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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/065004 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/KR2005/000713

(22) International Filing Date: 14 March 2005 (14.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2004-0106627
15 December 2004 (15.12.2004) KR

(71) Applicant *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161 Gajeong-Dong, Yuseong-Gu, Daejon 305-350 (KR).

(72) Inventors; and

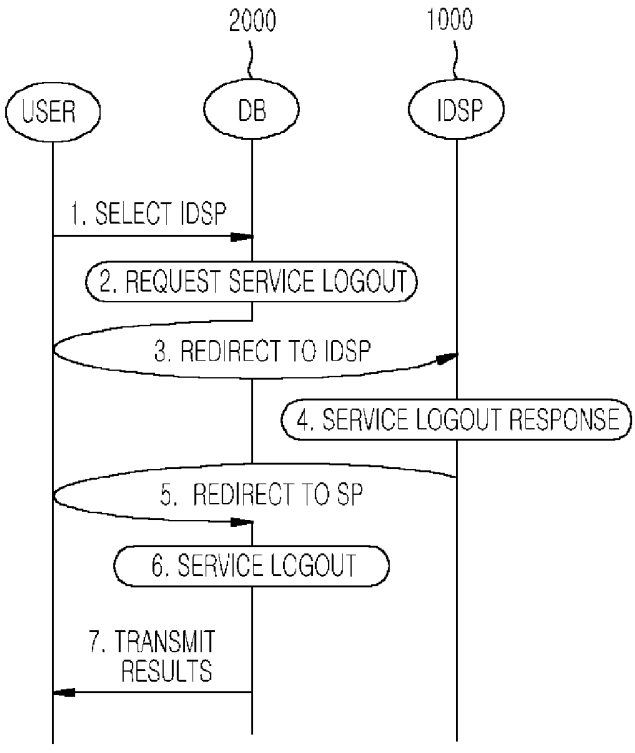
(75) Inventors/Applicants *(for US only)*: **CHO, Sang Rae** [KR/KR]; 103-1505 Jindalrae Apt., Wolpyeong-Dong, Seo-Gu, Daejon 302-754 (KR). **CHO, Yeong Sub** [KR/KR]; 107-902 Hanaro Apt., Wolpyeong-Dong, Seo-Gu, Daejon 302-748 (KR). **CHOI, Dae Seon** [KR/KR]; 101-508 Hwangsil Town Apt., Wolpyeong-Dong, Seo-Gu, Daejon 302-792 (KR). **NOH, Jong Hyouk** [KR/KR]; B-401 TwinVilla Jangdae-Dong 306-10, Yuseong-Gu, Daejon 305-308 (KR). **KIM, Taesung** [KR/KR]; 114-702 Hanmaeul Apt., Songgang-Dong, 200-4, Yuseong-Gu, Daejon 305-756 (KR). **KIM, Seung Hyun** [KR/KR]; 105-804 Garammaeul Apt., Dowon-Dong, 1439 Dalseo-Gu, Daegu 704-791 (KR). **JIN, Seung Hun** [KR/KR]; 104-1405 Baekhap Apt., Wolpyeong-Dong, Seo-Gu, Daejon 302-752 (KR).

(74) Agent: **LEE, Hwa Ik**; Young International Patent & Law Firm, 4th Fl. Yosam Bldg. 648-23, Yoksam-Dong, Kangnam-Gu, Seoul 135-748 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PERFORMING SERVICE LOGOUT IN SINGLE-SIGN-ON SERVICE USING IDENTITY



(57) Abstract: A system and a method for performing a service logout in a single-sign-on service are provided. The system includes a service-logout-request processor, a system policy manager, and a session manager. The service-logout-request processor receives a service-logout request from an SP (service provider) to refer to policies regarding a service logout through a system policy manager and refers to whether a session is valid through a session manager. The system policy manager refers to whether a user has rights for performing a service logout and refers to other policies necessary for the service logout. The session manager manages an authentication session and a service session of the user and refers to whether a session exists and is valid in order to logout from the service session.

WO 2006/065004 A1

MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *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.

Description

SYSTEM AND METHOD FOR PERFORMING SERVICE LOGOUT IN SINGLE-SIGN-ON SERVICE USING IDENTITY

Technical Field

[1] The present invention relates to a system and a method for performing a service logout in a single-sign-on service using federated identity.

