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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 June 2011 (09.06.2011)

PCT

(10) International Publication Number
WO 2011/067139 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/EP2010/068027

(22) International Filing Date:
23 November 2010 (23.11.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09306182.8 4 December 2009 (04.12.2009) EP

(71) Applicant *(for all designated States except US)*: **ALCATEL LUCENT** [FR/FR]; 3, avenue Octave Gréard, F-75007 Paris (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BOSCH, Peter** [NL/NL]; Distelvlinderstraat 4, NL-1432 MN Aalsmeer (NL). **KOLESNIKOV, Vladimir** [CA/US]; 206 W. Shearwater Ct. Apt 52, Jersey City, NJ 07305 (US). **MULLENDER, Sape** [NL/NL]; Prinsengracht 797b, NL-1017 KA Amsterdam (NL). **DAENEN, Koen** [BE/BE]; Neysetterstraat 25, B-3150 Haacht (BE).

(74) Agent: **ALU ANTW PATENT ATTORNEYS**; Copernicuslaan 50, B-2018 Antwerp (BE).

(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**: SYSTEM AND METHOD FOR ACCESSING PRIVATE DIGITAL CONTENT

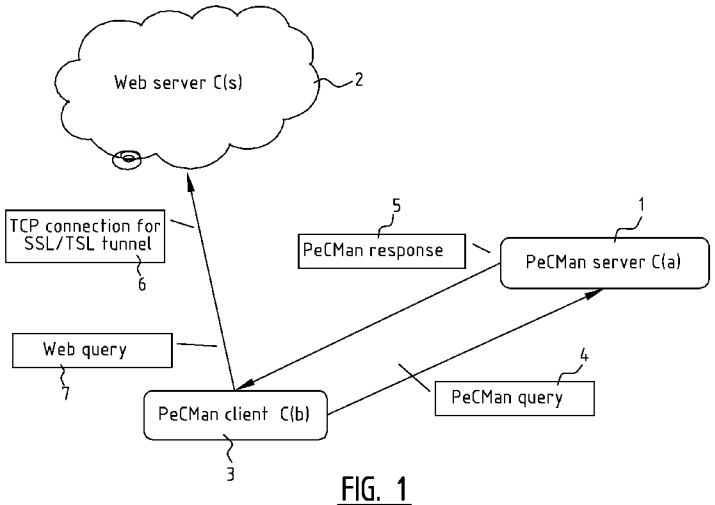

FIG. 1

(57) **Abstract**: Method for providing access to private digital content installed on a content server C (s), wherein a content manager server C (a) has a number of clients potentially interested in the private content; the method comprising the following steps performed at the content management server C (a) : establishing a first communication channel with a client C (b) of the number of clients; receiving a query for private digital content from the client C (b) and sending an appropriate response, causing the client to establish a second communication channel with the content server; establishing a secure session with the content server C (s) over the first and second communication channel; establishing a new session key for the secure session and transmitting said new session key to the client C (b), so that the client can obtain the queried private digital content from the content server as if the client is the content management server.

WO 2011/067139 A1

System and method for accessing private digital content

Technical field

The present invention relates to a system and method for accessing private digital content.

Background

PeCMan is a web application maintaining a list of web objects (data) in the form of URLs (references) with user-provided tags (information). These tags are then used to allow the original contributor (principal user) of the information to (re-)find the references and data, or to share the information and data with others (participant users). These participants can be friends, family, or generally groups of people. The operating model of PeCMan is that PeCMan only maintains the references and tags, and that the referred to objects themselves are retrieved by an application executing on the user's host. Thus the procedure for a participant user is to enter a few tags to PeCMan, PeCMan matches the tags to its information and returns the references to the user, whereupon the user will try to obtain the referred to data.

The PeCMan method for obtaining information from the web works well for publicly available data but fails for private shared data. Private shared data are references to objects that are stored behind, e.g. a password protected web-site. In this case, a user needs to login into the web service offering the referred to data. This is reasonably straightforward if the owner of the referred to data is the same user that is looking for the data. However, sharing private data with participants is a challenge and can only be realized if the principal owner of the data can provide

the participant with the credentials for the service. According to the prior art, to support private non-shared and shared content, the principal PeCMan server typically stores the user credentials with the URL that is being pointed at. If private content is being addressed, a participant PeCMan client sets up a communication channel to a PeCMan server, which then establishes a connection to the storage provider on behalf of the participant PeCMan client, i.e. the PeCMan server acts as proxy for the participant PeCMan client. The downside of this method of data sharing in PeCMan is that all private data are transmitted through the PeCMan proxy. This means that PeCMan can become a bottleneck for accessing private content.

