



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

(21) International Application Number:
PCT/EP2011/000649

(22) International Filing Date:
11 February 2011 (11.02.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **NEC EUROPE LTD.** [DE/DE]; Kurfuersten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GIRAO, Joao** [PT/DE]; Seilerstrasse 23, 67063 Ludwigshafen (DE). **ENDO, Yukiko** [JP/DE]; Koenigsbruecker Strasse 76A, 01099 Dresden (DE).

(74) Agents: **ULLRICH & NAUMANN** et al.; Schneidmuehlstrasse 21, 69115 Heidelberg (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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).

Published:

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

(54) Title: METHOD AND SYSTEM FOR SUPPORTING USER AUTHENTICATION TO A SERVICE

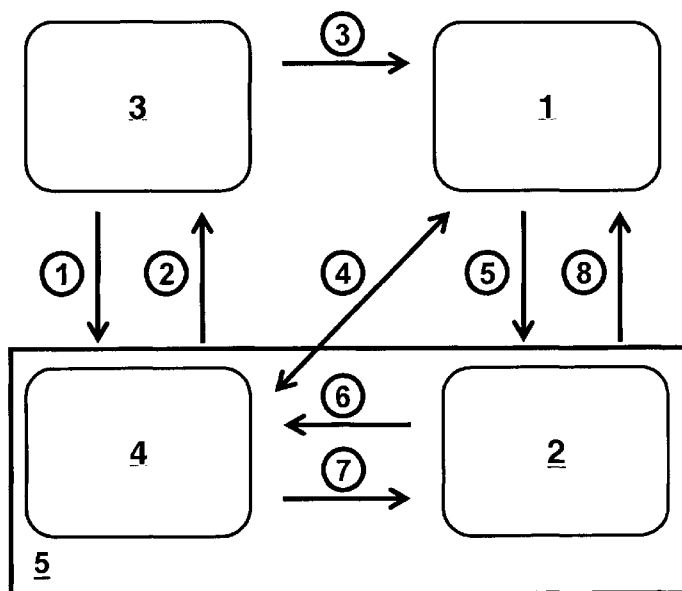


Fig. 1

(57) Abstract: A method for supporting user authentication to a service, wherein the user accesses said service from a terminal device, in particular a public and/or untrusted terminal device, is characterized in that an authentication session is established between a trusted device of the user - delegator device (3) - and a delegation service (4), wherein said delegation service (4) provides a token to said delegator device (3), wherein, upon said token being provided to said terminal device - delegate device (1) -, said authentication session is delegated from said delegator device (3) to said delegate device (1). Furthermore, a corresponding system for supporting user authentication to a service is disclosed.

METHOD AND SYSTEM FOR SUPPORTING USER AUTHENTICATION TO A SERVICE

The present invention relates to a method for supporting user authentication to a service, wherein the user accesses said service from a terminal device, in particular a public and/or untrusted terminal device.

Furthermore, the present invention relates to a system for supporting user authentication to a service, including a terminal device, in particular a public and/or untrusted terminal device, from which the user accesses said service.

Generally, when a user accesses a service, in most cases, the first step is to authenticate either to the service or, if available, to the IDP which then provides credentials to the SP. However, in some situations such as for example accessing from internet café or airport lounge, the user would rather not disclose his/her credentials in the device he/she is currently on. In these cases, authentication can be delegated to a device of the user specific for authentication (e.g. a one time password). While this situation is common, it depends on external specific hardware, e.g. an RFID token, and does not allow for full control on the authentication mechanism after the user stops using the service. In particular, once the session is open, an attacker may make use of the established connection.

Especially when the user is accessing a public device, he/she not only wants to delegate the authentication from a different device but also be in control of when that association is no longer valid. In addition, the user wants to protect his/her credentials as much as possible, since when we use another device and introduce our passwords, we leave a trace that can later be used to steal our accounts.

