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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 March 2014 (27.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/044641 A1

(51) International Patent Classification:
*H04L 29/08* (2006.01) *H04W 36/22* (2009.01)
*H04L 29/06* (2006.01) *H04W 88/06* (2009.01)
*H04W 28/08* (2009.01)

(21) International Application Number:
PCT/EP2013/069178

(22) International Filing Date:
16 September 2013 (16.09.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12306126.9 18 September 2012 (18.09.2012) EP

(71) Applicant: **THOMSON LICENSING** [FR/FR]; 1-5 rue Jeanne d'Arc, F-92130 Issy-les-Moulineaux (FR).

(72) Inventors: **LE SCOUARNEC, Nicolas**; c/o Technicolor R&D France, 975 avenue des Champs Blancs, CS17616, F-35576 Cesson-Sévigné (FR). **LE MERRER, Erwan**; c/o Technicolor R&D France, 975 avenue des Champs Blancs, CS17616, F-35576 Cesson-Sévigné (FR). **STRAUB, Gilles**; c/o Technicolor R&D France, 975 avenue des Champs Blancs, CS17616, F-35576 Cesson-Sévigné (FR).

(74) Agents: **HUCHET, Anne** et al.; 1-5 rue Jeanne d'Arc, F-92130 Issy-Les-Moulineaux (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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).

**Declarations under Rule 4.17**:

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

*[Continued on next page]*

(54) Title: METHOD AND DEVICE FOR SECURELY ACCESSING A WEB SERVICE

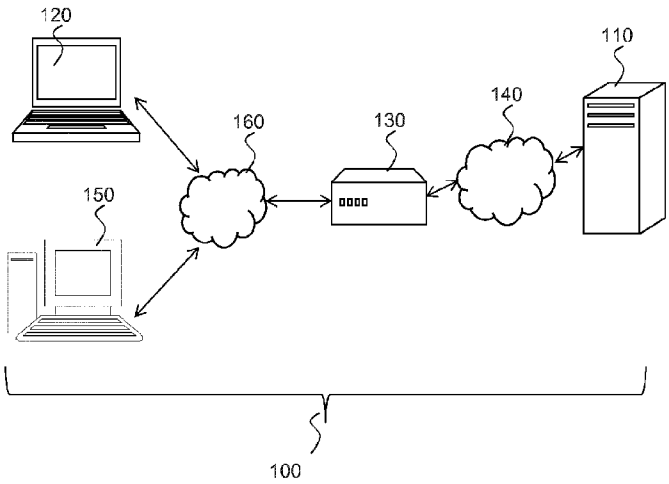


Figure 1

(57) Abstract: The invention relates to a method for securely accessing a web service by a browser running a web application on a user device through a network. The web service is hosted by at least a device among which a local device is being accessed by the user device. The local device comprises a global name that uniquely identifies the local device and a certificate associated to the global name. The method further comprises a step of sending by the web application to the network a request for accessing the web service by addressing a generic name that identifies any device hosting the web service; a step of receiving from the network by the web application a response to the request comprising the global name identifying the local device hosting the web service; a step of verifying by the web application that the received global name is comprised in a list; and when the verification is successful, a step of connecting to the local device by addressing the global name; a step of receiving the certificate from the local device; a step of verifying the certificate associated to the global name by the browser and a step of securely accessing the web service. A generic name is a name under which any local device is accessible, that is, is common to all devices hosting the web services. The list comprises global names of devices being trusted for hosting the web service.

WO 2014/044641 A1

**Published**:

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

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

# METHOD AND DEVICE FOR SECURELY ACCESSING A WEB SERVICE

## TECHNICAL FIELD

The present invention relates generally to the field of secure access to web service. More precisely, the invention relates to a method for securely accessing a web service by a browser running a web application on a user device through a network, wherein the web service is hosted by a local device.

## BACKGROUND

This section is intended to introduce the reader to various aspects of art, which may be related to various aspects of the present invention that are described and/or claimed below. This discussion is believed to be helpful in providing the reader with background information to facilitate a better understanding of the various aspects of the present invention. Accordingly, it should be understood that these statements are to be read in this light, and not as admissions of prior art.