Summary of the invention

According to embodiments of the invention, there is provided an improved method and system for enabling a content management server to establish a secure tunnel to a remote content server, authorizing itself by providing certain credentials, typically the user ID and password, establishing a new session key for the tunnel and signalling a client, typically present inside a user equipment, with the newly established session key to enable the client to continue the conversation with the content server as if the client is the content management server.

According to an embodiment of the invention there is provided a method for providing access to private digital content installed on a content server, wherein a content manager server has a number of clients potentially interested in the private content. The method comprises the following steps performed at the content management server:

- establishing a first communication channel with a client of the number of clients;
- receiving a query for private digital content from the client and sending an appropriate response; this will typically be a trigger for the client to establish a second communication channel with the content server;
- establishing a secure session with the content server over the first and second communication channel;
- establishing a new session key for the secure session and transmitting said new session key to the client C(b).

Typically, before establishing the new session key, a data request will be sent to the content server through the secure session established over the first and second communication channel, wherein e.g. login credentials are provided in case of a secure content server.

This embodiment of the method of the invention will allow the client to obtain the queried private digital content from the content server as if the client is the content management server.

A content management server in the context of the present invention has to be interpreted in the broad sense referring to any server capable of managing for example public and/or private shared and/or private unshared digital content of a plurality of users, such as pictures, video's, etc. The content itself can be stored locally or at a remote location. Examples of such a content management server are simple content management servers, such as used by content providers like Flickr, YoutTube, etc, any type of content aggregators such as PeCMan, SecondBrain, iGoogle, any types of owner's proxies, proxies with selective proxy functionality, etc.

A content server in the context of the present invention typically refers to a secure content server, and can for example be a secure Web-server. Other examples are a local disc with file sharing capabilities, any computer having installed thereon a server program so that the computer functions as a content server, etc.

According to a preferred embodiment the establishing of the secure session consists in establishing any one of the following secure tunnels: a SSL/TLS tunnel, an ESP tunnel. Further, the establishing of the first and/or second communication channel preferably consists in establishing a first and/or second TCP/IP session.

According to a preferred embodiment the web server maintains a client authentication mechanism enabled for SSL/TLS, wherein the establishing of the secure session with the content server comprises authenticating the client node.

According to another embodiment of the invention there is provided a method for obtaining private digital content by a client of a content management server, which private content is installed on a content server. This method comprises the following steps performed by the client:

- establishing a first communication channel with the content management server;
- sending a query for private digital content to the content management server;
- establishing a second communication channel with the content server; said query will typically cause the content management server to set up with the content server a secure session over the first and second communication channel, and

to send a data request to the content server through said secure session;

- receiving a new session key established for the second secure session; and
- obtaining the queried private digital content from the content server using the new session key.

This method allows the client to obtain the private digital content as if the client is the content management server.

According to a possible embodiment a first secure session is established between the client and the content management server; and the new session key is received through said first secure session. In such an embodiment the secure session over the first and second communication channel can use the first secure session.

Further the invention relates to a content management server for organizing private digital content of a plurality of clients. According to an embodiment thereof the content management server is adapted

to establish a secure session with the content server through concatenated channels comprising a first communication channel between the content server and a client and a second communication channel established between said client and the content management server, after having received a query for private digital content from said client,

to send a data request to the content server through the secure connection, and

to establish a new session key for the secure session and transmit said new session key to the client C(b).

Further the invention relates to a system for accessing private digital content, comprising:

- a content management server;
- a content server with digital private content;
- a number of clients; wherein a client is adapted to receive a new session key and to use it for obtaining digital private content from the content server.

Finally the invention relates to a computer program product comprising computer-executable instructions for performing any of the above disclosed methods, when the program is run on a computer.

The accompanying drawings are used to illustrate presently preferred non-limiting exemplary embodiments of the present invention. The above and other advantages of features and objects of the invention will become more apparent and the invention will be better understood from the following detailed description when read in conjunction with the accompanying drawings in which:

Figure 1 illustrates an embodiment of a system according to the invention using a PeCMan system;

Figure 2 illustrates the structure of the communication system used in an embodiment of the method and system of the invention;

Figure 3 illustrates a call flow according to an embodiment implementing the method of the invention.

An exemplary embodiment of the invention will be illustrated below referring to a Personal Content MANagement (PeCMan) server as the content management server, but the skilled person will understand that the invention is applicable to any type of content management server (including owner's

proxies) as defined above. PeCMan is a web tool that organizes user's digital content such as documents, pictures, videos, etc. Figure 1 shows a schematic view of the PeCMan architecture as used in an embodiment of the present invention. A user interacts with the PeCMan server 1 using a client 3 (e.g. a web client, a desktop client or a client on a PDA, etc.) via which the user can e.g. add, remove or tag documents. An incoming request 4 from a client 3 is received by the PeCMan server 1 to be processed by the system. The system further comprises a metadata section (not shown) for storing metadata extracted from the documents or user-generated in the form of tags.