Existing mechanisms for delegation, such as E.N. Ceesay et al. "An authentication model for delegation, attribution and least privilege" in PETRA'10, June 23-25, 2010, Samos, Greece focus on the delegation of authentication across services or people (user subscriptions) but do not address the problem of delegation across devices nor the control over the delegation.

- 2 -

It is therefore an object of the present invention to improve and further develop a method and a system of the initially described type for supporting user authentication to a service in such a way that by protecting a user's credentials a session even from an untrusted terminal device is secured as much as possible.

In accordance with the invention, the aforementioned object is accomplished by a method comprising the features of claim 1. According to this claim, such a method is characterized in an authentication session is established between a trusted device of the user – delegator device – and a delegation service, wherein said delegation service provides a token to said delegator device, wherein, upon said token being provided to said terminal device – delegate device –, said authentication session is delegated from said delegator device to said delegate device.

Furthermore, the aforementioned object is accomplished by a system comprising the features of claim 20. According to this claim, such a system is characterized in that the system further includes

a trusted device of the user – delegator device – and a delegation service, with an authentication session being established between those two entities, wherein said delegation service is configured to provide a token to said delegator device, and

means that are configured to perform, upon said token being provided to said terminal device – delegate device –, delegation of said authentication session from said delegator device to said delegate device.

According to the present invention it has first been recognized that the above mentioned objective can be solved by multi-device authentication or, more specifically by the delegation of the authentication session to another device. In this context it has been further recognized that solutions such as SAML (<http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf>) and OpenID (http://openid.net/specs/openid-authentication-2_0.html) provide the tools for authentication and provisioning of identity from 3rd parties but do not address the problem of multi-device authentication or the delegation of this authentication session to another device.

According to the present invention a solution is proposed which extends an authentication session between a user in one device to an authentication of the same user in a different device. The user will be offered a token from a delegation service on his/her personal device. The delegation service will use this token to associate the existing authentication session to the public device. This operation can be regarded as authentication session delegation. The delegation service will treat the new authentication session as if it were part of the existing session, under the rules defined by the delegation (e.g. for a specific service, time or device).

It is important to note that although there are already one time password token/mobile solutions, they are not very convenient for users. In case of one time password token, user always needed to carry the token. Although even this was solved by introducing one time password functionality on mobile devices, existing solutions still always require users to input the one time password even to the trusted devices. Typically one time password is used for high secure access and not convenient for daily use. In contrast, the solution according to the present invention does not change the usual authentication scheme for daily use. Advantageously, the authentication session delegation scheme can be easily added on top of existing IdM solutions.

The present invention allows for users to use public devices without compromising security and under full control from the user-side on the extent of the delegation. There is no need for transferring sensitive security material to the (potentially untrusted) delegate device. The solution is particularly tailored for, but not limited to, web applications and does not depend on any specific hardware or modifications/adaptation on the client side, on the server side (if already using protocols like SAML (Security Assertion Markup Language), OpenID, CardSpace, etc), nor on the delegate device side.

According to another aspect, the present invention can be used for secure session hand-over amongst devices. Using multiple devices in parallel, e.g. two computers and/or mobile devices, is getting more and more common and important business issues are also handled for example from smart phone. Typical session hand-over

does not require strong authentication, but users need to have a more secure way to hand-over the session. By considering this situation, session hand-over amongst multiple devices is highly demanded. In accordance with the present invention secure session hand-over amongst multiple user devices is supported by delegating authentication session to another device.

In order to further increase security, it may be provided that the token includes a One Time Password (OTP), i.e. a password being valid only for a single login. The OTP ensures that, once the user has left the public and/or untrusted terminal device, it is impossible for another user to reactivate the previous session by using the same password as the user before. By using a one time password the achieved security level is equivalent to the OTP on the delegate side.