Digital data (e.g., photos, videos) are increasingly produced and managed on mobiles devices (e.g., smartphones, tablets, laptops). This data is also often shared, backed up, or processed via Internet. Indeed, a wide range of "cloud" services handle users' content, be they photo processing services, social networks or online storage. Most of these cloud services rely entirely on web technologies. As a consequence, users need to upload large amounts of content over HTTP to web applications. However, the speed of uploads is limited by the available bandwidth. Indeed, the connectivity speed to the Internet remains limited due to the use of legacy infrastructures (xDSL), or of shared medium (Cellular).

The long upload times prevent users from standing by or powering off their stand-alone devices and require these users to keep their devices

connected to handle the transfer over the Internet. In order to alleviate these issues, a mechanism to offload uploads over HTTP to a third party device which is permanently connected to the network, such as residential gateway, is proposed. A method for locating the third party device offering the offloading web service is therefore proposed.

However, offloading a task to a third party requires to trust this third party, in other words the third party device hosting the offload service has to be authenticated by the user stand/alone device. Known solution for authenticating a device or a web service are based on certification by a trust authority. Certificates are either delivered by a trust authority to a trusted operator owning the web service or to user's physical device. However, these solutions are not compatible with the legacy software, such as web browser, and standard web protocols wherein the processing environment is limited. In others words, the browser is limited in term of inputs and outputs, for instance the browser cannot access to the storage media (such as hard disk drive) of the device on which it is executed, cannot access directly to the network.

A solution for securely accessing a web service by a browser running a web application on a user device through a network, wherein the web service is hosted by a local device is therefore required. The method should deliberately be simple to ease implementation and use, and compatible with legacy software, adapted to be implemented in JavaScript and to run in the browser..

The present invention provides such a solution.

## SUMMARY OF INVENTION

In a first aspect, the invention is directed to a method for securely accessing a web service by a browser running a web application on a user device through a network. The web service is hosted by at least a device among which a local device is being accessed by the user device Advantageously, the local device is the device which hosts the web service and

which is closest to the user device. The local device comprises a global name that uniquely identifies the local device and a certificate associated to the global name. the method further comprises a step of sending by the web application to the network a request for accessing the web service by addressing a generic name that identifies any device hosting the web service; a step of receiving from the network by the web application a response to the request comprising said global name identifying the local device hosting the web service; a step of verifying by the web application that the received global name is comprised in a list; and when the verification is successful, a step of connecting to the local device by addressing the global name; a step of receiving the certificate from the local device; a step of verifying the certificate associated to the global name by the browser and a step of securely accessing the web service. Advantageously a generic name is a name under which any local device is accessible, that is, is common to all devices hosting the web services. Advantageously the list, also called white list, comprises global names of devices being trusted for hosting the web service. Advantageously, the list does not comprises an exhaustive list of global names of local devices being trusted for hosting the web service, since the number of global names could be huge, but patterns for matching global names of local devices.

According to an advantageous characteristic the local device is delivered a global name and a certificate associated to the global name by a trusted operator.

According to another advantageous characteristic, the white list is dynamically obtained from a trusted operator by the web application running in the browser. In a variant, the white list is hard coded in the web application running in the browser.

In a first preferred embodiment, the request for accessing the web service by addressing a generic name is a HTTP request and a request for securely accessing the web service by addressing the global name is a HTTPS request including a SSL request.

According to variant the local device is a gateway device, a set top box, a Network Attached Storage (a NAS).

In a second aspect, the invention is directed to a user device for securely accessing a web service by a browser running a web application through a network. The web service is hosted by at least a device among which a local device is being accessed by the user device. Advantageously, the local device is the device which hosts the web service and which is closest to the user device. The device comprises means for sending by the web application to the network a request for accessing the web service by addressing a generic name that identifies any devices hosting the web service; means for receiving from the network by the web application a response to the request comprising a global name uniquely identifying the local device hosting the web service; means for verifying by the web application that the received global name is comprised in a list, also called white list, wherein the list comprises global names of local devices being trusted for hosting the web service; and means for connecting by the web application to the local device by addressing the global name; means for receiving a certificate from the local device and means for verifying the certificate associated to the global name and means for securely accessing the web service.

