in order for the user authentication to remain secure. A rogue website operating at another subdomain under the protected domain, and visited by a user, can collect the user's session cookie from the user's browser. The leaked user's credential in the session cookie can be reused to obtain illicit access to other protected internal websites of subdomains under the domain.

[0004] There is therefore a need for a technique for protecting a single sign-on domain from credential leakage.

SUMMARY

[0005] An aspect of the invention may reside in a method for protecting a single sign-on domain from credential leakage. In the method, an authentication server provides an authentication cookie to a user browser client. The authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain. The authentication server receives the authentication cookie in an access request from the browser client. The access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from

the user browser client. Upon authentication of the user authentication credential in the received authentication cookie, the authentication server responds to the access request by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain. The authentication server receives a request from the content server to validate a session identifier of the limited-use cookie. The content server received the limited-use cookie from the user browser client. Upon validation of the session identifier of the limited-use cookie, the authentication server provides a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

[0006] In more detailed aspects of the invention, the limited-use cookie may be a one-time use cookie. Upon validation of the session identifier of the limited-use cookie, the authentication server may invalidate the limited-use cookie to prohibit further use of the limited-use cookie. The limited-use cookie may have a short expiration time. The short expiration time may comprise about one minute. The content server may comprise a subdomain of the single sign-on domain. The limited-use cookie may be only valid for the content server's subdomain. The session identifier may comprise a one-time session key.

[0007] Another aspect of the invention may reside in an authentication server, comprising: means for providing an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain; means for receiving the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client; means for responding to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain; means for receiving a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and means for providing, upon validation of the session identifier of the limited-use cookie, a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

[0008] Another aspect of the invention may reside in an authentication server, comprising: a processor configured to: provide an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain; receive the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client; respond to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain; receive a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and provide, upon validation of the session identifier of the limited-use cookie, a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

[0009] Another aspect of the invention may reside in a computer program product comprising computer-readable medium, comprising: code for causing a computer to provide an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain; code for causing a computer to receive the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client; code for causing a computer to respond to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain; code for causing a computer to receive a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and code for causing a computer to provide, upon validation of the session identifier of the limited-use cookie, a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is a flow diagram of a method for protecting a single sign-on domain from credential leakage, according to the present invention.

[0011] FIG. 2 is a block diagram showing a user browser client coupled to the internet enabling communications with an authentication server and a plurality of content servers.

[0012] FIG. 3 is a block diagram showing an example of a computer for implementing an authentication server.

[0013] FIG. 4 is another flow diagram of a method for protecting a single sign-on domain from credential leakage, according to the present invention.

DETAILED DESCRIPTION

[0014] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0015] With reference to Figures 1 and 2, an aspect of the invention may reside in a method 100 for protecting a single sign-on domain from credential leakage. In the method, an authentication server 210 provides an authentication cookie 102 to a user browser client 220 (step 110). The authentication cookie has at least one user authentication credential 112 for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain. The authentication server receives the authentication cookie in an access request 114 from the browser client (step 120). The access request is based on a redirection 116 received by the user browser client from a content server 230 within the single sign-on domain in response to a content request 118 from the user browser client. Upon authentication of the user authentication credential in the received authentication cookie (step 130), the authentication server responds to the access request by forwarding, to the user browser client, a limited-use cookie 132 for the single sign-on domain (step 140). The authentication server receives a request 134 from the content server to validate a session identifier of the limited-use cookie (step 150). The content server received the limited-use cookie from the user browser client (step 160). Upon validation of the session identifier of the limited-use cookie (step 170), the authentication server provides a valid

session message 182 to the content server for enabling the content server to forward requested content 184 to the user browser client (step 190).

[0016] In more detailed aspects of the invention, the limited-use cookie 132 may be a one-time use cookie. Upon validation of the session identifier of the limited-use cookie (step 150), the authentication server may invalidate the limited-use cookie to prohibit further use of the limited-use cookie (step 180). The limited-use cookie may have a short expiration time. The short expiration time may comprise about one minute. The limited-use cookie may be specific to a particular content server 230. The content server may comprise a subdomain of the single sign-on domain. The limited-use cookie may be only valid for the content server's subdomain. The session identifier may comprise a one-time session key.