According to a specific embodiment, once the user is offered the token from the delegation service on his/her (personal) delegator device, this token is introduced manually in the public computer, i.e. the delegate device. Alternatively, in a more sophisticated manner the token may be introduced into said delegate device as a QR code (Quick Response) or as a two-dimensional barcode. More specifically, the delegator device may display a QR code or a 2D barcode containing the token, which is then scanned at the delegator device. According to another alternative NFC (Near Field Communication) may be used between the devices in order to transfer the token from the user's delegate device to the delegator device, wherein the delegate device behaves as an NFC reader to exchange the token with the delegator device. It is also possible to provide the token to the delegate device by sending an SMS to a previously configured device (e.g. mTAN – mobile Transaction Authentication Number).

In an alternative embodiment the methods described above can be reversed in such a way that the delegate device is being configured to provide a secure URL where the token can be transferred. For instance, the delegate device can first be associated with a token, through the delegation service, which can then be provided and authorized by the delegator device, e.g. a QR code that contains post URL, and that the delegator device, e.g. a mobile device, takes a picture of the QR code and submits it to post URL.

However, in any case, i.e. independent of which of the above described techniques is applied for providing the token to the delegate device, since all methods require physical presence or access to a device that belongs only to the user, they cannot be easily intercepted, sniffed or spoofed.

Once the delegate device has received the token, it may be provided that it uses the token for accessing the delegation service. The delegate device may access the delegation service either directly or as a result of an access to a service. In any case, for the delegation service the access of the delegate device using the token may function as trigger for mapping the token to the existing authentication session between the delegation service and the user's delegator device. Such mapping of authentication sessions at the delegation service allows the delegation of the same credentials towards the services and the user to maintain the control over the delegated authentication session.

According to a further preferred embodiment it may be provided that in a next step the delegation service transmits a response message to the delegate device including the corresponding session cookie. With the delegation service installing the session cookie in the response message, i.e. with the insertion of the correct session authentication cookie as part of an answer to a correct token which maps the session, the delegate device is enabled to more efficiently control the session.

In a next step, when the delegate device accesses the service, it may be provided that the service verifies the authentication with the delegation service. In response, the delegation service may provide the service the authentication context in accordance with the authentication session that exists between the delegation service and the delegator device. After this step, the user may be provided the service through the delegate device.

Advantageously, the parameterization of the delegated authentication session is specified while the delegation is active. Alternatively, it may be provided that the parameterization of this session delegation is specified before the delegation is made and is adjusted while the delegation is active. In particular, the

parameterization may include rules that contain information regarding specific services, times and/or devices. As a consequence, the delegation service will treat the new authentication session, i.e. the delegated authentication session, as if it were part of the existing session, under the rules defined by the delegation.

The parameterization together with the strong authorization aspect further validates the proposed technology in real scenarios. In particular, it allows for control on critical operations from a (more) trusted device both when the public device is available, or not. For instance, the process can be further extended to create a gated system for critical operations. In this mode, certain operations require explicit user consent on the trusted device for the operation to proceed. For example, a user may access the facebook page, read and browse content but resulting from the chosen parameterization he/she cannot post or change data. Once a post action is taken, the service will contact the delegation service for authorization and, if this is not a trusted device, the delegation service will obtain the necessary green light from the trusted device. Through this mechanism one can ensure that critical operations are protected even in extreme conditions where the public device is only trusted, e.g., with read operations.

According to a preferred embodiment, in order to terminate the session to the service, it may be provided that the user dissociates the delegation of the authentication session from the delegator device, thus being able to control in realtime the validity of the authentication session delegation. The advantage of this is that the user, even after he has left the public device, can ensure that that session can never be used again. Any service currently logged in will receive an immediate logout message and the credentials used for the authentication session delegation may not be used again to establish a trust path to the user's account. This method provides the user with an advantage over the existing methods which are either relying on time or on the explicit logout of the user while in the borrowed device. Both of these methods suffer from the obvious problems of attacks during the (usually hours long) time window or a simple user that forgets to logout and never has the chance again.

In a specific embodiment a mobile terminal of the user is operated to function as delegator device, which is rather suitable since today the majority of users typically have a mobile phone at hand during the entire course of the day. Moreover, while a mobile device is far from optimal to do all normal operations of its user, it does offer the possibility to establish a more trusted environment for secret material. Thus, this association can then be used to avoid the littering of secret passwords in the public device.

