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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 August 2015 (20.08.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/122813 Al

(51) International Patent Classification:
G06F 17/30 (2006.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/SE20 14/050 184

(22) International Filing Date:
14 February 2014 (14.02.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **TELEFONAKTIEBOLAGET L M ERIC¬SSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: **WESTBERG, Lars;** Langtora Gran 11, S-745 96 Enkoping (SE). **ERIKSSON, Hans;** Runskogsvagen 44, S-192 48 Sollentuna (SE). **KÖHLI, Johan;** Slanbarss-lingan 22, S-185 39 Vaxholm (SE).

(74) Agent: **KRANSELL & WENNBORG KB;** P.O. Box 27834, S-1 15 93 Stockholm (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on nextpage]

WO 2015/122813 A1

(54) Title: CACHING OF ENCRYPTED CONTENT

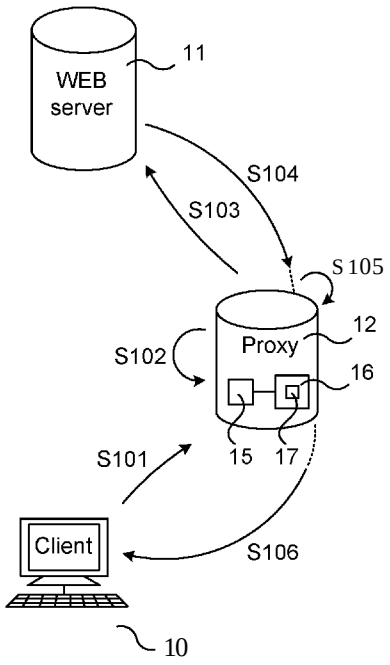

Fig. 2a

(57) Abstract: The invention relates to a transparent proxy as well as methods of caching and providing encrypted data content at the transparent proxy. In a first aspect of the present invention, a method of providing requested encrypted data content at a transparent proxy (12) in a communications network is provided. The method comprises receiving from a client (10) an encrypted identifier indicating the requested encrypted data content at the proxy, identifying the encrypted data content from the received encrypted identifier, determining whether the client is authorized to access the encrypted data content, and if so providing the requested encrypted data content to the client.

Declarations under Rule 4.17:

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

Published:

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

CACHING OF ENCRYPTED CONTENT

TECHNICAL FIELD

The invention relates to a transparent proxy as well as methods of caching and providing encrypted data content at the transparent proxy, and further a computer program and a computer program product.

BACKGROUND

Transparent Internet Caching (TIC) is an established technology for improving web browsing performance and resource utilization. In TIC, data content can be stored at a transparent proxy server, such as e.g. a Hypertext Transfer Protocol (HTTP) cache, being transparent to an end-user. This is undertaken by intercepting the HTTP traffic and creating a local cache of often requested content typically identified by frequently accessed Uniform Resource Locators (URLs) pointing to the data content. The popular data content is thus transferred to the transparent proxy server from a web server originally providing the content.

For instance, a user at a client browses a web site of a newspaper and requests a particular web page, and is directed to an HTTP proxy where the requested resource in the form of the particular web page is provided, for instance by fetching the web page from a proxy cache, or the HTTP proxy turns to the a web server of the newspaper for the requested resource, receives the resource, and finally provides the resource to the client. The purpose of the proxy is to enhance the user's experience through the faster and better responses it can provide. Further, by caching frequently requested content, the web server is relieved from responding to the requests. The proxy is transparent to the user in that the user does not know (or cares) that he/she is communicating with the proxy, and not with the server. Thus, the transparent proxy server is commonly arranged in a communication path between the client/user and the web server with which the client wishes to communicate in order to reduce response time to the user requests.

Encryption of data traffic over the Internet has drastically increased during the last years. In HTTP 2.0 based on SPDY protocol, URLs are encrypted using Transport Layer Security (TLS) cryptographic protocols. A problem remains in that encryption of URL makes caching of data difficult since the transparent proxy server cannot identify the content.

SUMMARY

An object of the present invention is to solve, or at least mitigate, this problem in the art and provide an improved transparent proxy and a method at a transparent proxy of providing encrypted data content to a client.

This object is attained in a first aspect of the present invention by a method of providing requested encrypted data content at a transparent proxy in a communications network. The method comprises receiving from a client an encrypted identifier indicating the requested encrypted data content at the proxy, identifying the encrypted data content from the received encrypted identifier, determining whether the client is authorized to access the encrypted data content, and if so providing the requested encrypted data content to the client.

This object is further attained by a transparent proxy in a communications network according to the first aspect of the present invention. The proxy comprises a processor and a memory, which memory contains instructions executable by the processor, whereby the proxy is operative to receive from a client an encrypted identifier indicating requested encrypted data content provided at the proxy, to identify the encrypted data content from the received encrypted identifier, and to determine whether the client is authorized to access the encrypted data content. Further, the proxy is operative to provide the requested encrypted data content to the client.