[0017] With additional reference to FIG. 3, a station comprising the authentication server 210 may be a computer 310 that includes a processor 320, memory 330 (and/or disk drives), a display 340, and keypad or keyboard 350. Similarly, another station comprising the user client 220 may be a computer that includes a processor, memory (and/or disk drives), a display, and keypad or keyboard. The user client computer may also include a microphone, speaker(s), camera, web browser software, and the like. Further, the stations may also include USB, Ethernet and similar interfaces, for communicating over a network, such as the internet 240.

[0018] With particular reference to Figure 4, the invention may be embodied in another method for protecting a single sign-on domain from credential leakage to a rogue server using the shared domain name. The method may use a domain level (e.g., domain_name.com) cookie to authenticate subdomain servers, and then may generate separate subdomain specific cookies. For single sign-on, a user browser client 220 requesting access to a website hosted by a first content server 230-1 (step 410) at a subdomain (e.g., cs1.domain_name.com) within the domain may be redirected to the authentication server 210 which uses the subdomain: login.domain_name.com (step 414). The authentication server may receive the redirection request and then procures the user's credentials for the domain (step 418, 422 and 426).

[0019] Ideally, the authentication server may generate cookies for specific lower level subdomains (e.g., cs1.domain-name.com). However a cookie cannot be set for a non-matching subdomain name. Instead, the authentication server may generate a one-time session key in a limited-use cookie (such as a one-time use cookie) for the domain:

domain_name.com. In addition, the authentication server may generate an authentication-server-specific cookie for the subdomain: login.domain_name.com, and provide the cookies to the browser client (step 430). When the user's browser client first gives the domain_name.com cookie to the website it wants to access (step 434), the website may check that session with the authentication server (step 438 and 442). The authentication invalidates that session to prevent reuse of the cookie (step 446), and then indicates to the website that the session was valid (step 450). The website then knows it is safe to give the user browser client a session cookie for its lower level subdomain (step 454).

[0020] If the user browser client 220 wishes to authenticate against a website in another subdomain hosted by a second content server 230-2 (step 458), it may be redirected to the authentication server 210 (step 462). The user browser client may provide the earlier obtained (step 430) login.domain_name.com cookie to the authentication server which may return a new one-time use cookie for the domain: domain_name.com (steps 466 and 470). As with the first content server (steps 434 – 454), the new one-time use cookie may be used by the second content server to authenticate the user browser client by inquiry to the authentication server and provides the requested content (step 474 – 494). Now that the user browser client has the subdomain cookie from the second content server, it does not need to re-authenticate within that subdomain (cs2.domain-name.com) during the session.

[0021] The limited-use aspect of the domain_name.com cookie prevents another website from replaying the domain_name.com cookie to gain access to a protected website. If the invalidated domain_name.com cookie is reused, the second authentication attempt would fail and that user would be prompted for their credentials.

[0022] Additionally, to prevent wasting time sending an invalidated cookie, the domain_name.com cookies are generated with short expiration times. Although the method of the invention increases the number of messages passed, it does not require any additional action on behalf of the user.

[0023] Since the only cookies that are valid for more than one connection are the subdomain specific cookies, the method may be more secure as these cookies are not sent to websites of other subdomains within the single sign-on domain. Thus, credential leakage to, for example, a rogue website may be prevented since the cookie for the

login.domain_name.com subdomain is not provided to any websites or servers other than the authentication server.

[0024] Another aspect of the invention may reside in an authentication server 210, comprising: means 310 for providing an authentication cookie 102 to a user browser client 220, wherein the authentication cookie has at least one user authentication credential 112 for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain; means 310 for receiving the authentication cookie in an access request 114 from the browser client, wherein the access request is based on a redirection 116 received by the user browser client from a content server 230 within the single sign-on domain in response to a content request 118 from the user browser client; means 310 for responding to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie 132 for the single sign-on domain; means 310 for receiving a request 134 from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and means 310 for providing, upon validation of the session identifier of the limited-use cookie, a valid session message 182 to the content server for enabling the content server to forward requested content 184 to the user browser client.

[0025] Another aspect of the invention may reside in an authentication server, comprising: a processor 320 configured to: provide an authentication cookie 102 to a user browser client 220, wherein the authentication cookie has at least one user authentication credential 112 for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain; receive the authentication cookie in an access request 114 from the browser client, wherein the access request is based on a redirection 116 received by the user browser client from a content server 230 within the single sign-on domain in response to a content request 118 from the user browser client; respond to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie 132 for the single sign-on domain; receive a request 134 from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and provide, upon validation of the session identifier of the limited-use

cookie, a valid session message 182 to the content server for enabling the content server to forward requested content 184 to the user browser client.