Users can for example upload URLs in PeCMan, semantically tag the information with free-format tags and later find that information back by querying PeCMan with the same tags. Since multiple URLs can be tagged with the same tags, PeCMan enables a user to organize all objects that are kept on a plethora of storage providers (e.g. web servers, home stores or mail servers) through one logical location akin a "virtual drive".

PeCMan recognizes three kinds of references: public, private non-shared and private shared content. Public content are URLs pointing at publicly available web sources. Accessing such content does not require user credentials, which implies that one can easily share such content with whomever is interested in that content. When public information is shared between users, PeCMan simply sends the requested URLs directly to the requesting or secondary PeCMan client and the secondary PeCMan client retrieves the content through e.g. WebDAV or HTTP.

Private content is typically content that can only be accessed through a secured location, typically a secured website (i.e. storage providers). To access secured storage providers 2, a web client 3 first establishes a secure connection 6 e.g. through SSL/TLS, and then provides the user credentials (typically a user-ID and password) to authenticate the user. After a user is authenticated, a web client 3 can access privately stored content via web queries 7. Typically inside the addressed web server 2 a state is allocated that is associated with the communication channel. This state indicates to the web server 2 that the requesting web client 3 has authenticated itself.

According to the prior art, to support private non-shared and shared content, PeCMan typically stores the user credentials with the URL that is being pointed at. If private content is being addressed, a secondary PeCMan client 3 sets up a communication channel to PeCMan 1, which then establishes a connection to the storage provider 2 on behalf of the secondary PeCMan client, i.e. the PeCMan server 4 acts as proxy for the secondary PeCMan client 3. This proxy maintains the secure connection to the web server 2 and is also the one that provides the user credentials to the storage provider 2. PeCMan does this for both shared and non-shared private content references.

The downside of this method of data sharing in PeCMan for private content is that all data associated with the objects pointed at are transmitted through the PeCMan proxy. This means that PeCMan can become a bottleneck for accessing private content and that if charges are associated with data transfers through PeCMan, the PeCMan operator may incur hefty fees for offering private content. Further, executing

the proxy in the realm of the web client is typically not an option since that would imply that user credentials of users need to be shared with the secondary PeCMan client.

An alternative approach for accessing privately shared content is disclosed in European patent application No. 09 305 500.2 in the name of Applicant.

The difference between that patent and this patent is that the former relies that all participants support OAUTH, while this patent disclosure enables the establishment of delegated tunnels without the use of this new standard. In other words, SSL/TLS delegation can be used on web servers that do not use the new OAUTH standard.

In the following discussion the PeCMan server 1 will often be referred to as C(a), and the PeCMan client operating in user equipment (phone, Personal Computer, etc.) will often be referred to as C(b). According to an embodiment of the invention the PeCMan server 1 holds on to user credentials and establishes SSL/TLS sessions with web servers 2, and once the PeCMan server has logged in on a web server 2, it delegates the SSL/TLS tunnel to C(b). How this can be implemented will be further explained with reference to figures 2 and 3.

Figure 3 illustrates an embodiment implementing the method of the invention. Figure 3 shows an exemplary signalling flow in which seven phases can be distinguished for the establishment and delegation of a SSL/TLS session between a PeCMan server C(a), a PeCMan client C(b) and a web server C(s).

In a first phase, the PeCMan client-server communication channel is set up, see steps 301-303 of figure 3. This first phase typically executes when the PeCMan client C(b) is started and establishes a first communication with the PeCMan server C(a). First a communication channel 20 is established between the PeCMan client C(b) and the PeCMan server C(a), see figure 2. Typically TCP endpoints record the remote IP address of the respective correspondent node and maintain protocol state variables on each end of the connection. Given that TCP sessions cannot relocate easily between correspondent nodes and that the eventual communication channel is required between C(s) and C(b), a further TCP session 21 will typically be established between C(b) and C(s), see further below (third phase). Although the figure shows the establishment of a TCP session between two entities, the skilled person will understand that other communication channels can be applicable here.

In a second phase, a secure communication channel is established between the PeCMan client C(b) and the PeCMan server C(a) using the communication channel, in particular the TCP session established in the first phase. The details of the establishment of the secure communication channel are omitted in the figure, but those steps can e.g. be similar to the steps of the fifth stage which is described in detail below. According to a possible embodiment, an encryption protocol providing security for communications over networks is used, such as the Secure Sockets Layer (SSL) or the Transport Layer Security (TLS) protocol (see RFC 5246). Typically, a SSL/TLS session is used with client and server authentication. However, the skilled person will understand that alternate secure tunnel mechanisms would work equally well, such as an Encapsulating Security Payload (ESP) tunnel

as defined in RFC 4303. ESP is a protocol used in the Internet Protocol Security (IPsec) suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. ESP provides origin authenticity, integrity, and confidentiality protection of packets.