Background Art

[2] Thanks to development and expansion of the Internet, an electronic commerce has been rapidly expanded and actively in use. Lots of users become a member of a plurality of on-line service providers (SP) and receive services thereof. The SP requests an user to register an identifier(ID) and a password when the user joins the SP. The SP provides the services after performing a user authentication using the ID and the password registered by the users. However, due to overflowing of numerous SPs, the users have so many IDs and passwords that the users cannot actually memorize all the IDs and the passwords. Thus, lots of systems currently provide a single-sign-on function that allows the users to use web-services without additional authentication if the users pass through an authentication procedure for one time.

[3] For example, a Korean patent application No.10-2000-0044999 titled "Method for performing automatic joining and automatic login of an Internet site and system using the same" discloses an authentication technology such that when the member of the site accesses another external site linked by the site, the member is allowed to achieve the same rights as the member of the external site without a separate login- procedure. Particularly, the above Korean application discloses an SSO (Single-Sign-On) method, in which when the users intend to become a member of a predetermined site (sub-site) the system delivers member information of a site (main-site) already joined by the users to the sub-site, thereby allowing the users to achieve the same rights as the member of the main site also in the sub-site without a separate login-procedure.

[4] However, the above-described Korean application does not provide a service for logging-out when users intend to quit using a service for respective websites in case the users have logged-in multiple websites using SSO.

[5] To solve the above-described problems, Liberty Alliance group provides a single-logout service in which respective SPs manage user IDs and passwords and work in cooperation with one another to provide an Internet SSO service to users and the users are allowed to logout from all the logged-in SPs at a time if the users desire to logout. However, even Liberty Alliance does not provide a service for allowing the users to logout a single website when the users may want to leave the visited website and no

longer wish to come back that site.

Disclosure of Invention

Technical Problem

[6] Accordingly, the present invention is directed to a system and a method for performing a service logout in a single-sign-on service that substantially obviate one or more of the problems due to limitations and disadvantages of the related art.

[7] An object of the present invention is to provide a system and a method for performing a service logout in a single-sign-on service using a federated identity capable of processing service-logout requests in cooperation with system policies and sessions so as to support logouts from respective sites which cannot be provided by a related art SSO.

Technical Solution

[8] To achieve these and other advantages and in accordance with the purpose of the present invention, as embodied and broadly described, there is a system provided performing a service logout in a single-sign-on service using a federated identity, which includes: a service-logout-request processor for receiving a service-logout request from an SP to refer to policies regarding a service logout through a system policy manager and referring to whether a session is valid through a session manager; a system policy manager for referring to whether a user has rights for performing a service logout and referring to other policies necessary for the service logout; and a session manager for managing an authentication session and a service session of the user and referring to whether a session exists and is valid in order to logout from the service session.

[9] According to another aspect of the present invention, there is a method provided for performing a service logout in a single-sign-on service using a federated identity, which includes the steps of: referring to service-logout polices through a policy database (DB) when a service-logout request is received; judging whether the service-logout request is valid on the basis of the above-referred policy; if the service-logout request is valid as a result of the judgment, referring to session information using a session ID and checking whether a session is valid; and if the session is valid currently as a result of the checking, deleting the session.

Brief Description of the Drawings

[10] FIG. 1 is a view schematically illustrating a structure of a system for performing a service logout in a single-sign-on service using a federated identity according to the present invention;

[11] FIG. 2 is a view schematically illustrating a structure and an operation principle of a system policy manager according to the present invention;

[12] FIG. 3 is a view schematically illustrating a structure and an operation principle of a session manager according to the present invention;

[13] FIG. 4 is a flowchart illustrating a schematic processing procedure of a method for performing a service logout in a single-sign-on service using a federated identity according to the present invention; and

[14] FIG. 5 is a flowchart illustrating a method for performing a service logout in a single-sign-on service using a federated identity according to the present invention.

Best Mode for Carrying Out the Invention

[15] Hereinafter, preferred embodiments of the present invention will be described in detail with reference to accompanying drawings.

[16] FIG. 1 is a view schematically illustrating a structure of a system for performing a service logout in a single-sign-on service using a federated identity according to the present invention.

[17] The SP 2000 is intended for providing services to users through on-line. The SP 2000 has a service-logout request and response processor for requesting an ID service provider (IDSP) 1000 to perform a service logout and receiving a response thereto from the IDSP 1000 to output a response message to a user's web-browser.