[0026] Another aspect of the invention may reside in a computer program product comprising computer-readable medium 330, comprising: code for causing a computer 310 to provide an authentication cookie 102 to a user browser client, wherein the authentication cookie has at least one user authentication credential 112 for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain; code for causing a computer 310 to receive the authentication cookie in an access request 114 from the browser client, wherein the access request is based on a redirection 116 received by the user browser client from a content server 230 within the single sign-on domain in response to a content request 118 from the user browser client; code for causing a computer 310 to respond to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie 132 for the single sign-on domain; code for causing a computer 310 to receive a request 134 from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and code for causing a computer 310 to provide, upon validation of the session identifier of the limited-use cookie, a valid session message 182 to the content server for enabling the content server to forward requested content 184 to the user browser client.

[0027] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0028] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular

application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0029] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0030] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[0031] In one or more exemplary embodiments, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software as a computer program product, the functions may be stored on as one or more instructions or code on a computer-readable medium. Computer-readable media includes computer storage media that facilitates transfer of a computer program from one place to another. A storage media may be any available media that

can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store desired program code in the form of instructions or data structures and that can be accessed by a computer. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media. The computer-readable medium may be non-transitory such that it does not include a transitory, propagating signal.

[0032] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS:

CLAIMS

1. A method for protecting a single sign-on domain from credential leakage, comprising:

an authentication server providing an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain;

the authentication server receiving the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client;

upon authentication of the user authentication credential in the received authentication cookie, the authentication server responding to the access request by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain;

the authentication server receiving a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use use cookie from the user browser client; and

upon validation of the session identifier of the limited-use cookie, the authentication server providing a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

2. A method as defined in claim 1, wherein the limited-use cookie comprises a one-time use cookie.

3. A method as defined in claim 1, further comprising:

upon validation of the session identifier of the limited-use cookie, the authentication server invalidating the limited-use cookie to prohibit further use of the limited-use cookie.

4. A method as defined in claim 1, wherein the limited-use cookie has a short expiration time.

5. A method as defined in claim 4, wherein the short expiration time comprises about one minute.

6. A method as defined in claim 1, wherein the content server comprises a subdomain of the single sign-on domain.

7. A method as defined in claim 6, wherein the limited-use cookie is only valid for the content server's subdomain.

8. A method as defined in claim 1, wherein the session identifier comprises a one-time session key.

9. An authentication server, comprising:

means for providing an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain;

means for receiving the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client;

means for responding to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain;

means for receiving a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and

means for providing, upon validation of the session identifier of the limited-use cookie, a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

10. An authentication server as defined in claim 9, wherein the limited-use cookie comprises a one-time use cookie.

11. An authentication server as defined in claim 9, further comprising:

means for invalidating, upon validation of the session identifier of the limited-use cookie, the limited-use cookie to prohibit further use of the limited-use cookie.

12. An authentication server as defined in claim 9, wherein the limited-use cookie has a short expiration time.

13. An authentication server as defined in claim 12, wherein the short expiration time comprises about one minute.

14. An authentication server as defined in claim 9, wherein the content server comprises a subdomain of the single sign-on domain.

15. An authentication server as defined in claim 14, wherein the limited-use cookie is only valid for the content server's subdomain.

16. An authentication server as defined in claim 9, wherein the session identifier comprises a one-time session key.

17. An authentication server, comprising:

a processor configured to:

provide an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain;

receive the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client;

respond to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain;

receive a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and

provide, upon validation of the session identifier of the limited-use cookie, a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

18. An authentication server as defined in claim 17, wherein the limited-use cookie comprises a one-time use cookie.

19. An authentication server as defined in claim 17, wherein the processor is further configured to:

invalidate, upon validation of the session identifier of the limited-use cookie, the limited-use cookie to prohibit further use of the limited-use cookie.

20. An authentication server as defined in claim 17, wherein the limited-use cookie has a short expiration time.

21. An authentication server as defined in claim 20, wherein the short expiration time comprises about one minute.

22. An authentication server as defined in claim 17, wherein the content server comprises a subdomain of the single sign-on domain.