In a third phase (step 305), the PeCMan client C(b) queries the PeCMan server C(a) for content. The PeCMan server matches the query to its database and returns a set of URL's that match the query to the PeCMan client. The PeCMan client C(b) will then select one or more URL's for retrieval. In the example it is assumed that at least one of the URL's points to privately shared content on web server C(s), that PeCMan server C(a) holds the user credentials for that web server, and that the communication to the web server holding the content is secured by a SSL/TLS session. According to a preferred embodiment, the query and response requests 305 may be transmitted over the secure channel set up in the second phase, or may be transmitted in the clear over a separate communication channel (not shown).

In a fourth stage, a communication channel is established between the PeCMan client C(b) and the remote web server C(s), see steps 306-308. According to a possible embodiment, this communication channel is based on a simple TCP communication channel.

In a fifth stage (steps 309-312 in figure 3), a SSL/TLS session 22 (see figure 2) is established between the web server C(s) and the PeCMan server C(a) through the TCP communication channel between the C(s) and C(b) established in the fourth stage and the TCP communication channel

established between C(b) and C(a) in the first stage. Details about the exchanged messages can be found in RFC 5246. Note that arrows 310, 311 and 312 do not represent the sending of one single message, but the exchanging of a number of messages as detailed in RFC 5246. In other words the key exchange takes place between the C(s) and C(a) through the TCP endpoint of C(b), through a secured end-2-end channel using two concatenated TCP sessions, wherein it is made impossible for C(b) to capture the web-server credentials. This is a key stage of this embodiment of the invention which will allow the PeCMan client C(b) to continue the conversation with C(s) as if it is C(a) using the new session key established for the tunnel.

The communication between C(b) and C(a) may be transmitted over the SSL/TLS tunnel established in the second phase, or may be transmitted over a non-secured communication (not shown). According to a possible embodiment, client based authentication may be enabled. In such a case, the certificate of C(b) could be used, in which case C(b) needs to sign the last message of the SSL/TLS protocol (steps 309-315). According to an alternative, a new derived certificate that speaks for C(b) may be used by C(a). This will be further elucidated below.

During the fifth stage, typically both ends of the communication channel authenticate each other through the regular SSL/TLS authentication mechanisms. For this the web server C(s) maintains a certificate held in a PKI such as a X.509 certificate as defined in RFC4210. As explained above, if client authentication is enabled for SSL/TLS (which is not by default), the web server authenticates the corresponding node, in the present case C(b). However, since

the SSL/TLS session is first established between C(s) and C(a), C(a) needs C(b)'s certificate. Since C(b)'s certificate is private for C(b) and it is not desirable to share C(b)'s private signing key with C(a), as explained above, three options exist:

- the regular SSL/TLS establishments procedure is followed, but C(a) re-uses C(b)'s certificate when C(s) requests it. According to a possible embodiment C(a) requests C(b) to sign the final SSL/TLS protocol message of step 311 before C(a) transmits the message to C(s). According to an alternative embodiment, the certificate of C(b) is copied to C(a) before the procedure starts; note that this copying can be performed out-of-band, e.g. long before the procedure of figure 3 starts; or
- a new certificate is used that speaks for C(b) and is held by C(a). Such a technique is e.g. disclosed in Butler Lampson et al, entitled "Authentication in Distributed Systems: Theory and Practice", ACM Trans. Computer Systems 10, 4, November 1992, pp 265-310. This new certificate is created and signed by C(b) and used when SSL/TLS executes the client side authentication procedure. The web server C(s) can then verify the authenticity of the new certificate by traversing the key hierarchy starting from the derived certificate held by C(a). Also, typically the new certificate is copied to C(a) before the procedure starts.
- C(a) can request C(b) to sign a certificate with C(b)'s private key, e.g. in cases where certificate chaining is not allowed. In the latter case, C(s) can verify C(a)'s certificate through C(b)'s public key.

In a sixth stage, once the SSL/TLS initiation procedure has completed, data requests can be sent back and forth between the web server C(s) and the PeCMan server C(a), through

C(b)'s TCP session. According to a preferred embodiment, the web server is a typical secured web server, and the PeCMan server C(a) provides the user credentials on the remote web server C(s) by interaction with the web server through the SSL/TLS session set up in the fifth stage. Even though all communication goes through the PeCMan client C(b), this client cannot decipher the messages as it has no knowledge of the used session key for the SSL/TLS tunnel. The web server will send a web page enabling the user to provide its credentials to login to the web server, see step 314. In this case, the PeCMan server C(a) provides the user ID and password for the web server and sends this information to C(s) through the secured SSL/TLS tunnel maintained in part by C(b)'s TCP session, see step 315. Since C(b) does not know the session key for the SSL/TLS tunnel, it can only act as an intermediary and copy the data verbatim between the end points. The PeCMan server C(a) typically remains active on the SSL/TLS tunnel to complete the entire login procedure.