In a basic solution the service and the delegation service may be part of the same administrative domain. However, according to a more sophisticated and global approach it may be provided that the delegation service is part of an identity provider IDP. As is common, the IDP may operate one or more identity management functions that control a plurality of services. The communication between the identity management functions and the services may be realized via typical IDM protocols like SAML and OpenID. Advantageously, the delegated authentication session is adapted to this kind of protocols to ensure full and seamless compatibility with existing services.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end, it is to be referred to the patent claims subordinate to patent claim 1 on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained. In the drawings:

Fig. 1 is a schematic view illustrating a system for supporting user authentication to a service according to a first embodiment of the present invention, and

Fig. 2 is a schematic view illustrating a system for supporting user authentication to a service according to a second embodiment of the present invention.

Fig. 1 schematically illustrates a first embodiment of a system according to the present invention. Generally, in a solution in accordance with the present invention an authentication session between a user in one device is extended to an authentication of the same user in a different device. This authentication session delegation is in full control of the user and is exchanged by executing the steps described in detail hereinafter.

In the embodiment of Fig. 1, the system includes a delegate device 1, which might be a public and/or untrusted terminal device, e.g. an Internet cafe PC, which the user intends to employ for accessing a specific service 2, e.g. Facebook. The present invention requires a secondary device, denoted delegator device 3 hereinafter, which the users expected to already have, e.g. a mobile phone. Furthermore, the system illustrated in Fig. 1, includes a delegation service 4, e.g. an identity provider or an authentication provider, which in the context of the embodiment of Fig. 1 is assumed to belong to the same administrative domain 5 as service 2. The assumption is made that the user is already authenticated with the Delegation Service 4.

In order to initiate service session, in step (1) the user employs his/her personal trusted device – delegator device 3 – to contact the delegation service 4 to obtain a token, which in the described embodiment is assumed to be a One Time Password OTP. In step (2) the user receives the OTP from the delegation service 4.

Subsequent to the provisioning steps (1) and (2), the instantiation steps (3) and (4) are executed. More specifically, in step (3) the user provides the OTP to the delegate device 1. This can be done in many different ways, for instance by manually entering the OTP or by scanning a QR code at the delegator device 3. Alternatively, NFC (Near Field Communication) between the devices may be deployed.

In step (4) the delegate device 1 accesses the delegation service 4, either directly or as a result of an access to a Service, thereby using the OTP received from the delegator device 3. It is to be noted that this step may be executed before step (3) is being executed. As a consequence the delegation service 4 maps the OTP to the session. Furthermore, the delegation service 4 may generate a response message to the delegate device 1, in which it installs the respective session cookie.

In step (5) the delegate device 1 accesses the service 2, which in return verifies in step (6) the authentication with the delegation service 4. In step (7) the delegation service 4 provides to the service 2 the authentication context in accordance with the initial authentication session established between a delegation service 4 and the delegator device 3. Finally, in step (8) the service 2 is provided to the user through the delegate device 1.

Generally, it is important to note that steps (1) to (8) as described above may be executed simultaneously independently of the number of authentication session delegations.

In addition, it is important to note that the operations as described above can be combined with the authentication at the service provider. Such approach would constitute a more monolithic solution, in which the delegation service is offered by the service itself.

Fig. 2 illustrates a second embodiment of a system according to the present invention, which basically is similar to in the embodiment described in connection with Fig. 1. Therefore, in Fig. 2 same reference numerals denote the same components as in Fig. 1.

In contrast to Fig. 1, in which a single service 2 was concerned, the embodiment of Fig. 2 relates to a combination with an Identity Management (IDM) solution.

Identity Management was birthed in the need for single sign on amongst enterprise applications. This need was greatly motivated by the expensive system

integration costs a normal enterprise would have to cover when first establishing their IT infrastructure. Quickly Identity Management became a market on its own and expanded both in terms of features, such as profile and data management, access control/authorization, billing, etc, but also in domain and is now also common in the websphere. Several Identity Management standardization activities spawned from protocols such as SAML, OpenID and Cardspace and the IDM space is now as heterogeneous as it is encompassing.