23. An authentication server as defined in claim 22, wherein the limited-use cookie is only valid for the content server's subdomain.

24. An authentication server as defined in claim 17, wherein the session identifier comprises a one-time session key.

25. A computer program product, comprising:

computer-readable medium, comprising:

code for causing a computer to provide an authentication cookie to a user browser client, wherein the authentication cookie has at least one user authentication credential for the single sign-on domain, and is associated with an authentication subdomain of the single sign-on domain;

code for causing a computer to receive the authentication cookie in an access request from the browser client, wherein the access request is based on a redirection received by the user browser client from a content server within the single sign-on domain in response to a content request from the user browser client;

code for causing a computer to respond to the access request, upon authentication of the user authentication credential in the received authentication cookie, by forwarding, to the user browser client, a limited-use cookie for the single sign-on domain

code for causing a computer to receive a request from the content server to validate a session identifier of the limited-use cookie, wherein the content server received the limited-use cookie from the user browser client; and

code for causing a computer to provide, upon validation of the session identifier of the limited-use cookie, a valid session message to the content server for enabling the content server to forward requested content to the user browser client.

26. A computer program product as defined in claim 25, wherein the limited-use cookie comprises a one-time use cookie.

27. A computer program product as defined in claim 25, further comprising:

code for causing a computer to invalidate, upon validation of the session identifier of the limited-use cookie, the limited-use cookie to prohibit further use of the limited-use cookie.

28. A computer program product as defined in claim 25, wherein the limited-use cookie has a short expiration time.

29. A computer program product as defined in claim 28, wherein the short expiration time comprises about one minute.

30. A computer program product as defined in claim 25, wherein the content server comprises a subdomain of the single sign-on domain.

31. A computer program product as defined in claim 30, wherein the limited-use cookie is only valid for the content server's subdomain.

