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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 April 2020 (16.04.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/074401 A1

(51) International Patent Classification:
*H04L 29/06* (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/EP2019/076982

(22) International Filing Date:
04 October 2019 (04.10.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/744,310 11 October 2018 (11.10.2018) US

(71) Applicant: **DIGITAL TANGIBLE, S.L.** [ES/ES]; C/ GIRONA 130, PPAL 2ª, 08037 BARCELONA (ES).

(72) Inventor: **EFFING, Simon**; GLEIMSTR. 17, 10437 BERLIN (DE).

(74) Agent: **ESPIELL GÓMEZ, Ignacio**; C/ PAU CLARIS Nº 77, 1º 2ª, 08010 BARCELONA (ES).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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,

WO 2020/074401 A1

(54) Title: WEB ACCESS CONTROL METHOD

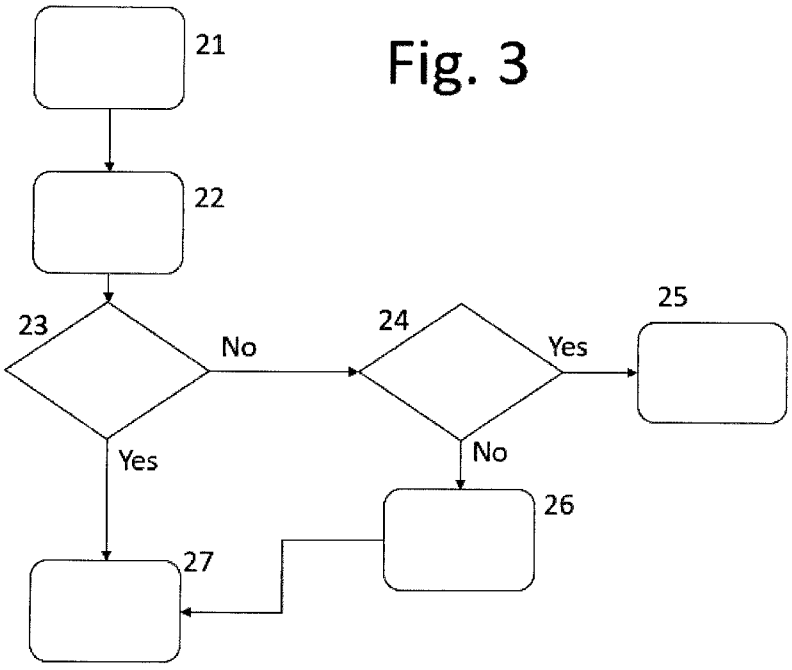



Fig. 3

(57) Abstract: A method for web access control that comprises the following steps: - creating a content item (1) in a content management system; - generating a series of unique secure random access tokens (2) and storing them in a database (3); - generating a file containing the ATs with their corresponding direct link URLs - when a client device accesses the content using a browser (11), checking with the server if the request's BID is already registered for this AT; o if it is already registered, allowing access to the content; o if not, checking if a preset limit of allowed registered BIDs for the AT has been reached; # if the limit has been reached, denying access to the content; # if not, registering the new BID with the AT and allowing access to the content.

[Continued on next page]

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 the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**Published:**

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

# DESCRIPTION

## WEB ACCESS CONTROL METHOD

### Object of the invention

The invention, as stated in the title of the present specification, relates to a method for accessing content placed in a content management system, e.g. a web, that ensures that the content is accessed by the allowed number of users without requiring the introduction and sharing of passwords, nor the supervision of an administrator of the web.

For instance, it can be used to allow any number of users to download, stream o play an audio guide to a museum, to obtain extra content when buying tickets to a concert, etc. Those users will keep their identity and personal data private and will not share it.

### Background of the invention

Several ways to protect a web-app to be freely accessed have been developed. The most common system is a registration with an email-address and a password followed by logins every time the user wants to access the same content again. Sometimes digital content and data hosted on a website get an additional protection against password-theft by the so-called two-factor-authentication, that adds an additional token to the login process via a code received on the mobile phone-number of the user or a Time-based One-time Password Algorithm (TOTP). Sometimes the registration makes sure that the person seeking access is human and not a bot by adding a so-called "captcha", that consists of a small action that theoretically con not be fulfilled by a robot to demonstrate that the person seeking access is human.

This kind of content protection serves mostly two purposes: privacy, since they prevent certain data from being publicly accessible against the will of the owner, security, making sure that no bot and no illegitimate user gets access, but also the protection of intellectual property. Some digital newspapers, for instance, require a registration and a login system to prevent nonsubscribers to read a content that should only be made accessible to subscribers.