Advantageously, encrypted data content designated by an encrypted identifier, such as e.g. an encrypted URL pointing to the data content, is used to provide security at a transparent proxy. Thus, the encrypted identifier is interpreted at the transparent proxy, however without being decrypted

thereby conserving confidentiality, in order for the proxy to know to which particular encrypted data content the client request is made; a great number of encrypted data content is typically stored at the proxy. Further, in order to enhance security, the transparent proxy determines whether the client is authorized to access the encrypted data content. This can be undertaken in various different manners, as will be discussed in the following. For instance, the cryptographic key used to encrypt the identifier designating the encrypted data content must be the same as the key that was used for encrypting the data content. If so, the encrypted data content is provided to the client by the transparent proxy. In this context, it should be noted that the transparent proxy is not capable of decrypting the encrypted data content to provide the data content in clear text.

The object of the present invention is further attained in a second aspect of the present invention by a method of caching requested encrypted data content at a transparent proxy in a communications network. The method comprises receiving from a client an encrypted identifier indicating the requested encrypted data content to be provided at the proxy, determining whether the requested encrypted data content should be cached at the proxy, and sending a request for the encrypted data content to a server providing the encrypted data content. Thereafter, the requested encrypted data content is associated with the received encrypted identifier and cached at the proxy.

Moreover, the object is attained by a transparent proxy in a communications network according to the second aspect of the present invention. The proxy comprises a processor and a memory, which memory contains instructions executable by the processor, whereby the proxy is operative to receive from a client an encrypted identifier indicating requested encrypted data content to be provided at the proxy, to determine whether the requested encrypted data content should be cached at the proxy, and to send a request for the encrypted data content to a server providing the encrypted data content. Further, the proxy is operative to associate the requested encrypted data content with the received encrypted identifier and to cache the requested encrypted data content at the proxy.

Advantageously, encrypted data content designated by an encrypted identifier, such as e.g. an encrypted URL pointing to the data content, is used to provide security at a transparent proxy. Thus, the encrypted identifier is interpreted at the transparent proxy, however without being decrypted thereby conserving confidentiality, in order for the proxy to know to which particular encrypted data content the client request is made; a great number of encrypted data content is typically stored at the proxy. Further, in case the requested encrypted data content is not stored at the proxy, the proxy determines whether in fact it should be stored. If so, the transparent proxy fetches the requested encrypted data content from the a server designated by the encrypted identifier, whereby the encrypted data content is received by the proxy from the server and associated with the encrypted identifier (e.g. the encrypted URL), and caches the encrypted data content such that it subsequently can be provided to a requesting client. Again, the transparent proxy does not have access to the data content in clear text, but only to the encrypted version, thereby providing an appropriate degree of confidentiality.

Thus, a group of data content are considered as "allowed for caching", for instance a group of data content provided by one and the same content provider, or a group of data content provided by one and the same content server. Consequently, in an embodiment of the present invention, all identifiers (e.g. URLs) and the corresponding data content belonging to the same group can be encrypted with the same encrypted key, thereby providing security while still easing the burden for the transparent proxy to identify encrypted data content from encrypted identifiers designating the encrypted content. The encrypted identifiers may be interpreted using well known deep packet inspection (DPI) methods or HTTP protocol information in order to identify the corresponding encrypted data content without actually decrypting the encrypted identifiers.

In a further embodiment of the present invention, it is determined at the transparent proxy that the requested encrypted data content should be cached at the proxy if the number of requests for the encrypted data content

exceeds a request threshold value. Thus, much requested encrypted data content are advantageously cached at the transparent proxy. This embodiment will further advantageously allow the transparent proxy to detect that the same URL (even if encrypted) is requested many times and with that information (the same encrypted URL) understand that encrypted data content designated by that URL should be cached. It should be noted that the data content not necessarily are static but in practice oftentimes are dynamic, such as for instance news information provided by a newspaper web server. Again, the proxy does not know the cleartext URL or the cleartext data content, but is still capable of caching the encrypted data content and associating it with its encrypted identifier.

As can be deducted from the above, the present invention allows transparent caching of encrypted URLs and correspondingly designated encrypted data content in e.g. HTTP 2.0. The caching is more secure as the proxy neither knows the actual, clear text URL address nor the corresponding encrypted data content. Only clients capable of verifying their right to access a particular encrypted data content (e.g. by means of proving that they in fact have access to the encryption key for instance by presenting a key identifier). A content provider can thus advantageously control a client's access to encrypted data content in a simple and straightforward yet secure manner.

In a further advantageous embodiment of the present invention, encrypted data content is flushed from the cache of the proxy if it has not been requested for some time period. The content provider could thus change encryption key to improve security, and the data content encrypted with the "old" encryption key will thus be removed from the cache since it is no longer requested; even if the URL would be selected to be the same for a new encrypted data content as for a previously stored data content encrypted with the old key, the identifier created by means of encrypting the URL with the new key would differ.

Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise

herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is now described, by way of example, with reference to the accompanying drawings, in which:

Figure l illustrates a communications network in which the present invention maybe implemented;

Figure 2a illustrates a transparent proxy according to an embodiment of the present invention;

Figure 2b illustrates a flowchart of a method at the transparent proxy of Figure 2a according to an embodiment of the present invention;

Figure 3a illustrates a transparent proxy according to a further embodiment of the present invention;

Figure 3b illustrates a flowchart of a method at the transparent proxy of Figure 3a according to a further embodiment of the present invention;

Figure 4a illustrates a proxy according to another embodiment of the present invention; and

Figure 4b illustrates a proxy according to yet another embodiment of the present invention.

DETAILED DESCRIPTION

The invention will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth

herein; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout the description.

Figure l illustrates a communications network in which the present invention maybe implemented comprising a client io, a web server n , and a transparent proxy 12 providing resources on behalf of the web server 11. The web server will in the following be referred to as "the server". The client 10 is a network node typically embodied in the form of user equipment (UE) such as a mobile phone, a personal digital assistant (PDA), a smart phone, a tablet, a laptop, a media player, etc.

For instance, a user at the client 10 browses a web site of a newspaper and requests a particular web page, and is directed to the proxy 12 where the requested resource in the form of the particular web page is provided, for instance by fetching the web page from a proxy cache, or the proxy 12 turns to the server 11 for the requested resource, receives the resource, and finally provides the resource to the client 10. The purpose of the proxy is to enhance the user's experience through the faster and better responses it can provide. The proxy is transparent to the user in that the user does not know (or cares) that he/ she is communicating with the proxy 12, and not with the server 11.

An example of a proxy is a caching proxy which speeds up service requests of clients by retrieving, from the server 11, content saved from a previous request made by the same client or even other clients. Thus, caching proxies advantageously store local copies of frequently requested resources, allowing reduction of client bandwidth usage (typically a great number of clients are routed via the caching proxy, such as e.g. all users in a larger enterprise), while increasing performance.

Figure 2a and 2b respectively illustrates a transparent proxy 12 according to an embodiment of the present invention, and a flowchart of a method at a transparent proxy in a communications network according to an embodiment

of the present invention. Figures 2a and 2b illustrate an embodiment of an aspect of the invention where data content requested by the client 10 yet not has been cached at the transparent proxy 12. The method at the proxy 12 is typically performed by a processing unit 15 embodied in the form of one or more microprocessors arranged to execute a computer program 17 downloaded to a suitable storage medium 16 associated with the microprocessor, such as a Random Access Memory (RAM), a Flash memory or a hard disk drive. The processing unit 15 is arranged to at least partly carry out the method according to embodiments of the present invention when the appropriate computer program 17 comprising computer-executable instructions is downloaded to the storage medium 16 and executed by the processor 15. The storage medium 16 may also be a computer program product comprising the computer program 17. Alternatively, the computer program 17 may be transferred to the storage medium 16 by means of a suitable computer program product, such as a Digital Versatile disc (DVD) or a memory stick. As a further alternative, the computer program 17 may be downloaded to the storage medium 16 over a network. The processing unit 15 may alternatively be embodied in the form of an application specific integrated circuit (ASIC), a field-programmable gate array (FPGA), a complex programmable logic device (CPLD), a digital signal processor (DSP), etc.

Thus, with reference to Figures 2a and 2b, a user at the client 10 requests data content, for instance by using a browser at the client 10 to access a home page hosted by the web server 11. Since communication is required to be secure, at least a part of the HTTP request is encrypted at the client 10 before being submitted by using an encryption key which is common with that used at the web server 11 for encrypting the requested data content. The transparent proxy 12 receives in step S101 the request for data content, which comprises an encrypted identifier designating the requested data content. In in example, the encrypted identifier is an encrypted URL addressing the requested data content. The proxy 12 uses e.g. DPI for interpreting the encrypted URL in order to be able to address the web server 11 (or as will be described, to fetch the requested encrypted data content from a local cache).

Hence, due to confidentiality requirements, the proxy 12 is not capable of decrypting the encrypted URL but uses DPI or any other appropriate approach for addressing the destination of the request, i.e. the web server 11. When receiving the request. The proxy 12 determines in step S102 whether the requested content should be cached, typically as a result of the data content being frequently requested. If that is the case for this particular requested data content (and given that the requested data content is not already cached at the proxy), the proxy 12 sends in step S103 a request for the encrypted data content to the web server 11 providing the encrypted data content in accordance with the encrypted URL comprised in the request previously sent by the client 10 to the proxy 12. It should be noted that the web server 11 is capable of decrypting the encrypted URL, as well as stored encrypted data content. In step S104, the proxy receives the requested encrypted data content and associates the encrypted data content with the previously received encrypted URL and stores the encrypted data content in a cache 16. It is also possible that a hashing operation is performed on the encrypted URL at the proxy 12 to produce an identifier identifying the requested content. Subsequently, the encrypted data content may be provided by the proxy 12 to the client 10 in step S105.

Figure 3a and 3b respectively illustrates a transparent proxy 12 according to a further embodiment of the present invention, and a flowchart of a method at a transparent proxy in a communications network according to an embodiment of the present invention. Figures 3a and 3b illustrate an embodiment of an aspect of the invention where data content requested by the client 10 has been cached at the transparent proxy 12, as was described with reference to Figures 2a and 2b. The method at the proxy 12 is typically performed by a processing unit 15 embodied in the form of one or more microprocessors arranged to execute a computer program 17 downloaded to a suitable storage medium 16 associated with the microprocessor as described in detail in the above.