Any characteristic or embodiment described for the method for securely accessing a web service through a network by a browser running a web application on a user device, wherein the web service is hosted by a local device is compatible with the user device or the local device adapted to implement the disclosed method.

The method according to a first embodiment is advantageously compatible with current software and standard web protocols. Hence, it can be deployed without requiring changes to the users' browsers or to the protocols used.

## BRIEF DESCRIPTION OF DRAWINGS

Preferred features of the present invention will now be described, by way of non-limiting example, with reference to the accompanying drawings, in which:

**Figure 1** illustrates an exemplary network in which the present invention may be used;

**Figure 2** illustrates the steps of the secure access method according to a first embodiment of the present invention;

**Figure 3** illustrates the steps of the secure access method according to a preferred embodiment of the present invention; and

**Figure 4** illustrates a local device implementing the secure access method according to a preferred embodiment of the present invention.

## DESCRIPTION OF EMBODIMENTS

**Figure 1** illustrates an exemplary network 100 in which the present invention may be used. The network 100 comprises a server device 110 hosting a web application, such as a photo sharing application. A user owns personal devices 120, such as battery powered devices (tablet, laptop computer, mobile phone) or computers, on which a web browser is available. The client part of a web application, for instance a photo sharing application, is executed on the browser of a user device 120 and the web application accesses the server part of the web application. The client part of the web application can also access the web service, such as an offloading service. The user device connects to the web service running on a local device such as an Internet router, a set top box, another user computer, a residential gateway, a NAS 150 by the local area network 160. The client part of the web application, and the web service can access the server part of the web application through a network access device 130 such as a wireless Internet router or residential gateway. Thus the residential gateway is at the frontier between a fast local area network 160 and

a relatively slow broadband network 140 wherein the access to the slow broadband network is an issue for uploading data to the server part of the web application. In a preferred embodiment, the network access device 130 is the local device since a network access device is always powered-up. In a variant, wherein for instance such network access device 130 does not support the offloading function, the local device is any type of device of the local network 140 preferably of type always-on as above detailed, for instance a NAS 150. The invention provides a solution for authenticating the local device 130, 150 or more precisely the web service running on the local device 130, 150 so that the uploaded data temporarily transiting in the local device are protected from attackers by avoiding attackers to impersonate the local device.

A salient inventive idea of the present invention is to locate, from the browser, a local web service to be used within a web application, and to authenticate the local service. The method can be used to locate an offloading service, but it advantageously compatible with other application such as locating a Web to DLNA/UPNP relay wherein a web application is authorized to control through a web service to DLNA/UPNP relay, users' devices.

In a preferred embodiment, the method is adapted to be executed by JavaScript language. Hence the method is advantageously adapted to fit into the constrained execution environment offered by the web browser. These constraints help the browser to ensure that any malicious code has a very limited power.

Besides, the method for securely accessing the web service dynamically determines both the existence of the service, and its address. The mechanism also takes care of authenticating re-located service. The mechanism also allows to implement dynamic adaptation of the client part of the web application depending on the existence of the service.

**Figure 2** illustrates the steps of the secure accessing method according to a first embodiment of the present invention.

The browser can only access the network using XMLHttpReq implemented in a so-called browser network API. The browser further comprises a JavaScript machine. The authentication/certification mechanism present in the browser is the TLS/SSL mechanism.

In a preliminary step, not represented on figure 2, a trusted operator buys a domain (offload.org) and request for a SSL certificate for that domain. Each trusted devices running the service receives a unique name (for instance af34a), and a certificate (af34a.offload.org) corresponding to its name. The trusted operator runs a DNS service (available on the Internet), which trusted devices are able to update, so that the name af34a.offload.org always map to the right local IP address.

In a first step 210 of the location/authentication procedure, the browser trying to access a locally hosted web service sends a request to a generic name (offload.local) to the network. More precisely, the JavaScript issues, through the browser network API, a local query to some fixed address (offload.local) common to any device running the service on any local network. The DNS present in gateway will reply to the DNS query with a local IP address and the browser network API connects to this IP address, i.e; the IP address of the local device hosting the web service, using unsecure HTTP protocol. The issue consists in that it wouldn't be possible to get a certificate for "offload.local" since this name belongs to nobody, and no certification authority will deliver such a certificate.