The typical Identity Management scenario involves an Identity Provider (IDP) and a Service Provider (SP) and the user. The SP, rather than deploying its own user database and authentication methods, relies partly or entirely on the services of the IDP. When the user accesses the SP, the SP contacts the IDP to obtain authentication, identification or data about the user. It's the IDPs responsibility to ensure the process is secure and the user's data protected.

Basically, in the embodiment of Fig. 2 steps (1) to (8) are the same as in Fig. 1. However, both the delegate device 1 (in steps (5) and (8)) and the delegation service 4 (in steps (6) and (7)) do not contact the service 2 requested by the user directly, but via identity management functions 6. Together with the delegation service 4 the identity management functions 6 are part of an Identity Provider IDP 7. The identity management functions 6 typically control a plurality of different services 1...N.

As a further difference to the embodiment of Fig. 1, in step (5) the delegate device 1 accesses the service 2, which may be a consequence of step (4), if initiated by the service 2 which is common in IDM scenarios.

In both embodiments, when the user has finished the operations which require the authentication session delegation the OTP used in the public delegate device 1 is destroyed and cannot be reused to access the delegation. The user can dissociate the delegation from the private delegator device 3, invalidating the delegation from that point on, and he/she can create other delegations if necessary by repeating the process.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. Method for supporting user authentication to a service, wherein the user accesses said service from a terminal device, in particular a public and/or untrusted terminal device,
c h a r a c t e r i z e d i n that an authentication session is established between a trusted device of the user – delegator device (3) – and a delegation service (4), wherein said delegation service (4) provides a token to said delegator device (3), wherein, upon said token being provided to said terminal device – delegate device (1) –, said authentication session is delegated from said delegator device (3) to said delegate device (1).
2. Method according to claim 1, wherein said token includes a one time password.
3. Method according to claim 1 or 2, wherein said token is introduced manually into said delegate device (1).
4. Method according to any of claims 1 to 3, wherein said token is introduced into said delegate device (1) as a Quick Response code or as a two-dimensional barcode.
5. Method according to any of claims 1 to 4, wherein said token is introduced into said delegate device (1) by means of Near Field Communication.
6. Method according to any of claims 1 to 5, wherein said delegate device (1) provides a secure URL where said token can be transferred to.
7. Method according to any of claims 1 to 6, wherein said delegate device (1) accesses said delegation service (4) using said token.
8. Method according to claim 7, wherein said delegation service (4) maps said token to the existing authentication session between said delegation service (4) and said delegator device (3).

9. Method according to claim 7 or 8, wherein said delegation service (4) transmits a response message to said delegate device (1) including the session cookie.
10. Method according to any of claims 1 to 9, wherein said service (3), upon said delegate device (1) accessing said service (2), verifies the authentication with said delegation service (4).
11. Method according to any of claims 10, wherein said delegation service (4) provides said service (2) the authentication context in accordance with the existing authentication session between said delegation service (4) and said delegator device (3).
12. Method according to any of claims 1 to 11, wherein the user is provided said service through said delegate device (1).
13. Method according to any of claims 1 to 12, wherein the parameterization of said delegation of said authentication session is specified while said delegation is active.
14. Method according to claim 13, wherein said parameterization includes information regarding specific services, times and/or devices.
15. Method according to any of claims 1 to 14, wherein said user, in order to terminate the session to said service (2), dissociates said delegation of said authentication session from said delegator device (3).
16. Method according to any of claims 1 to 15, wherein a mobile terminal of the user is operated as said delegator device (3).
17. Method according to any of claims 1 to 16, wherein said service (2) and said delegation service (4) belong to the same administrative domain (5).

18. Method according to any of claims 1 to 17, wherein said delegation service (4) is part of an identity provider (7) including one or more identity management functions (6).