Thus, with reference to Figures 3a and 3b, a user at the client 10 requests data content, for instance by using a browser at the client 10 to access a home

page hosted by the web server 11. Since communication is required to be secure, at least a part of the HTTP request is encrypted at the client 10 before being submitted by using an encryption key which is common with the encryption key that initially was used at the web server 11 for encrypting the requested data content. The transparent proxy 12 receives in step S201 the request for data content, which comprises an encrypted identifier designating the requested data content. In an example, the encrypted identifier is an encrypted URL addressing the requested data content. It is further possible that a hashing operation is performed on the encrypted URL at the proxy 12 to produce an identifier identifying the requested content. The proxy 12 uses e.g. DPI for interpreting the encrypted URL in step S202 in order to be able to fetch the requested encrypted data content from the local cache 16. Hence, due to confidentiality requirements, the proxy 12 is not capable of decrypting the encrypted URL but uses DPI or any other appropriate approach for addressing the destination of the request, i.e. the particular address(es) in the cache 16 where the requested encrypted data content is stored. In step S203, it is determined whether the client 10 in fact is authorized to access the requested encrypted data content. This can be undertaken in various different manners, as will be discussed in the following. For instance, the cryptographic key used to encrypt the identifier designating the encrypted data content must be the same as the key that was used for encrypting the data content. This maybe indicated by means of a numeric key identifier included in the request. If the client 10 is authorized, the encrypted data content is provided to the client 10 by the proxy 12 in step S204.

In traditional caching systems, it is possible to specify data sharing classes for different data content. Currently, following classes are possible:

a. Public shared content, used for instance in applications relating to Digital Rights Management (DRM) where intermediates should not be capable of modifying data content,

b. Private content, and

c. Private and shared, associated for a group of end-users.

The present invention is well suited for handling these different data sharing classes by using different encryption approaches depending on the selected data sharing class:

a. "Public shared content" are allocated with the same encryption key for a particular data content, i.e. the same encryption key are utilized for all clients to access the same URL. This may be used in a relatively large group, such as an organization comprising hundreds or even thousands of people.

b. "Private content" have an individual encryption key per client and URL, i.e. only a single user is capable of accessing data content located at a particular URL.

c. "Private and shared" have a unique encryption key per client group and URL, i.e. a limited number of clients are capable of accessing data content located at a particular URL. This is typically a smaller group than that under a "Public shared content", such as a team within an large organization.

As previously mentioned, the same encryption key is typically used for encrypting the identifier (i.e. URL) and the data content addressed by the identifier.

It should be noted that the proxy 12 could be associated with different web servers, or domains, one of which is embodied by the server 11. A way for the proxy 12 to distinguish between different domains is to use the so called fully qualified domain name (FQDN). The domain name maybe associated with encryption key in order for the proxy 12 to identify different domains.

In a further embodiment of the present invention, in order to determine whether a client is authorized to access encrypted data content, an International Mobile Subscriber Identity (IMSI) of the client is used. Thus, when determining whether the client is authorized to receive requested encrypted data content, the proxy compares the IMSI with a previously registered list of IMSIs supplied by the web server to indicate which clients

should be entrusted with the encrypted data content cached at the proxy. However, it should be noted that other unique client identifiers could be used, such as Media Access Control (MAC) address, Network Access Identifier (NAI) address (e.g. "yourname@mydomain"), or client device serial number, or any other appropriate unencrypted parameter added to the request by the client.

Figure 4a shows a transparent proxy 12 according to an embodiment of the first aspect of the present invention. The proxy 12 comprises receiving means 21 adapted to receive, from a client, an encrypted identifier indicating requested encrypted data content at the proxy, and identifying means 22 adapted to identify the encrypted data content from the received encrypted identifier. The receiving means 21 may comprise a communications interface for receiving and providing information to the client, and/ or for receiving and providing information to other devices, such as a server. Further, the proxy 12 comprises determining means 23 adapted to determine whether the client is authorized to access the encrypted data content. Moreover, the proxy 12 comprises providing means 24 adapted to providing the requested encrypted data content to the client. The providing means 24 may comprise a communications interface for providing information to the client, and/ or for providing information to other devices, or share communications interface with the receiving means 21. The providing means 24 may further comprise a local storage for caching data. The receiving means 21, identifying means 22, determining means 23 and providing means 24 may (in analogy with the description given in connection to Figure 2a) be implemented by a processor embodied in the form of one or more microprocessors arranged to execute a computer program downloaded to a suitable storage medium associated with the microprocessor, such as a RAM, a Flash memory or a hard disk drive. The receiving means 21 and providing means 24 may comprise one or more transmitters and/or receivers and/or transceivers, comprising analogue and digital components and a suitable number of antennae for radio communication.