Thus, in a second step 220 the browser obtains a fully qualified name (af34a.offload.org), called global name, for web service hosted by the local device and associated to the local device IP address. However, as already explained, the fully qualified name may be corrupted.

In a third step 230, the browser checks that the obtained global name (af34a.offload.org) is managed by some trusted operator. Indeed, while someone may have a valid certificate for hacker.org, this is not a sufficient condition. A further requirement is that the owner of the certificate is trusted.

Hence, the browser verifies the obtained global name against a white list, to be sure that the sub-certificate (af34a.offload.org) comes from a trusted operator (offload.org). The skill in the art will appreciate that the white list may not comprise an exhaustive list of the global name of each trusted devices but a pattern matching scheme used to verify the global name.

In a last step 240, when the verification succeeds, the browser sends a request for securely accessing the global name. More precisely, the browser network API performs a new query to the fully qualified name (af34a.offload.org). The DNS operated by the trusted operator answers with the local IP address. The browser connects in HTTPS to this local IP address and checks that the certificate associated to the global name corresponds to the device it connects to and that the certificate is valid and has not been revoked using the certificate collection of the browser. The step 240 advantageously allows that the local device is authenticated, and the step 230 advantageously allows that the local device was approved by the trusted operator.

Hence, the web service available at https://af34a.offload.org is safely and securely used.

Any failure at any step means that the service is either not available or that it cannot be trusted because of some authentication issues. Hence, it should not be used.

**Figure 3** illustrates the steps of the secure accessing according to a preferred embodiment of the present invention. As already explained, in the preferred embodiment the web service is a web service for offloading uploads .

The location service is available at a fixed URL http://offload.local/test. For the sake of clarity, we omit the port number in the whole description. However, in order to avoid conflicts with existing services, we use non-standard HTTP/HTTPS ports (e.g., 8787 for HTTP and 8788 for HTTPS). The fully qualified name and the port are fixed and common to all gateways. As a consequence, the web application running in the browser, which can access the network only using XMLHttpRequest, can access the service. The browser resolves the generic fully qualified name (offload.local 300) to the IP address of

the gateway and connects to it. Any connection error (failed DNS resolution, connection timeout, 404, 403. . . ) indicates that the service is not available. If the offloading service is running and can accept offload requests, the browser will receive OK as an answer.

The location service relies heavily on the DNS to resolve a fixed name to the IP address of the device supporting the service on the LAN. Most gateways run their own DNS server, and can hence register as offload.local on their own. If offloading service is offered by another device, this device can still register the name offload.local in the DNS of the gateway thanks to the DHCP protocol. Since the DNS resolution may be easily affected by anyone on the same LAN registering for offload.local using DHCP, the web developer may be willing to ensure that the resolution leads to a trusted (according to the browser's SSL certificates) gateway. The solution is to rely on the HTTPS authentication mechanism. To this end, each gateway has its own self-signed certificate, and the user manually adds certificates from gateways he trusts to his browser's certificate list. Requests are sent to https://offload.local/ instead of http://offload.local/. If the gateway is not trusted, requests to the location service will result in connection errors. Hence, the offloading won't be enabled. However, this process requires the user to manually approve each new gateways he uses by adding the appropriate certificate in his browser. This process may be tricky and inhibit a fully transparent user's experience.

To make the process seamless, the method according to a preferred embodiment, advantageously provides an enhanced location method that also takes care of authenticating the gateway. The method is meant to be used with embedded devices running trusted software and whose certificate cannot be copied. **Figure 3** illustrates the whole location and authentication process. This process enhances the non-authenticated location service described here before. In this case, each gateway is associated with a unique name (for instance af34a.offload.org 301), and has the corresponding certificate signed by

a trusted authentication authority. Each gateway publishes its local IP address onto a dynamic DNS service running for the trusted domain offload.org.