32. A computer program product as defined in claim 25, the session identifier comprises a one-time session key.

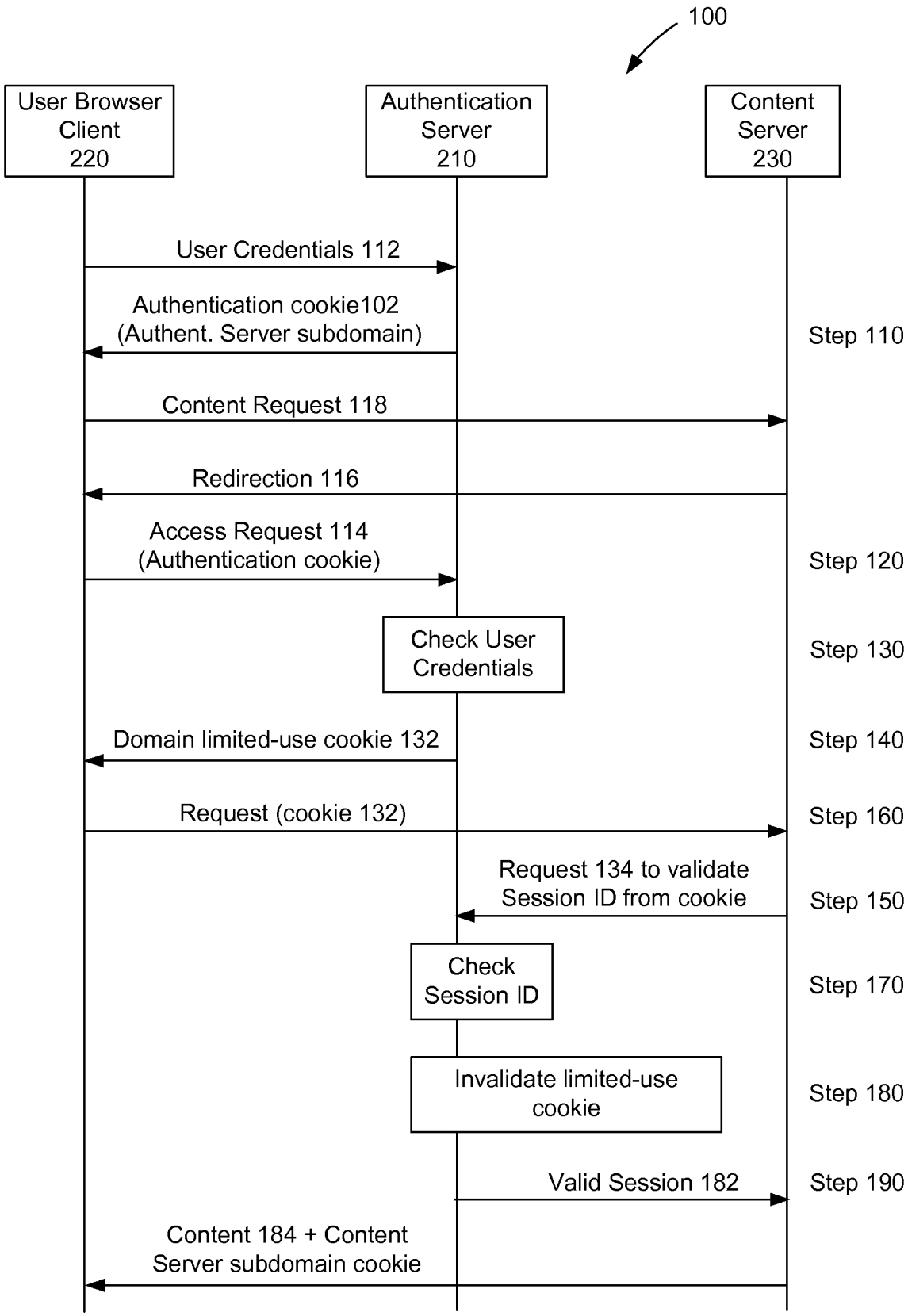

100
User Browser Client 220
Authentication Server 210
Content Server 230
User Credentials 112
Authentication cookie102 (Authent. Server subdomain)
Step 110
Content Request 118
Redirection 116
Access Request 114 (Authentication cookie)
Step 120
Check User Credentials
Step 130
Domain limited-use cookie 132
Step 140
Request (cookie 132)
Step 160
Request 134 to validate Session ID from cookie
Step 150
Check Session ID
Step 170
Invalidate limited-use cookie
Step 180
Valid Session 182
Step 190
Content 184 + Content Server subdomain cookie

FIG. 1

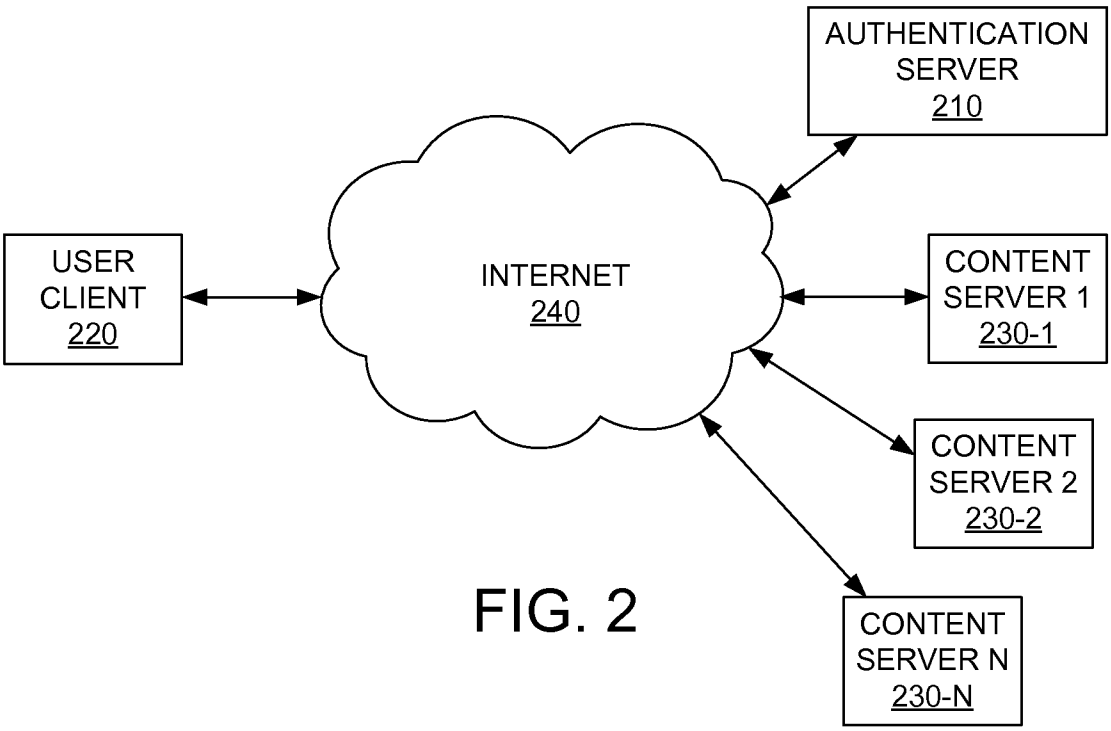

AUTHENTICATION SERVER 210
USER CLIENT 220
INTERNET 240
CONTENT SERVER 1 230-1
CONTENT SERVER 2 230-2
CONTENT SERVER N 230-N