The seventh stage consists in the delegation of the SSL/TLS tunnel from C(a) to C(b). First the PeCMan C(a) and the web server C(s) establish a new session key (not shown in figure 3), and then the PeCMan server C(a) transmits all parameters required for the PeCMan client C(b) to maintain the secure tunnel, the newly established session key being typically an important parameter. Note that it is important to calculate a new key to avoid leakage of the web server credentials to C(b). The parameters required for the PeCMan client C(b) to maintain the secure tunnel include the parameters to cipher/decipher the SSL/TLS session. It is assumed that the web server does not transmit data on the SSL/TLS session during this delegation, since data is only expected when the

client requests data. The communication channel required for the delegation is the secure communication channel established in the second phase above, since the transmitted ciphering material must typically not be transmitted in the clear. Once the PeCMan client has deciphering material, it can obtain privately shared data directly from the web server C(s) as if the request is transmitted form the PeCMan server C(a).

While the principles of the invention have been set out above in connection with specific embodiments, it is to be clearly understood that this description is merely made by way of example and not as limitation of the scope of protection which is determined by the appended claims.

Claims

1. Method for providing access to private digital content installed on a content server C(s), wherein a content manager server C(a) has a number of clients potentially interested in the private content;
the method comprising the following steps performed at the content management server C(a):
- establishing a first communication channel with a client C(b) of the number of clients;
- receiving a query for private digital content from the client C(b) and sending an appropriate response, causing the client to establish a second communication channel with the content server;
- establishing a secure session with the content server C(s) over the first and second communication channel;
- establishing a new session key for the secure session and transmitting said new session key to the client C(b), so that the client can obtain the queried private digital content from the content server as if the client is the content management server.

2. Method of claim 1, wherein the method further comprises sending a data request to the content server through the secure session established over the first and second communication channel.

3. Method according to claim 1 or 2, wherein the establishing of the secure session consists in establishing any one of the following secure tunnels: a SSL/TLS tunnel, an ESP tunnel.

4. Method according to any of the previous claims, wherein the establishing of the first and/or second communication channel consists in establishing a first and/or second TCP/IP session.

5. Method according to any of the previous claims, wherein the web server C(s) maintains a client authentication mechanism enabled for SSL/TLS, wherein the establishing of the secure session with the content server C(s) comprises authenticating the client node C(b).

6. Method according to claim 5, wherein the authenticating of the client node C(b) is made possible by re-using the client's certificate when requested by the content server by requesting the client to sign the final SSL/TLS protocol message before transmitting said message to the content server.

7. Method according to claim 5, wherein the authenticating of the client node C(b) is made possible by using a new certificate signed by the client C(b) and held by the content management server C(a), such that the content server C(s) can verify the authenticity of the new certificate.

8. Method for obtaining private digital content by a client C(b) of a content management server C(a), which private content is installed on a content server, comprising the following steps performed by the client:
- establishing a first communication channel with the content management server C(a);
- sending a query for private digital content to the content management server;

- establishing a second communication channel with the content server C(s), said query causing the content management server to set up with the content server a secure session over the first and second communication channel;
- receiving a new session key established for the second secure session; and
- obtaining the queried private digital content from the content server using the new session key as if the client is the content management server.

9. Method of claim 8, wherein said query further causes the content management server to send a data request to the content server through said secure session.

10. Method of claim 8 or 9, wherein a first secure session is established between the client C(b) and the content management server C(a); and the new session key is received through said first secure session.

11. Method of any of the claims 8-10, wherein the secure session over the first and second communication channel uses the first secure session.

12. Content management server for organizing private digital content of a plurality of clients, adapted

to establish a secure session with the content server after having received a query for private digital content from a client, and

to establish a new session key for the secure session and transmit said new session key to the client C(b), so that the client can obtain the queried private digital content from the content server as if the client is the content management server.

13. Content management server of claim 12, wherein the content management server is a content aggregator such as a PeCMan server.

14. System for accessing private digital content, comprising:
- a content management server according to claim 12 or 13;
- a content server with digital private content;
- a number of clients; wherein a client is adapted to receive said new session key and to use it for obtaining digital private content from the content server.

15. A computer program product comprising computer-executable instructions for performing a method according to any of the claims 1-11, when the program is run on a computer.