[18] The IDSP 1000 is intended for allowing users to login a plurality of sites through an Internet SSO service under a federated identity environment and to logout from the respective sites. The IDSP 1000 includes a service-logout-request processor 100 for receiving a service-logout request of a user transmitted from the SP 2000 and referring to policies regarding service logout by communicating with a system policy manage; the system policy manager 200 for referring to whether a user has rights for performing a service logout and referring to other policies necessary for the service logout; and a session manager 300 for managing an authentication session and a service session of the user and referring to whether a session exists and is valid in order to logout from the service session. The service-logout-request processor 100 determines whether to logout from the service session and perform the logout on the basis of the information referred through the system policy manager 200 and the session manager 300 and transmits results to the SP.

[19] FIG. 2 is a view schematically illustrating a structure and an operation principle of a system policy manager 200 for managing policies regarding an SSO according to the present invention. The system policy manager 200 has a policy request receiver 201 for receiving requests regarding a variety of policies and a policy dispatcher 202 for classifying the requests according to the their kind to send the classified requests to the relevant module. The policies are roughly classified into registration, inquiry, change, and deletion operations. The system policy manager 200 refers to the policies through

a policy database (DB) when performing each operation.

[20] FIG. 3 is a view schematically illustrating a structure and an operation principle of a session manager 300 for managing SSO sessions according to the present invention. The session manager 300 has a session handler 301 for receiving and analyzing all operations regarding the session and sending a request to the relevant operation. Since the session handler manages session information on a memory and records the session information on a session DB so that log information may be left afterwards, the session handler accesses the DB to leave the record when generating and deleting the session. On the contrary, when referring to and updating the session, the session handler performs the operations directly on the memory.

[21] FIG. 4 is a flowchart illustrating a schematic processing procedure of a method for performing a service logout in a single-sign-on service using a federated identity according to the present invention. If users designate an IDSP at an SP 2000 to make a service-logout request, the SP 2000 generates a service-logout request message and transmit the same to the IDSP 1000 through a user's web-browser. At this time, a redirection which is one of communication methods generally used on the web is used.

[22] The SP 2000 transmits a login ID of the user and a session ID given when logging in the SP 2000 together with the request message.

[23] The IDSP 1000 that has received the request message executes a service logout upon request of the user, makes a response message using results thereof, and transmits the response message to the SP 2000 using a redirection. The SP 2000 that has received the response message informs the user of the results regarding the requested service.

[24] FIG. 5 is a flowchart illustrating a method for performing a service logout in a single-sign-on service using a federated identity according to the present invention. If the service-logout-request processor 100 of the IDSP 1000 receives a service-logout request, the service-logout policies are referred to by the system policy manager 200 first (S11), and whether the user has rights to request a service logout is judged on the basis of the referred policy (S12). Next, the session information is referred to using the session ID through the session manager 300 (S13). Whether the session information exists and is currently valid are checked (S14) and the session manager is requested to delete the relevant service session (S15). After the service session is deleted, a response message is generated and transmitted to the SP 2000, whereby a service-logout procedure is completed.

Industrial Applicability

[25] The present invention increases security in the SSO service as well as enhances reliability of the service and increases efficiency of the system management by providing

the service-logout service in that the users of the SSO service using the federated identity may be allowed to separately logout from the respective sites.

[26] While the present invention has been described and illustrated herein with reference to the preferred embodiments thereof, it will be apparent to those skilled in the art that various modifications and variations can be made therein without departing from the spirit and scope of the invention. Thus, it is intended that the present invention covers the modifications and variations of this invention that come within the scope of the appended claims and their equivalents.

Claims

[1] A system for performing a service logout in a single-sign-on service using a federated identity, the system comprising:
a service-logout-request processor for receiving a service-logout request from an SP (service provider) to refer to policies regarding a service logout through a system policy manager and referring to whether a session is valid through a session manager;
the system policy manager for referring to whether a user has rights for performing a service logout and referring to other policies necessary for the service logout; and
the session manager for managing an authentication session and a service session of the user and referring to whether a session exists and is valid in order to logout from the service session.

[2] The system of claim 1, further comprising a service provider for requesting the service-logout-request processor to allow a service logout, receiving processing results from the service-logout-request processor, and transmitting the results to a web-browser.