19. Method according to claim 18, wherein said one or more identity management functions (6) and said service (2) are linked to each other via identity management protocols.

20. System for supporting user authentication to a service, in particular for executing a method according to any of claims 1 to 19, including a terminal device, in particular a public and/or untrusted terminal device, from which the user accesses said service,

characterized in that the system further includes

a trusted device of the user – delegator device (3) – and a delegation service (4), with an authentication session being established between those two entities, wherein said delegation service (4) is configured to provide a token to said delegator device (3), and

means that are configured to perform, upon said token being provided to said terminal device – delegate device (1) –, delegation of said authentication session from said delegator device (3) to said delegate device (1).

1/2

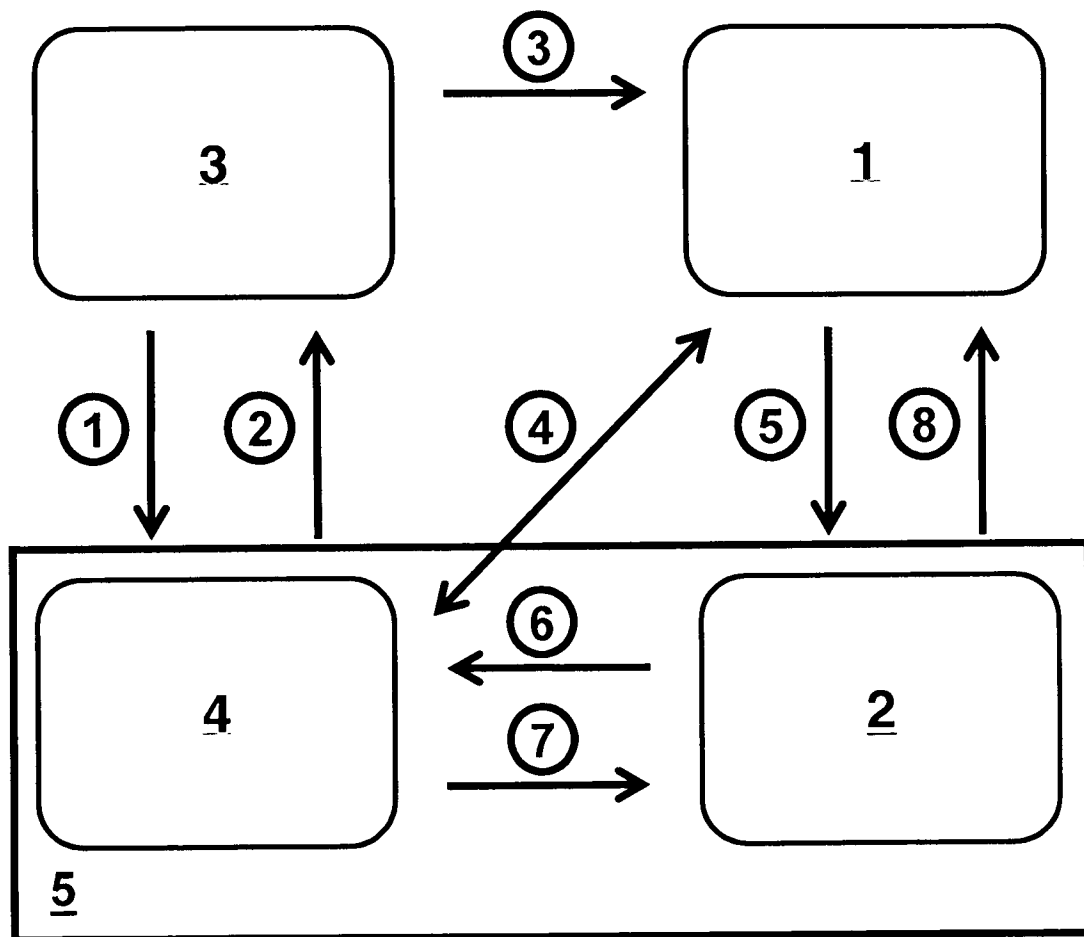
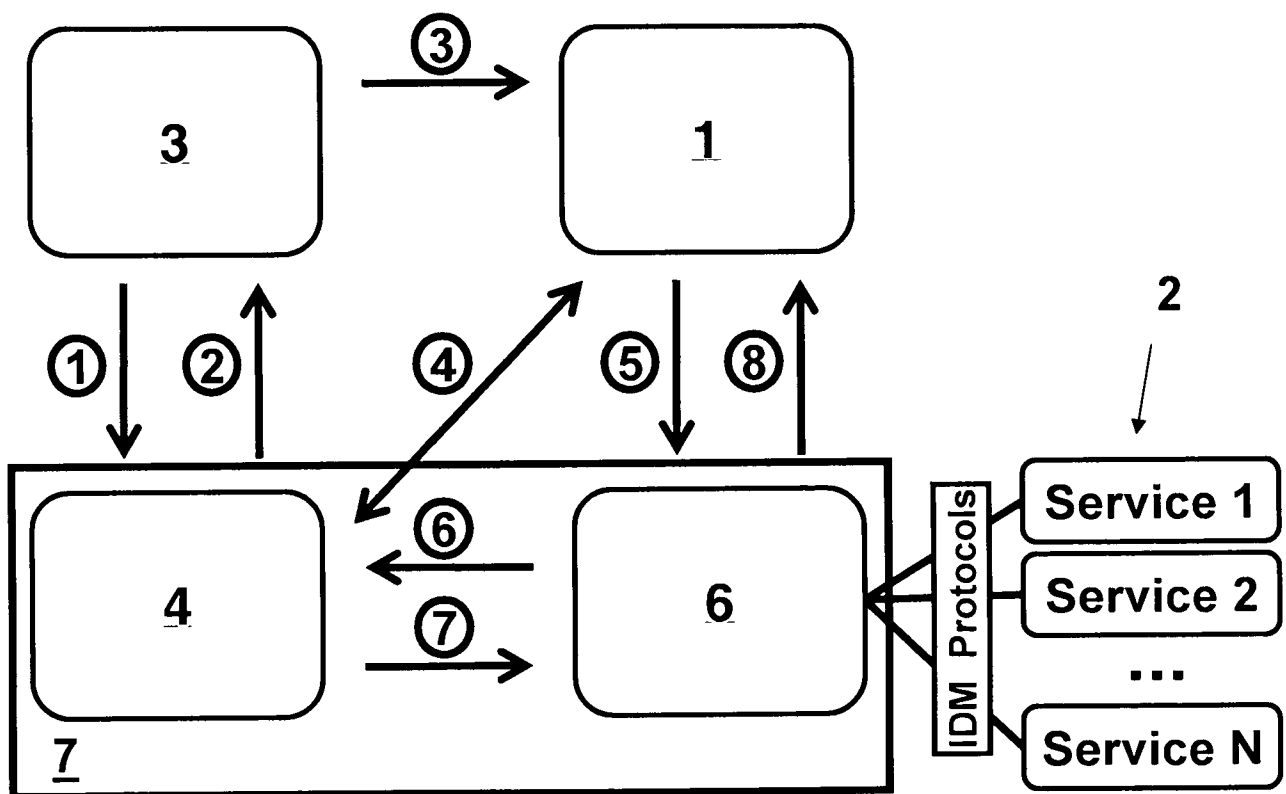


Fig. 1

2/2

**Fig. 2**

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/000649

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 practical, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 262 164 A1 (MICROELECTRONICA ESPANOLA S A [ES]) 15 December 2010 (2010-12-15) abstract paragraph [0025] - paragraph [0029] paragraph [0051] - paragraph [0082] figures 7,8 -----	1-20



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 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

2 November 2011

Date of mailing of the international search report

10/11/2011

Name and mailing address of the ISA/

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

Authorized officer

Dujardin, Corinne

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2011/000649

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
EP 2262164	A1	15-12-2010	WO 2009103824 A1	27-08-2009
			US 2011131640 A1	02-06-2011