The process now consists in locating the gateway and then authenticating it. To this end, a request to http://offload.local/auth is issued. This request returns the unique fully qualified name (e.g., af34a.offload.org 301) for the gateway. This fully qualified name is matched with a white-list of domains to ensure that the certificate has been issued by a proper authentication authority: not all valid SSL domain (i.e., approved according to the browser certificate list) map to trusted gateways. Only a few domains (e.g., offload.org) are trusted for this purpose and as such are listed in the white-list. Up to this point, the gateway is not trusted and information obtained may have been manipulated. However, the fully qualified name maps to a trusted set of gateways. Next, a request to https://af34a.offload.org/test is issued. The browser checks the certificate of the gateway thus preventing any hijacking. If the certificate is legitimate, the offloading mechanism can be enabled and requests can be posted to https://af34a.offload.org/upload/.

Again, as in the basic location process, any error means that the offloading mechanism cannot be enabled. Since each device has its own certificate, it is possible to revoke individual certificates in case they are stolen, or in case a security issue is discovered on a subset of devices. At most, if an attacker succeeds in disrupting the location service by tampering with DNS entries, the web application will simply fall back onto the regular service without offloading capability, thus resulting in a no service disruption for the user apart from offloading being inactive.

The skilled person will also appreciate that as the method can be implemented quite easily without the need for special equipment, it may be implemented by 'normal' user devices such as PCs, mobile phones, gateways in home networks and so on. The invention is further compatible with 802.11 communication (Wi-Fi), or any wire or wireless access such as Bluetooth or UWB. The invention is advantageously compatible with a web service located on a hotspot of a wireless network.

**Figure 4** illustrates an exemplary user device according to a preferred embodiment of the present invention. The user device 400 comprises a software module called browser or web browser. The browser runs a web application trying to securely access a web service through the network. According to different variants, the user device may be implemented in a computer, a mobile device, a tablet.

The user device 400 comprises a network interface 410, such as a 802.11 wireless card, at least one processor 420 (hereinafter "processor") and memory 430. The network interface 410 is adapted to connect the user device to the network, and thus to connect the user device to the local device. The network interface 410 for instance physically transmits requests for accessing a remote web service and physically receives response to the request. In a variant, the network interface 410 is a wired interface such as Ethernet. The processor 420 is adapted to execute instructions implementing the software module called web browser. The web browser is adapted to run a web application. Only the features necessary for the comprehension of the invention are detailed hereafter. The web application sends request through the network interface 410 for accessing a web service by addressing a generic name that identifies any device hosting the web service. The web application receives, through the network interface 410, a response to the request comprising a global name that uniquely identifying a local device hosting the web service and which the user device can securely access. The web application verifies that the received global name is comprised in a list comprising global names of devices being trusted for hosting the web service. Advantageously the list is stored in memory 430. The web application establishes a connection, through the network interface 410, to the local device by addressing the global name and the browser verifies the received certificate associated to the global name of the local device. Thus the web application securely accesses the web service. In a variant, the secure functions are implemented in a piece of hardware, such as a secure processor.

The description is focussed on upload to web application however the invention is compatible with mechanisms wherein a web service is locally served.

Each feature disclosed in the description and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination. Features described as being implemented in software may also be implemented in hardware, and vice versa. Reference numerals appearing in the claims are by way of illustration only and shall have no limiting effect on the scope of the claims.

## CLAIMS

1. Method for securely accessing a web service by a browser running a web application on a user device (120) through a network (160), wherein said web service is hosted by at least a device among which a local device (150, 130) is being accessed by the user device, the method being characterised in that said local device (150, 130) comprises a global name (301) that uniquely identifies said local device and a certificate associated to said global name; the method further comprising:
    - Sending by the web application to the network (160) a request for accessing said web service by addressing a generic name (300) that identifies any device hosting said web service;
    - Receiving from the network (160) by the web application a response to said request, said response comprising said global name (301) identifying said local device (130, 150) hosting said web service;
    - Verifying by the web application that said received global name is comprised in a list;
    - And when the verification is successful, connecting to said local device (150, 130) by addressing said global name (301); receiving said certificate from said local device; verifying said certificate associated to said global name by the browser and securely accessing said web service.

2. Method according to claim 1 wherein said list comprises global names of devices being trusted for hosting said web service.

3. Method according to claim 1 or 2 wherein the local device is delivered said global name and said certificate associated to said global name by a trusted operator.

4. Method according to claim 3, wherein said list is dynamically obtained from said trusted operator by said web application running in the browser.