[3] The system of claim 1, further comprising: a policy request receiver for receiving requests regarding a variety of policies from the system policy manager; and a policy dispatcher for classifying the requests according to their kind and transmitting the classified requests to a relevant module.

[4] The system of claim 1, wherein the session manager has a session handler for receiving and analyzing all operations regarding the session and transmitting a request to a relevant operation.

[5] The system of claim 4, wherein the session handler accesses a session DB (database) when generating and deleting the session and performs operations directly on a memory when referring to and updating the session without an access to the session DB.

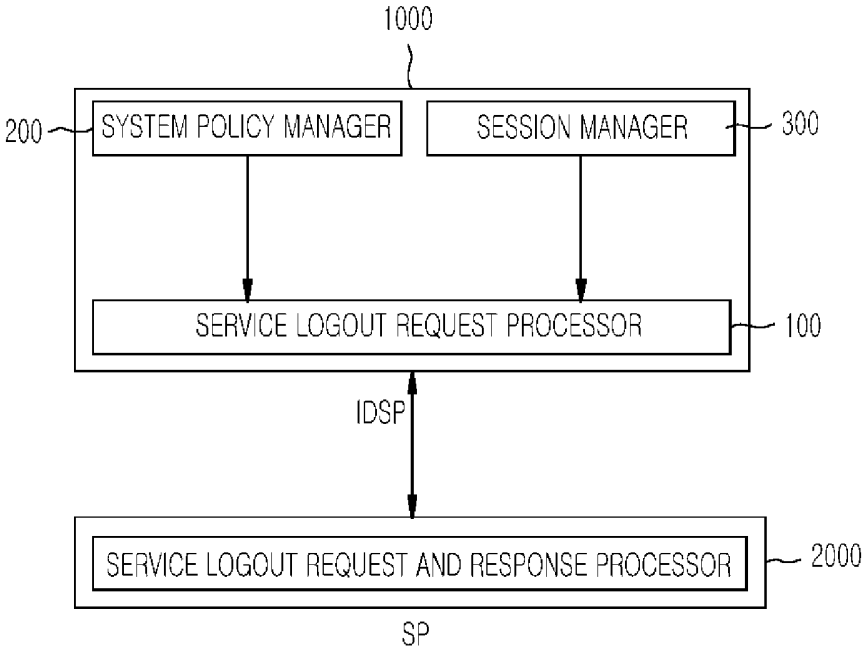
[6] A method for performing a service logout in a single-sign-on service using a federated identity, the method comprising the steps of:
generating a service-logout-request message including a login ID (identification) and a session ID of a user by a service-logout request;
redirecting the generated service-logout-request message to an IDSP (ID service provider) through a web-browser;
executing a service logout from a single service requested through a service-logout-request message; and
redirecting a response message representing results of the executed service

logout to an SP (service provider).

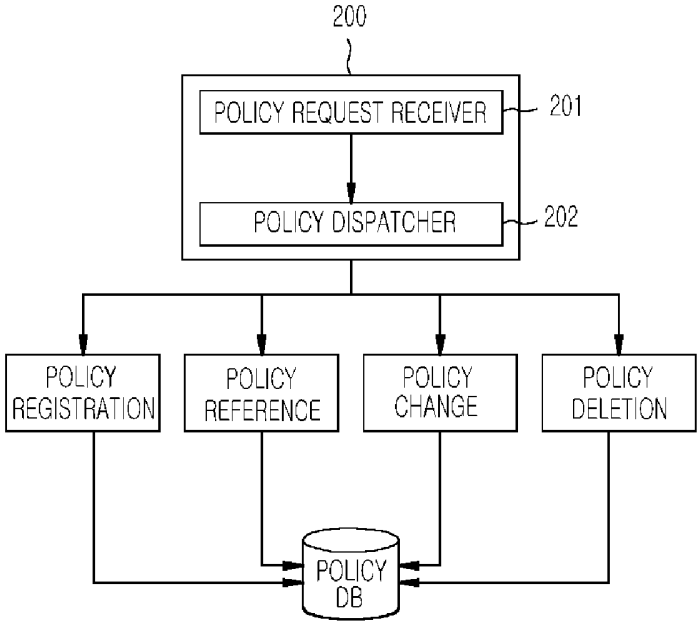
[7] A method for performing a service logout in a single-sign-on service using a federated identity, the method comprising the steps of:
referring to service-logout polices through a policy DB (database) when a service-logout request is received;
judging whether the service-logout request is valid on the basis of the above-referred policy;
if the service-logout request is valid as a result of the judgment, referring to session information using a session ID (identification) and checking whether a session is valid; and
if the session is valid currently as a result of the checking, deleting the session.