Figure 4b shows a transparent proxy 12 according to an embodiment of the second aspect of the present invention. The proxy 12 comprises receiving means 31 adapted to receive, from a client, an encrypted identifier indicating requested encrypted data content to be provided at the proxy, and determining means 32 adapted to determine whether the requested encrypted data content should be cached at the proxy. The receiving means 31 may comprise a communications interface for receiving and providing information to the client, and/ or for receiving and providing information to other devices, such as a server.

Further, the proxy 12 comprises sending means 33 adapted to send a request for the encrypted data content to a server providing the encrypted data content, and associating means 34 adapted to associate the requested encrypted data content with the received encrypted identifier. The sending means 33 may comprise a communications interface for providing information to the server, and/ or for providing information to other devices, or share communications interface with the receiving means 21. The proxy 12 also comprises caching means 35 adapted to cache the requested encrypted data content received from the server at the proxy. The caching means 35 may further comprise a local storage for caching data. The receiving means 31, determining means 32, sending means 33, associating means 34 and caching means 35 may (in analogy with the description given in connection to Figure 2a) be implemented by a processor embodied in the form of one or more microprocessors arranged to execute a computer program downloaded to a suitable storage medium associated with the microprocessor, such as a RAM, a Flash memory or a hard disk drive. The receiving means 31 and sending means 33 may comprise one or more transmitters and/or receivers and/or transceivers, comprising analogue and digital components and a suitable number of antennae for radio communication.

The invention has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims.

CLAIMS

1. A method of providing requested encrypted data content at a transparent proxy in a communications network, comprising:

receiving (S201) from a client an encrypted identifier indicating the requested encrypted data content at the proxy;

identifying (S202) the encrypted data content from the received encrypted identifier;

determining (S203) whether the client is authorized to access the encrypted data content; and if so

providing (S204) the requested encrypted data content to the client.

2. The method of claim 1, wherein the identifier and the data content are encrypted with the same cryptographic key.

3. The method of claim 2, wherein the step of determining whether the client is authorized to access the encrypted data content comprises:

verifying that the client has access to the cryptographic key used to encrypt the identifier and the data content.

3. The method of claims 1 or 2, further comprising the step of:

performing a hashing operation on the encrypted identifier, wherein the encrypted data content is identified from the hashed encrypted identifier.

4. The method of any one of claims 1-3, the encrypted identified being an encrypted Universal Resource Locator, URL.

5. The method of any one of claims 1-4, wherein all clients requesting the encrypted data content uses the same encryption key to encrypt the identifier indicating the encrypted data content.

6. The method of any one of claims 1-4, wherein a group of clients requesting the encrypted data content uses the same encryption key to encrypt the identifier indicating the encrypted data content.

7. The method of any one of claims 1-4, wherein each client requesting the encrypted data content uses an individual encryption key to encrypt the identifier indicating the encrypted data content.

8. The method of any one of the preceding claims, wherein the step of determining whether the client is authorized to access the encrypted data content comprises:

verifying that a client identifier received from the client matches a client identifier received from a server (11) providing the requested encrypted data content to the proxy.

9. The method of claim 8, the client identifier is one or more of International Mobile Subscriber Identity, IMSI, Media Access Control, MAC, address, Network Access Identifier, NAI, address, or client device serial number.

10. A method of caching requested encrypted data content at a transparent proxy in a communications network, comprising:

receiving (S101) from a client an encrypted identifier indicating the requested encrypted data content to be provided at the proxy;

determining (S102) whether the requested encrypted data content should be cached at the proxy;

sending (S103) a request for the encrypted data content to a server providing the encrypted data content;

associating (S104) the requested encrypted data content with the received encrypted identifier; and

caching (S105) the requested encrypted data content at the proxy.

11. The method of claim 10, wherein it is determined that the requested encrypted data content should be cached at the proxy if the number of requests for the encrypted data content exceeds a request threshold value.

12. The method of claims 10 or 11, wherein a selected group of encrypted data content and a corresponding group of encrypted identifiers identifying a

respective encrypted data content are encrypted with the same cryptographic key.

13. The method of any one of claims 10-12, further comprising:

removing the encrypted data content from the proxy if it has not been requested for a predetermined time period.

14. A transparent proxy (12) in a communications network comprising: a processor (15) and a memory (16), said memory containing instructions executable by said processor, whereby said proxy is operative to:

receive from a client (10) an encrypted identifier indicating requested encrypted data content provided at the proxy;

identify the encrypted data content from the received encrypted identifier;

determine whether the client is authorized to access the encrypted data content; and if so

provide the requested encrypted data content to the client.

15. The transparent proxy (12) of claim 14, wherein the identifier and the data content are encrypted with the same cryptographic key.

16. The transparent proxy (12) of claim 15, wherein the proxy is operative to determine whether the client (10) is authorized to access the encrypted data content by verifying that the client has access to the cryptographic key used to encrypt the identifier and the data content.

17. The transparent proxy (12) of any one of claims 14-16, wherein the proxy is operative to determine whether the client (10) is authorized to access the encrypted data content by verifying that a client identifier received from the client matches a client identifier received from a server (11) providing the requested encrypted data content to the proxy.