FIG. 2

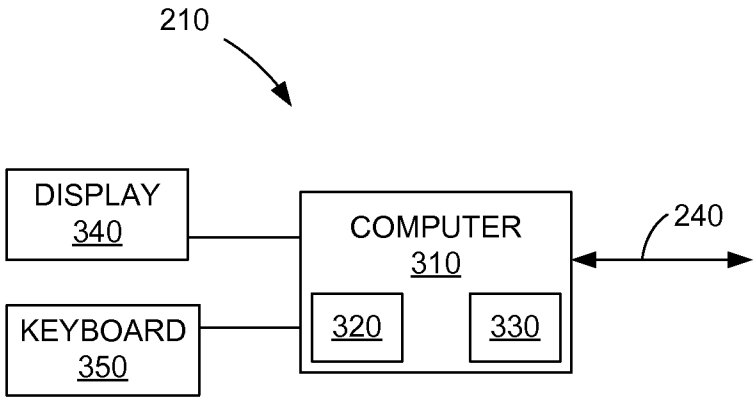

210
DISPLAY 340
KEYBOARD 350
COMPUTER 310
320
330
240

FIG. 3

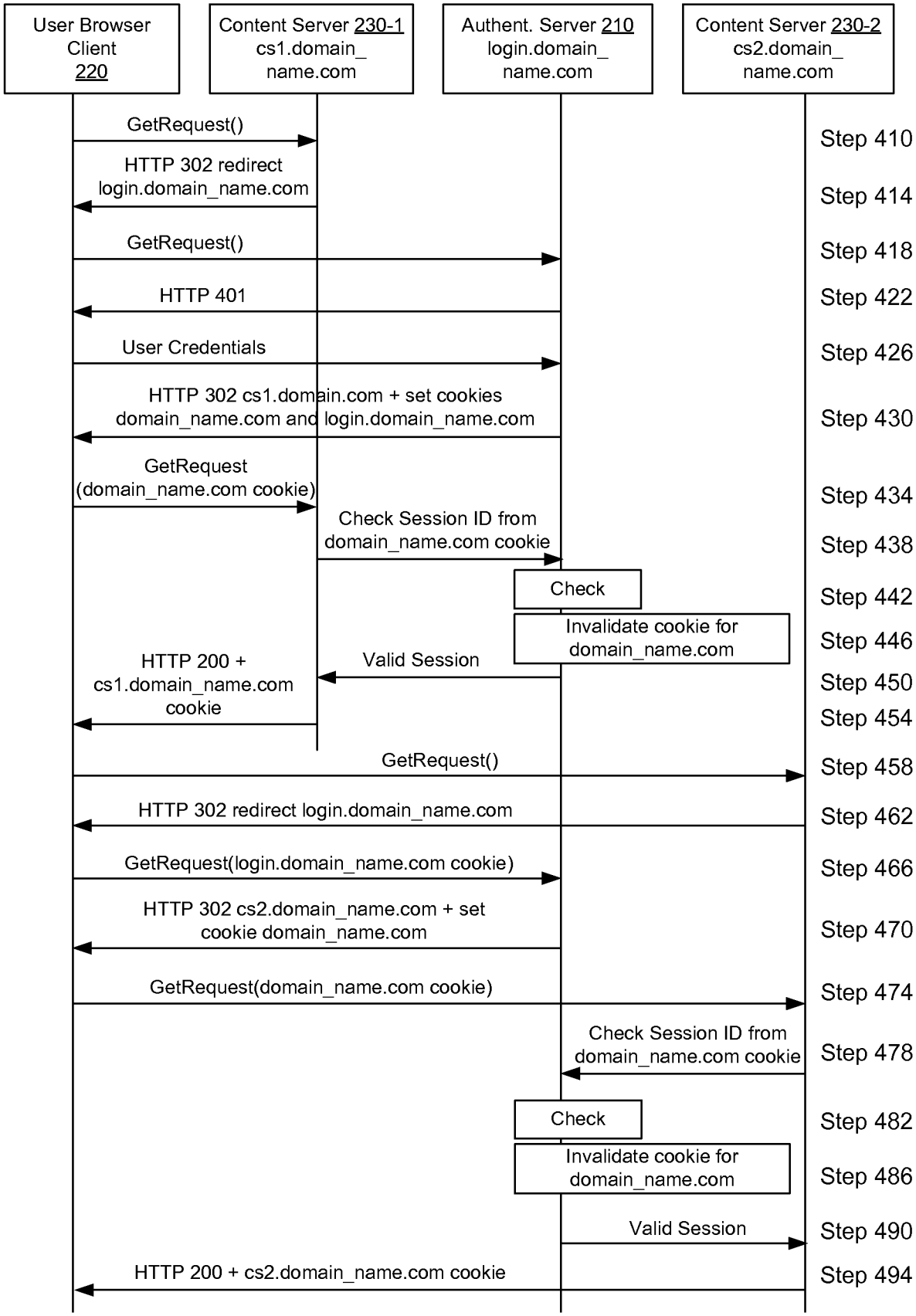

User Browser Client 220
Content Server 230-1 cs1.domain_name.com
Authent. Server 210 login.domain_name.com
Content Server 230-2 cs2.domain_name.com
GetRequest()
Step 410
HTTP 302 redirect login.domain_name.com
Step 414
GetRequest()
Step 418
HTTP 401
Step 422
User Credentials
Step 426
HTTP 302 cs1.domain.com + set cookies domain_name.com and login.domain_name.com
Step 430
GetRequest (domain_name.com cookie)
Step 434
Check Session ID from domain_name.com cookie
Step 438
Check
Step 442
Invalidate cookie for domain_name.com
Step 446
Valid Session
HTTP 200 + cs1.domain_name.com cookie
Step 450
Step 454
GetRequest()
Step 458
HTTP 302 redirect login.domain_name.com
Step 462
GetRequest(login.domain_name.com cookie)
Step 466
HTTP 302 cs2.domain_name.com + set cookie domain_name.com
Step 470
GetRequest(domain_name.com cookie)
Step 474
Check Session ID from domain_name.com cookie
Step 478
Check
Step 482
Invalidate cookie for domain_name.com
Step 486
Valid Session
Step 490
HTTP 200 + cs2.domain_name.com cookie
Step 494

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/058789

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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)
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 practicable, search terms used)