[8] The method of claim 7, further comprising the step of: preparing a response message informing that the session has been deleted and redirecting the response message.

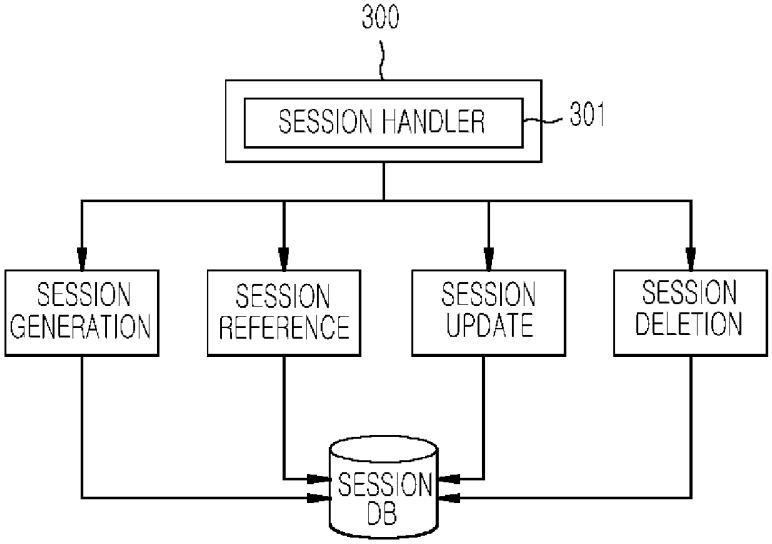
[Fig. 1]


1000
200
SYSTEM POLICY MANAGER
SESSION MANAGER
300
SERVICE LOGOUT REQUEST PROCESSOR
100
IDSP
SERVICE LOGOUT REQUEST AND RESPONSE PROCESSOR
2000
SP

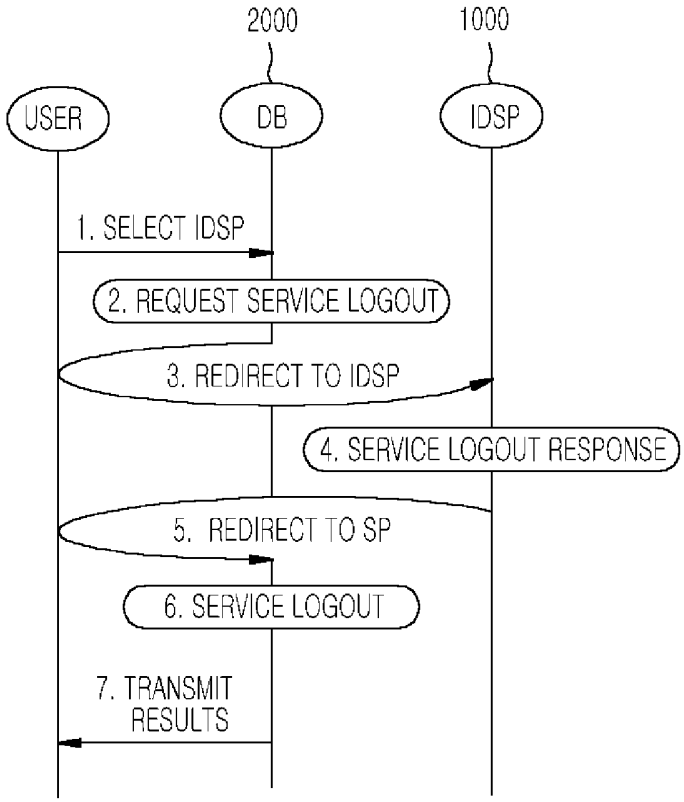
[Fig. 2]


200
POLICY REQUEST RECEIVER
201
POLICY DISPATCHER
202
POLICY REGISTRATION
POLICY REFERENCE
POLICY CHANGE
POLICY DELETION
POLICY DB