18. A transparent proxy (12) in a communications network comprising: a processor (15) and a memory (16), said memory containing instructions executable by said processor, whereby said proxy is operative to:

receive from a client (10) an encrypted identifier indicating requested encrypted data content to be provided at the proxy;

determine whether the requested encrypted data content should be cached at the proxy;

send a request for the encrypted data content to a server (11) providing the encrypted data content;

associate the requested encrypted data content with the received encrypted identifier; and

cache the requested encrypted data content at the proxy.

19. The transparent proxy (12) of claim 18, wherein the proxy is operative to determine that the requested encrypted data content should be cached at the proxy if the number of requests for the encrypted data content exceeds a request threshold value.

20. The transparent proxy (12) of any one of claims 18 or 19, the proxy further being operative to:

remove the encrypted data content from the proxy if it has not been requested for a predetermined time period.

21. A computer program (17) comprising computer-executable instructions for causing a device (12) to perform the steps recited in any one of claims 1-13 when the computer-executable instructions are executed on a processor (15) included in the device.

22. A computer program product comprising a computer readable medium (16), the computer readable medium having the computer program (17) according to claim 21 embodied therein.

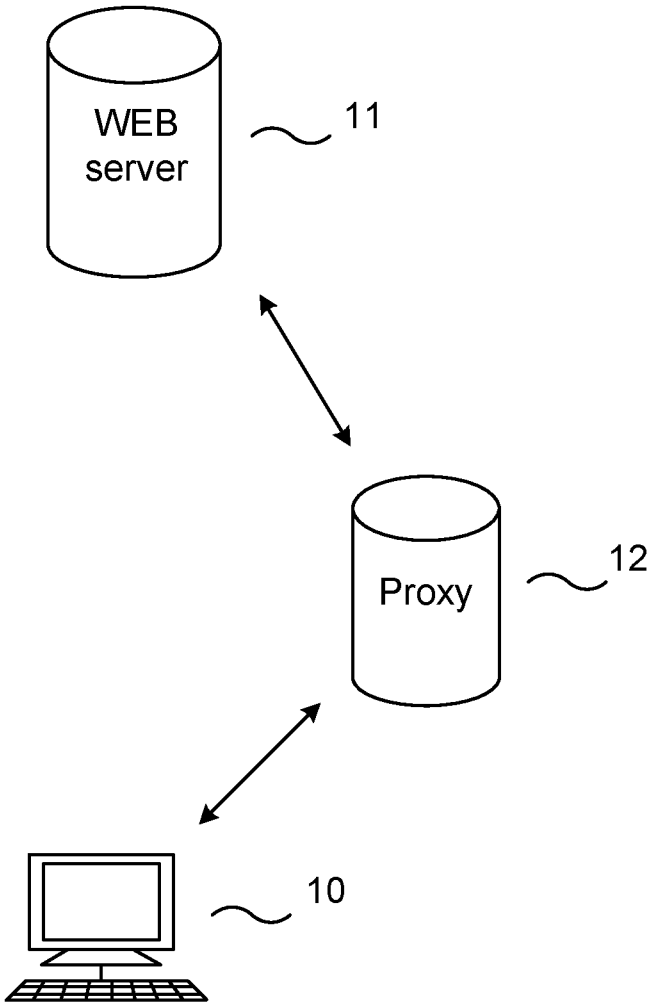

Fig. 1

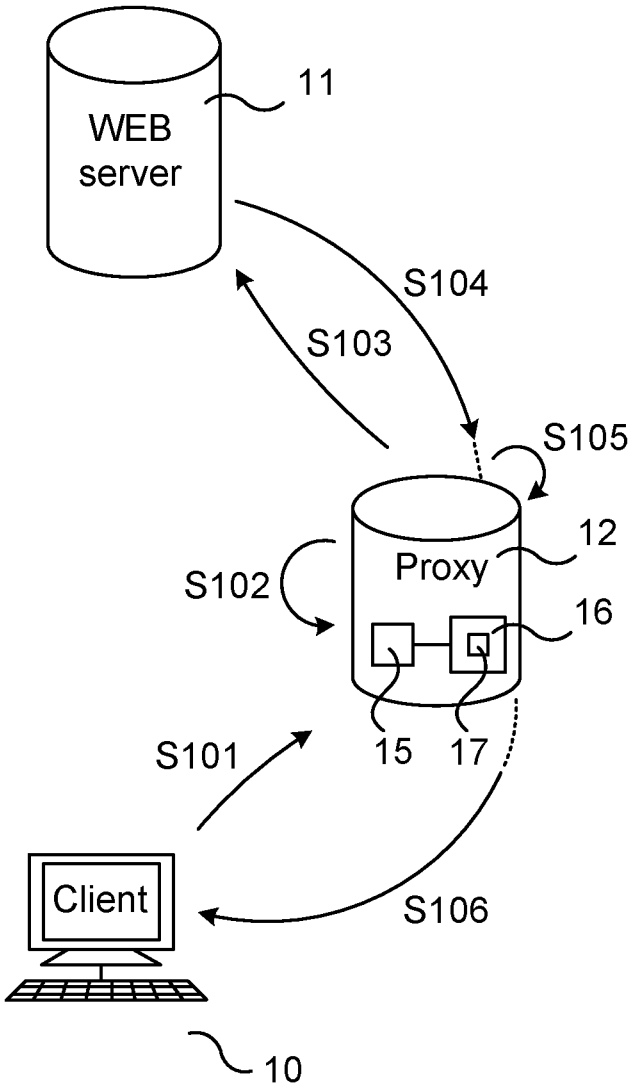
WEB
server
11
S104
S103
S105
12
Proxy
S102
16
15
17
S101
Client
S106
10