EPO-Internal, WPI Data, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Chris Dunne: "Build and implement a single sign-on solution", , 8 November 2010 (2010-11-08), XP055049042, Retrieved from the Internet: URL:http://web.archive.org/web/20101108160239/http://www.ibm.com/developerworks/web/library/wa-singlesign/#resources [retrieved on 2013-01-09] the whole document ----- -/--	1-32

[X] Further documents are listed in the continuation of Box C.

[X] See patent family 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 application or patent 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	Date of mailing of the international search report
21 January 2013	30/01/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ströbeck, Anders

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/058789

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Bill Hines ET AL: "IBM WebSphere Session Management", , 23 March 2006 (2006-03-23), XP055049080, Retrieved from the Internet: URL:http://web.archive.org/web/20060323193212/http://www.ibmpressbooks.com/articles/article.asp?p=332851&seqNum=2 [retrieved on 2013-01-09] the whole document	1-32
A	WO 2007/076074 A2 (CATALOG COM INC [US]; CRULL ROBERT WAYNE [US]; MILLER BILL CODY [US];) 5 July 2007 (2007-07-05) page 12, line 21 - page 13, line 11; figure 7	1-32

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2012/058789

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007076074 A2	05-07-2007	CA 2634201 A1	05-07-2007
		CA 2634206 A1	05-07-2007
		EP 1969477 A2	17-09-2008
		EP 1969478 A2	17-09-2008
		EP 2518637 A1	31-10-2012
		EP 2541430 A2	02-01-2013
		US 2007150603 A1	28-06-2007
		US 2007169165 A1	19-07-2007
		WO 2007076072 A2	05-07-2007
		WO 2007076074 A2	05-07-2007