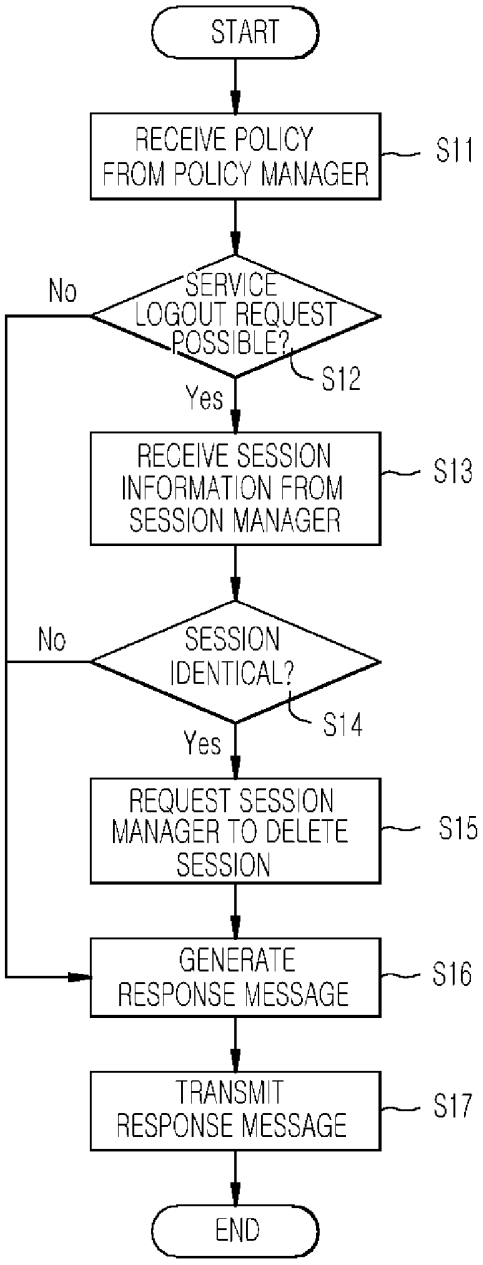
[Fig. 3]


300
SESSION HANDLER
301
SESSION GENERATION
SESSION REFERENCE
SESSION UPDATE
SESSION DELETION
SESSION DB

[Fig. 4]


2000
1000
USER
DB
IDSP
1. SELECT IDSP
2. REQUEST SERVICE LOGOUT
3. REDIRECT TO IDSP
4. SERVICE LOGOUT RESPONSE
5. REDIRECT TO SP
6. SERVICE LOGOUT
7. TRANSMIT RESULTS

[Fig. 5]


START
RECEIVE POLICY FROM POLICY MANAGER
S11
SERVICE LOGOUT REQUEST POSSIBLE?
S12
No
Yes
RECEIVE SESSION INFORMATION FROM SESSION MANAGER
S13
SESSION IDENTICAL?
S14
No
Yes
REQUEST SESSION MANAGER TO DELETE SESSION
S15
GENERATE RESPONSE MESSAGE
S16
TRANSMIT RESPONSE MESSAGE
S17
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/000713

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 9/32

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)

IPC7 H04L

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

KR : AS ABOVE

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Jun Miyoshi "Network-based Single Sign-On Architecture for IP-VPN" In : IEEE Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on Volume 1, 28-30 Aug. 2003 Page(s):458 - 461 vol.1 (see abstract, figure 2, pages 459-460)	1 ~ 8
A	WO 2004/075035 A1(Telefonaktiebolaget LM Ericsson) 2 Sep 2004 (see abstract)	1 ~ 8
A	WO 03/073242 A1(Telefonaktiebolaget LM Ericsson) 4 Sep 2003 (see abstract)	1 ~ 8

☐ Further documents are listed in the continuation of Box C.

☒ 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 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
08 SEPTEMBER 2005 (08.09.2005)	**09 SEPTEMBER 2005 (09.09.2005)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

LEE, Dong Hwan

Telephone No. 82-42-481-5755

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2005/000713

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO2004075035A1	02.09.2004	AU2003212261A1	09.09.2004
		WO2004075035A1	02.09.2004
WO03073242A1	04.09.2003	AU2003212742A1	09.09.2003
		EP1497705A1	19.01.2005
		WO03073242A1	04.09.2003