5. Method according to claim 3, wherein said list is hard coded in said web application running in the browser.

6. Method according to any of claims 1 to 5 wherein connecting to said local device (150, 130) by addressing said global name (301) further comprises sending to an external network (140) a second request for accessing said web service by addressing a global name (301); receiving from the network (140) a response to said second request, said response comprising a local IP address of the local device (130, 150).

7. Method according to claim 6 further comprising a preliminary step of publishing the local IP address of the local device associated the global name on a trusted operator.

8. Method according to claim 6 or 7 wherein a mapping between the local IP address of the local device and the global name is maintained by a DNS service run by said trusted operator.

9. Method according to any of claims 1 to 8, wherein said request for accessing said web service by addressing a generic name is a HTTP request.

10. Method according to any of claims 1 to 9, wherein a request for securely accessing the web service by addressing said global name is a HTTPS request.

11. Method according to any of claims 1 to 10 wherein the local device is a gateway.

12. A user device (120, 400) for securely accessing a web service by a browser running a web application through a network, wherein said web service is hosted by a at least a device among which a local device is being accessed by the user device, the device comprising:

- means for sending by the web application to the network a request for accessing said web service by addressing a generic name that identifies any device hosting said web service;
- means for receiving from the network by the web application a response to said request comprising a global name uniquely identifying said local device hosting said web service;
- means for verifying by the web application that said received global name is comprised in a list, wherein said list comprises global names of devices being trusted for hosting said web service;
- means for connecting by the web application to said local device by addressing said global name, means for receiving a certificate received from said local device and means for verifying said certificate associated to said global name by the browser and means for securely accessing said web service.