Fig. 2a

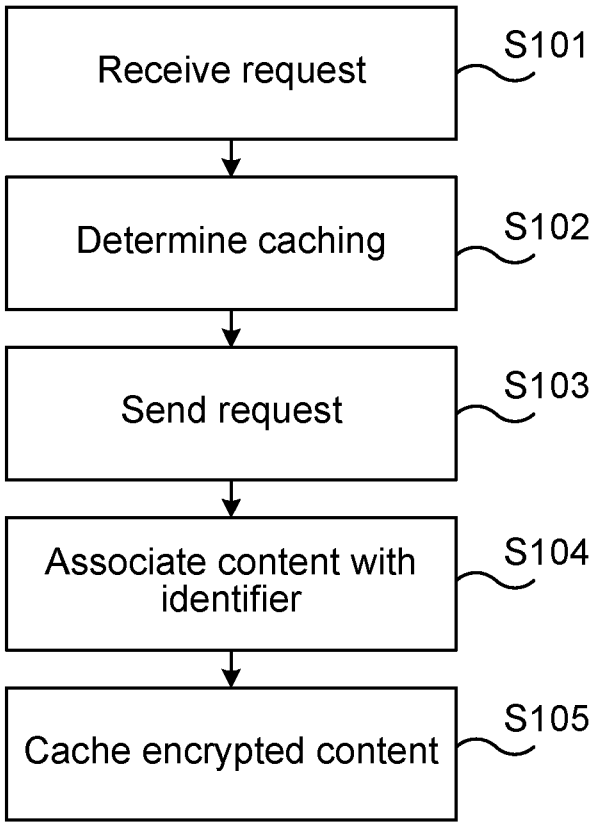
Receive request
S101
Determine caching
S102
Send request
S103
Associate content with identifier
S104
Cache encrypted content
S105