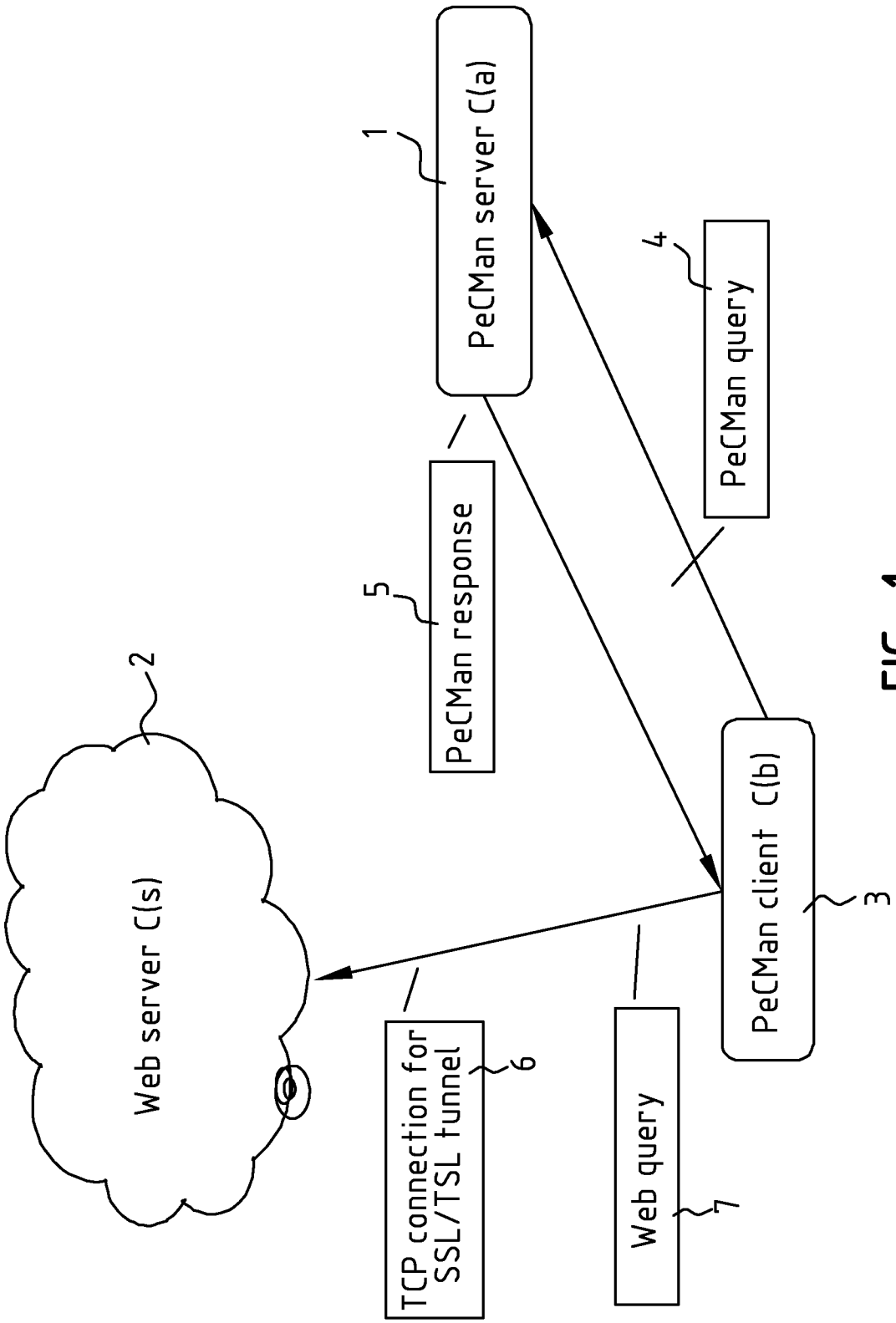
PeCMan server C(a)
1
PeCMan query
4
PeCMan response
5
Web server C(s)
2
PeCMan client C(b)
3
TCP connection for SSL/TSL tunnel
6
Web query
7