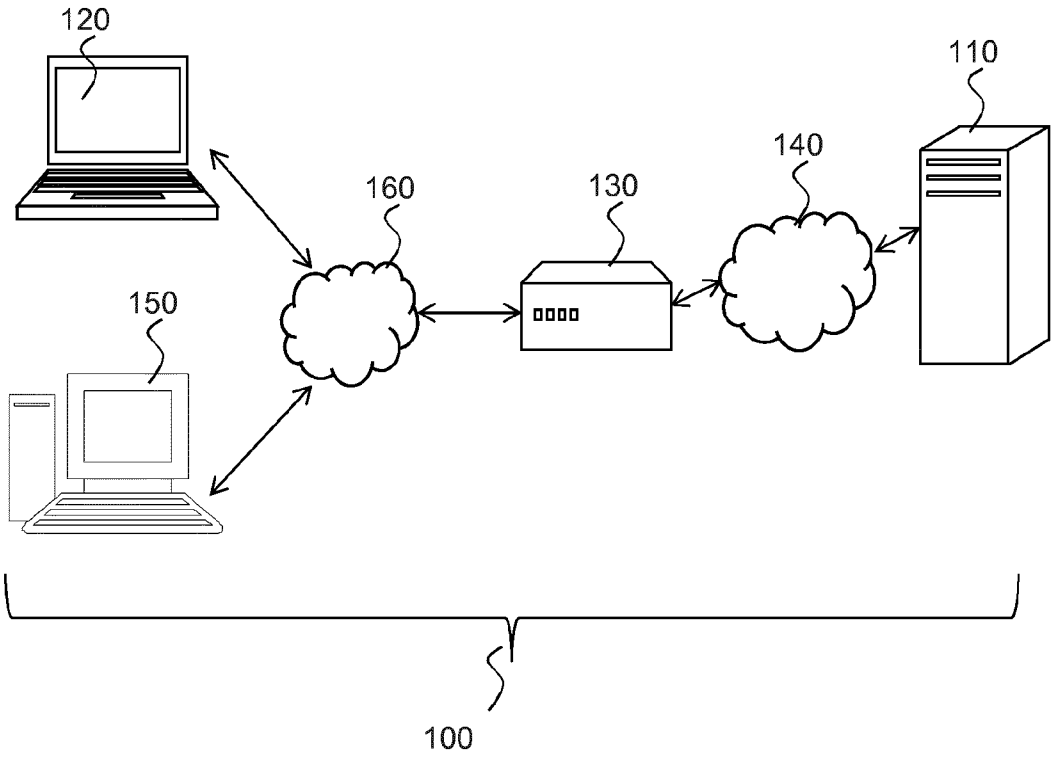


Figure 1

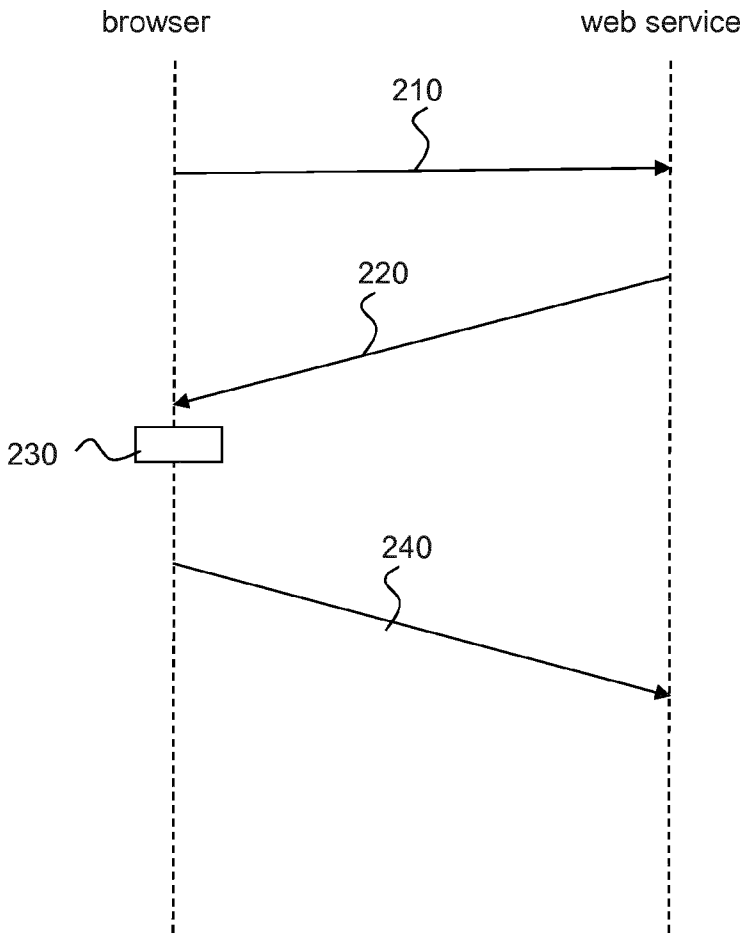


Figure 2

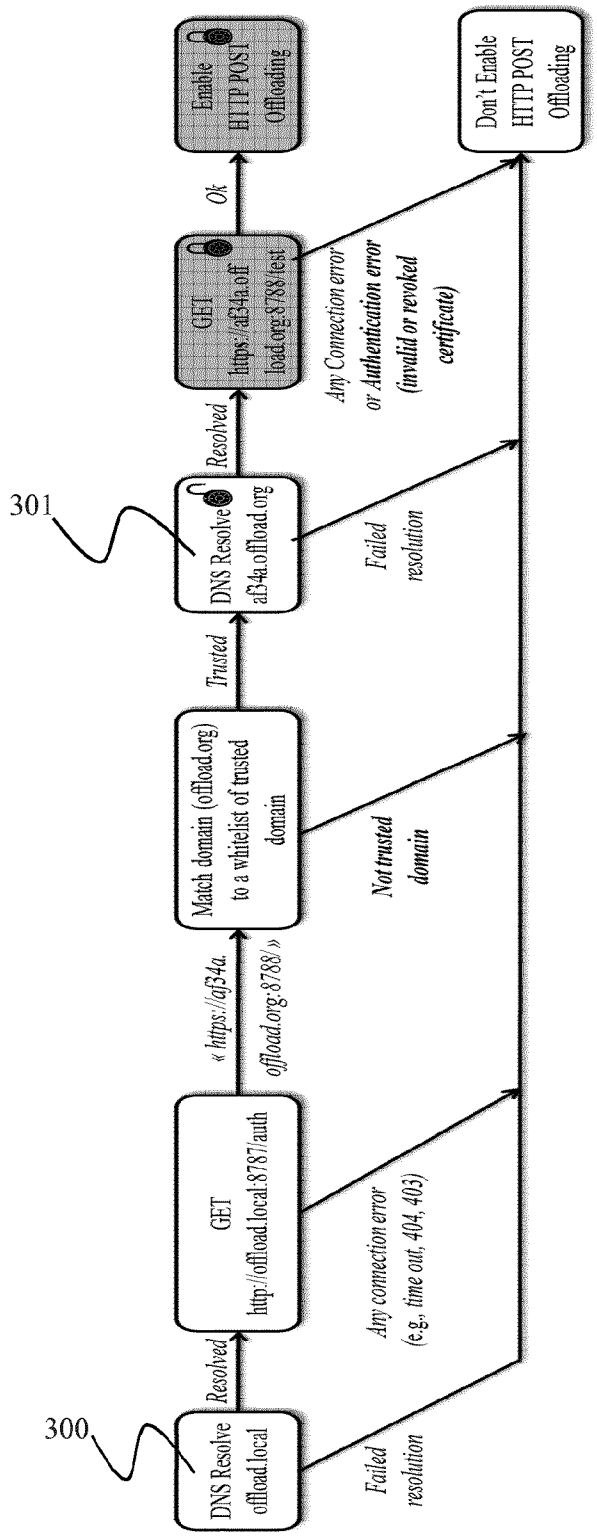
Enable HTTP POST Offloading
Ok
GET https://af34a.offload.org:8788/test
Resolved
DNS Resolve af34a.offload.org
Trusted
Match domain (offload.org) to a whitelist of trusted domain
« https://af34a.offload.org:8788/ »
GET http://offload.local:8787/auth
Resolved
DNS Resolve offload.local
Don't Enable HTTP POST Offloading
Any Connection error or Authentication error (invalid or revoked certificate)
Failed resolution
Not trusted domain
Any connection error (e.g., time out, 404, 403)
Failed resolution
301
300

Figure 3

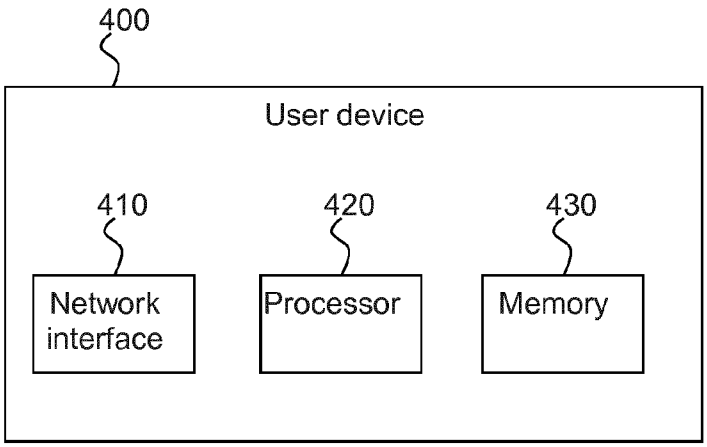
400
User device
410
420
430
Network interface
Processor
Memory

Figure 4

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/069178

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08 H04L29/06 H04W28/08 H04W36/22
ADD. H04W88/06

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

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 2011/098660 A1 (NOTAVA OY [FI]; LAPPETELAEINEN ANTTI [FI]; TUUPOLA JUHA-MATTI [FI]; ER) 18 August 2011 (2011-08-18) paragraph [0004] page 6, line 20 - line 23 page 7, line 8 - line 18 page 8, line 43 - line 46 page 11, line 36 - line 41 figures 2,7 ----- | 1-12 |
| A | US 7 181 506 B1 (VIGUE CHARLES L [US] ET AL) 20 February 2007 (2007-02-20) column 2, line 24 - line 39 page 11, lines 9-19,42-62 figures 1,9 ----- | 1-12 |

☐ 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 |
|---|---|
| 14 January 2014 | 06/02/2014 |

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

1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/069178

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 2011098660 A1 | 18-08-2011 | CN 102783218 A | 14-11-2012 |
| | | EP 2534889 A1 | 19-12-2012 |
| | | US 2013042316 A1 | 14-02-2013 |
| | | WO 2011098660 A1 | 18-08-2011 |
| US 7181506 B1 | 20-02-2007 | NONE | |