Fig. 2b

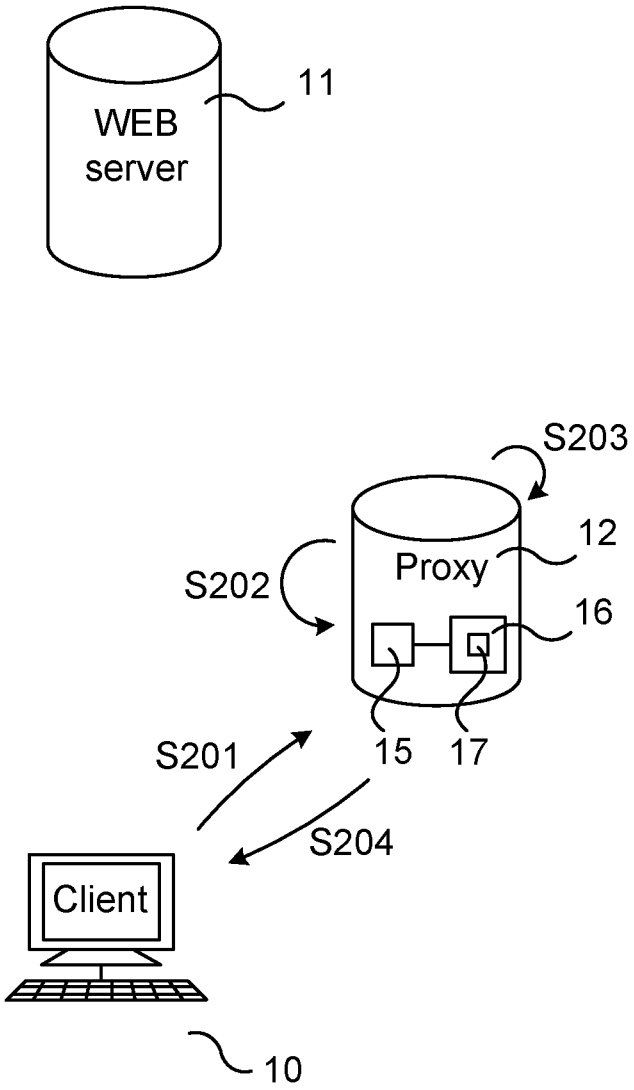

Fig. 3a

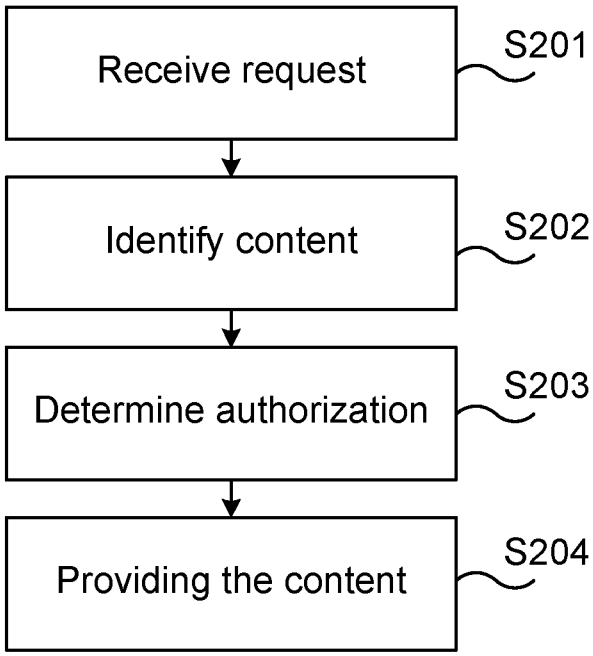
Receive request
S201
Identify content
S202
Determine authorization
S203
Providing the content
S204

Fig. 3b

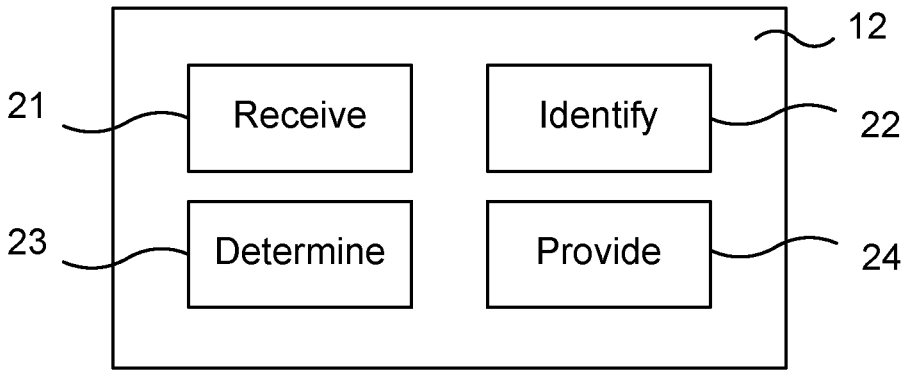
12
21
Receive
Identify
22
23
Determine
Provide
24

Fig. 4a

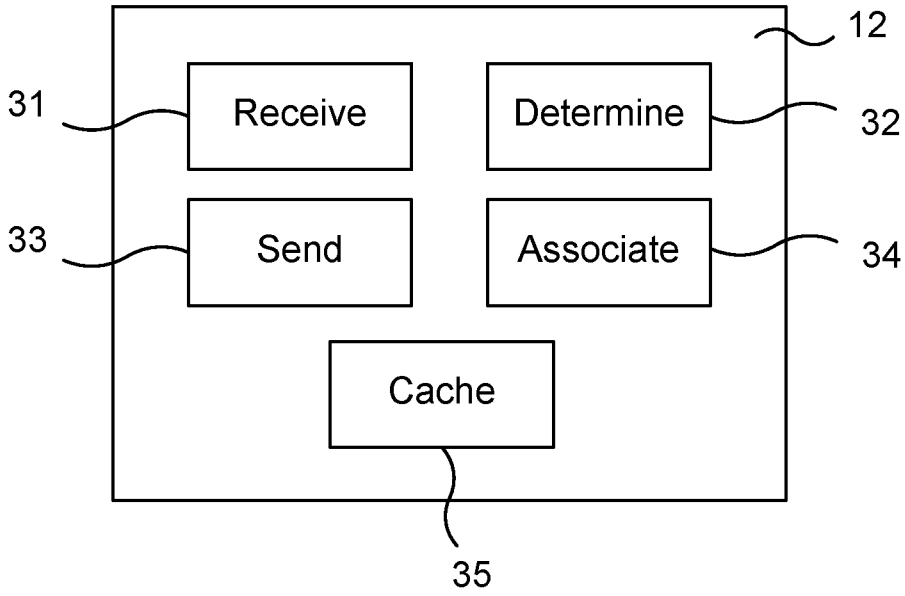
12
31
Receive
Determine
32
33
Send
Associate
34
Cache
35

Fig. 4b

INTERNATIONAL SEARCH REPORT

International application No
PCT/SE2014/050184

A. CLASSIFICATION OF SUBJECT MATTER

INV. G96F17/30 H04L29/08 HQ4L29/G6
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)
G06F H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, 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	US 2004/015725 A1 (BONEH DAN [US] ET AL) 22 January 2004 (2004-01-22) paragraph [0055] - paragraph [0056] ; figure 11	1-22
A	US 2013/046883 A1 (LIENTZ ANDREW [US] ET AL) 21 February 2013 (2013-02-21) paragraph [0089] - paragraph [0099]; figure 8	1-22

☐ 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 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
6 October 2014	14/10/2014

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	Raposo Pires, Joao

INTERNATIONAL SEARCH REPORT

Information on patent Tamlly members

International application No
PCT/SE2014/050184

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004015725 A1	22-01-2004	NONE	
US 2013046883 A1	21-02-2013	NONE	