This system (password-login, sometimes with a two-factor authentication and a captcha) are

the common state-of-the art and provide an acceptable grade of security, but at the cost of requiring personal data from the user (like an email-address) and of the trouble generated by having to find a way to memorize or to store securely several passwords and losing time solving captchas. Although this trouble and privacy issues are accepted by the user when its purpose is to secure his own content, like bank-accounts or private information contained in social networks, it is often upsetting when its only purpose is to generate an artificial barrier to prevent non-authorized people to access intellectually protected content.

Traditional registration and login systems are annoying, slow down the access to the digital content on a protected web-app and violate privacy by requiring giving away personal data like name and/or email and/or a mobile phone-number.

It is known from US7950065 a method and a system to control access to content stored on a web server. It creates an encrypted link. When the authorized user accesses the content with the link, the client system is registered so the content is only shown to this system.

Thus, the need arises to find a simpler and more immediate way to protect access to content and to limit to a minimum the invasion of the user's privacy, like is provided by the light-weight web access control, subject of this invention.

On the other hand, and as a reference to the current state of the art, it should be noted that, as far as the applicant is concerned, they are not aware of the existence of any other application having the same or similar technical characteristics to those claimed herein.

**Description of the invention**

The following is intended to be a brief summary of the invention and is not intended to limit the scope of the invention.

The light-weight method for web access control (LWAC) of the invention uses a combination of unique secure random access-tokens or codes (AT) and a browser ID (BID). The ATs may be printed on a physical surface (e.g. plastic or cardboard card) so they have to be entered into a web form. Additionally, a direct link including the AT may be encoded in a QR code that would be also printed on a physical surface. The BID is a secure unique random generated on the fly when a browser accesses the web-app for the first time and is stored in a cookie. Each AT allows only a limited number of BIDs. An optional email-opt-in can allow

additional access.

The combination of the three mentioned elements allows a fast and convenient access to a protected content without compromising the privacy or convenience of the user.

The Light-Weight Web Access Control (LWAC) method allows any user a fast, anonymous, direct and secure access to a web-app without having to register, to login or to give away personal data. The user can access the content as often as desired by entering or scanning again the access token (AT) that has been printed on a physical surface, like a card or brochure, that the user can keep and reuse an indefinite number of times. But thanks to the unique access tokens (AT) and the browser ID (BID) registration, the access cannot be transferred and therefore keeps its commercial value.

Description of the benefits of this invention to its users:

By protecting digital content on a web-app with a light-weight method of web access control, museums or tour-operators could allow a controlled access to a digital audio guide by keeping their commercial value and being able to sell them; newspapers could tie their subscriptions to a device and avoid the piracy produced by misusing the subscriptor's login-data; publishers could sell ebooks, audiobooks or other digital publications on a physical way in brick-and-mortar stores; musicians could use this method to protect their music and to sell it in concerts by printing the access tokens (AT) on a physical surface without having to use expensive and environmentally unfriendly CDs.

By using the light-weight web access control (LWAC) method to access digital content on a web-app, users could free themselves from the hassle and privacy-concerns of entering personal data on a registration; they could have a much faster and immediate access to the digital content on a web-app; they could access the content several times by keeping the physical surface, like a plastic or cardboard card or a brochure, where the access token (AT) have been printed.

The light-weight method for web access control comprises the use of a combination of a unique secure random access-token (AT) and a browser ID (BID) using the following steps:

- First it creates a content item, or more, in a content management system.
- Then it generates a series of unique secure random access tokens and stores them in a database.

- It also generates a file with the appropriate format (e.g. CSV) which comprises the serial number, the ATs and a direct link URL (including the AT) to the content.
- As such, when a client device accesses the content with the direct link URL using a browser, the server checks if the request's BID is already registered for this AT.
    - If the request's BID is already registered, it allows access to the content.
    - If the request's BID is no registered, then the server checks whether a preset limit of allowed registered BIDs for the AT has been reached. If not, the request's BID is registered and the access to the content is granted. If the preset limit has already been reached, access is denied although an opt-in procedure may be initialized.

The code for direct access may be printed on a physical medium, e.g. using a QR code or similar.

In a preferred embodiment, the server checks the browser accessing the web-app for the content for a browser ID (BID) cookie before checking with the server if the request's BID is already registered for this AT. If the cookie does not exist, a new secure unique random number is generated and set as the BID cookie. The BIDs may be cryptographically signed by the server to prevent spoofing. This new secure unique random number might get registered with the requested AT later in the database. Alternatively, for some type of requests (e.g. a non-initial request), if the cookie does not exist, access is denied.

The opt-in procedure allows access to the content from other devices or to regain access after cookies have been deleted.

In a preferred embodiment, the BID registrations are marked with a timestamp and have a limited lifetime. This lifetime may be preset or correspond to the time of an upgrade to the content.

The invention also refers to a server configured to evaluate a request of a client device for access to created content characterized in that it uses a combination of a unique secure random access-token (AT) and a client-device browser ID (BID). The server checks if the request's BID is already registered for this AT:

- If it is already registered, allowing access to the content.
- If it is not already registered, checking if a preset limit of allowed registered BIDs for the AT has been reached;

- If the limit has been reached, denying access to the content;
- If the limit has not been reached, register the new BID with the AT and allowing access to the content.