FIG. 1

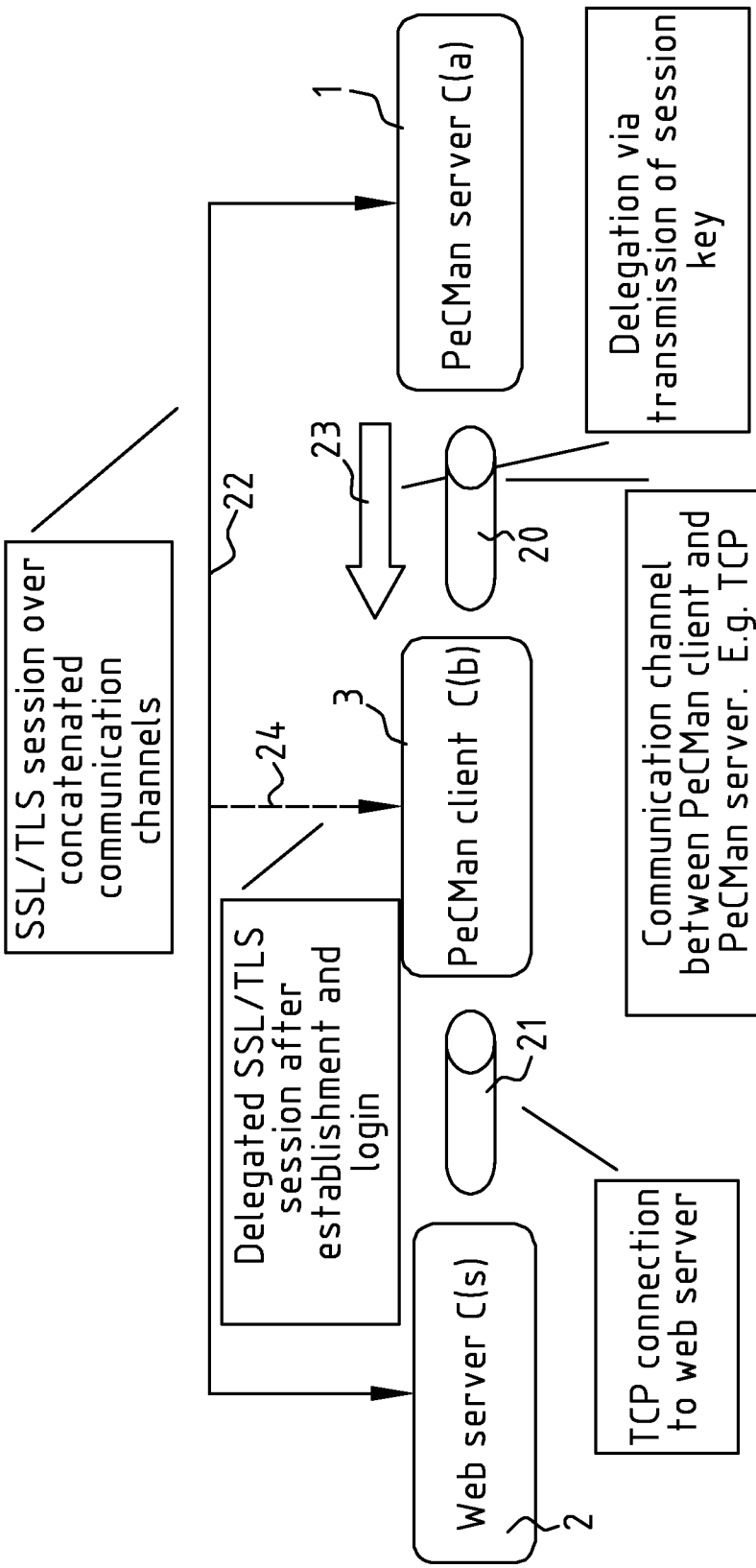
PeCMan server C(a)
1
Delegation via transmission of session key
23
22
20
SSL/TLS session over concatenated communication channels
Communication channel between PeCMan client and PeCMan server. E.g. TCP
24
3
PeCMan client C(b)
Delegated SSL/TLS session after establishment and login
21
TCP connection to web server
Web server C(s)
2

FIG. 2

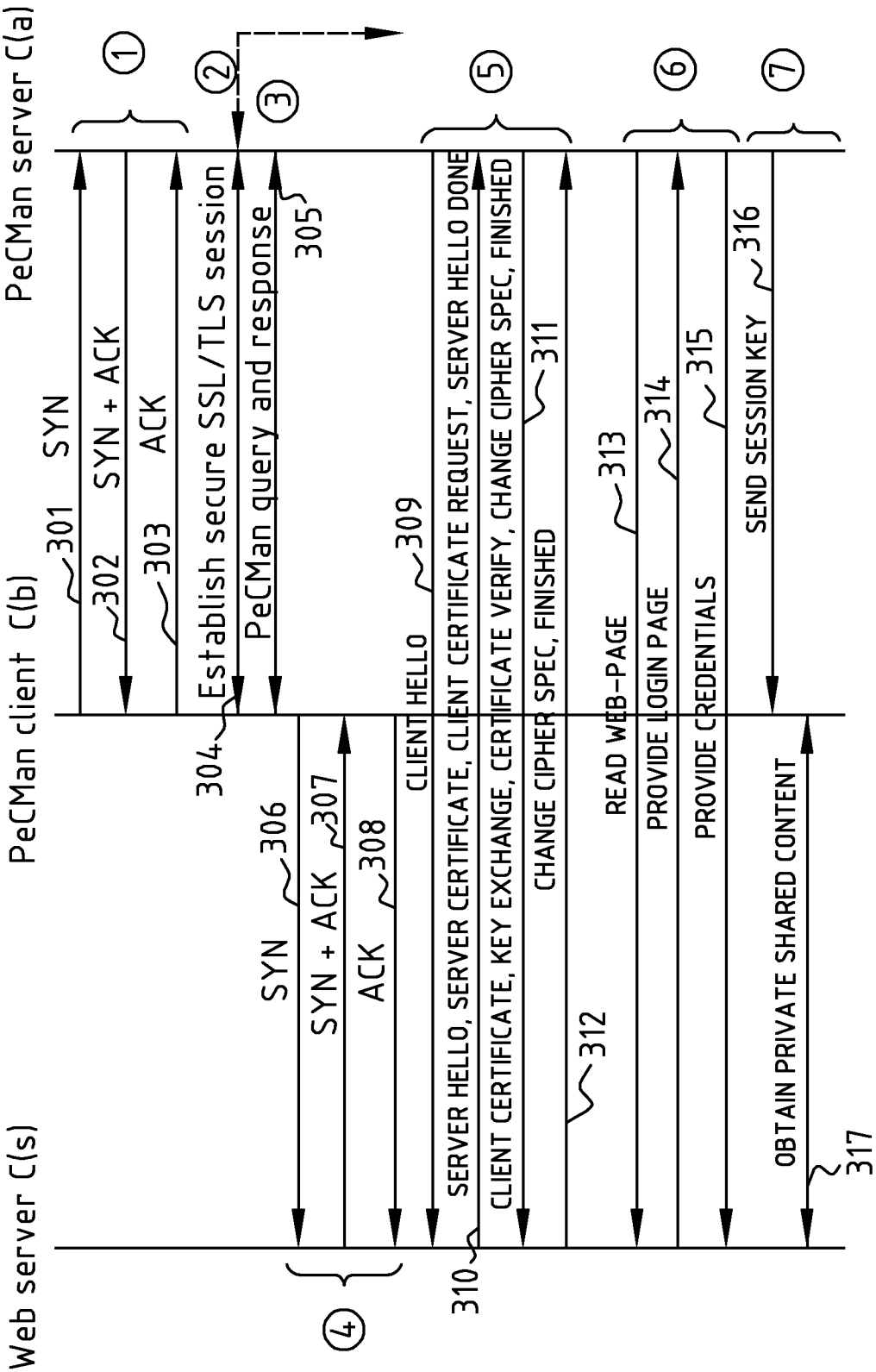
PeCMan server C(a)
PeCMan client C(b)
Web server C(s)
SYN
SYN + ACK
ACK
Establish secure SSL/TLS session
PeCMan query and response
CLIENT HELLO
SERVER HELLO, SERVER CERTIFICATE, CLIENT CERTIFICATE REQUEST, SERVER HELLO DONE
CLIENT CERTIFICATE, KEY EXCHANGE, CERTIFICATE VERIFY, CHANGE CIPHER SPEC, FINISHED
CHANGE CIPHER SPEC, FINISHED
READ WEB-PAGE
PROVIDE LOGIN PAGE
PROVIDE CREDENTIALS
SEND SESSION KEY
OBTAIN PRIVATE SHARED CONTENT
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
1
2
3
4
5
6
7

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/068027

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/08
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 H04W G06F

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

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

EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 260 224 B1 (INGLE KEN L [US] ET AL) 21 August 2007 (2007-08-21) * abstract; figures 1-4 column 2, line 36 - column 3, line 2 column 3, line 52 - column 4, line 38 column 6, lines 31-40 column 12, line 21 - column 14, line 19 column 16, lines 39-41 -----	1-15
X	EP 2 012 460 A1 (NOVELL INC [US]) 7 January 2009 (2009-01-07) * abstract; figures 1,3 paragraphs [0006], [0011] paragraphs [0014] - [0023] -----	1-15

-/--

[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 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	Date of mailing of the international search report
19 January 2011	28/01/2011

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	Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/068027

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006/155997 A1 (FRITZGES ERIC A [US] ET AL) 13 July 2006 (2006-07-13) * abstract; figures 1-3 paragraphs [0044] - [0063] paragraphs [0066] - [0073] -----	1-15
A	US 7 565 526 B1 (SHAW ANDREW [GB] ET AL) 21 July 2009 (2009-07-21) * abstract; figures 4,5 column 6, line 34 - column 9, line 41 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/068027

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7260224 B1	21-08-2007	NONE	
EP 2012460 A1	07-01-2009	EP 1662692 A2	31-05-2006
		US 2010211771 A1	19-08-2010
		US 2010239095 A1	23-09-2010
		US 2010223459 A1	02-09-2010
		US 2006115089 A1	01-06-2006
US 2006155997 A1	13-07-2006	NONE	
US 7565526 B1	21-07-2009	NONE	