The system configured to carry out the method comprises a Web application configured to manage browser IDs (BIDs) by means of cookies and register these BIDs with access tokens (ATs), so that each AT can be used only by a limited number of BIDs.

The codes can be printed on a physical surface or medium, like a plastic or cardboard card or a brochure. It includes at least a QR code, or an alphanumeric code that allows such access, on at least one of its faces.

**Description of the drawings**

As a complement to the description provided herein, and for the purpose of helping to make the characteristics of the invention more readily understandable, the present specification is accompanied by a set of drawings constituting an integral part of the same, which, by way of illustration and not limitation, represent the following:

Figure 1: Shows the steps of creation of access tokens according to one embodiment.
Figure 2: Shows how to assign a browser ID to the content according to one embodiment.
Figure 3: Direct access with browser ID registration according to one embodiment.
Figure 4: First steps of an email-opt-in or fallback according to one embodiment.
Figure 5: Last steps of an email token fallback according to one embodiment.

**Preferred embodiment of the invention**

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the term "and/or" includes any and all combinations of one or more of the associated listed items. As used herein, the singular forms "a," "an," and "the" are intended to include the plural forms as well as the singular forms, unless the context clearly indicates otherwise.

It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features,

steps, operations, elements, components, and/or groups thereof.

Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one having ordinary skill in the art to which this invention belongs. It will be further understood that terms, such as those defined in commonly used dictionaries, should be interpreted as having a meaning that is consistent with their meaning in the context of the relevant art and the present disclosure and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein.

In describing the invention, it will be understood that a number of techniques and steps are disclosed. Each of these has individual benefit and each can also be used in conjunction with one or more, or in some cases all, of the other disclosed techniques. Accordingly, for the sake of clarity, this description will refrain from repeating every possible combination of the individual steps in an unnecessary fashion.

Nevertheless, the specification and claims should be read with the understanding that such combinations are entirely within the scope of the invention and the claims. The present disclosure is to be considered as an exemplification of the invention. It is not intended to limit the invention to the specific embodiments illustrated by the figures or description below.

The present invention will now be described by referencing the appended figures representing preferred embodiments.

The method starts with the steps shown in Figure 1. After creating a content item (1) in a CMS or content management system, a series of unique secure random access tokens (AT) are generated (2). These ATs are stored in a database (3) which keeps track of each AT's usage. The ATs can be downloaded (4) in CSV format which contains the serial number, the AT in alphanumeric format and a direct link URL to the web-app that includes the AT. These URLs allow the generation of Quick-response (QR) codes for convenient direct access or another similar readable format. Alternatively, the AT can be entered in a web-app form. The ATs and QR codes can be either provided digitally or printed on a physical surface like a card or brochure (5).

The next steps are shown in figure 2. Each browser (11) accessing the web-app for the content is checked by the server for a browser ID (BID) cookie (12). If none exists, a new secure unique random number is generated (15) and set as the BID cookie. In either case,

the request (22) for content is passed on for further processing (16). Optionally some requests (22) might require a previously existing cookie (13) and result in a rejection (14) of the request if none exists.

In figure 3 it is shown the steps as the user ask for the content (21) by scanning de QR, entering the AT in the webform or similar procedures. The web-app receives the request (22) to the content. It is then checked (23) whether the request's BID is already registered with the AT or not. If it does, access to the content is granted (27). Otherwise the systems checks if the limit of allowed registered BIDs for this AT is reached in a confirmation step (24):

If the limit has not been reached, an additional BID is registered with the AT (26) and access to the content is granted (27).

If the limit has been reached, access is denied and it results in a rejection (14). The user might be offered an email-opt-in-fallback (25). The number of BIDs allowed may be one, several... and will usually be defined when creating the content or setting up the method.

In figures 4 and 5 the email-opt-in procedure is shown. It allows for accessing the content from other devices or to regain access after cookies have been deleted. It starts with the check if there is already a a user's email registered with the AT (31). If a email registration exitsts , the user is asked if a new email token link (ET link) should be sent to this email (33). It should be impossible to enter a different email to avoid misappropriation. Otherwise the user is prompted to enter their email address (32). If approved, an ET is generated, and a link is sent to the corresponding email address (34).

If the user clicks on the new link, the web-app receives the new request (35). If the AT doesn't have a registered email (36), it proceeds with the registration of the ET's email (42) with the AT and the BID is registered with the ET. To allow later direct BID cookie access on the current client device, the requests BID is additionally registered with the AT (40) and access is granted (41).

If the AT already has a registered email (36), this email is checked against the ET's email (37). If not equal, the request is rejected (38). Otherwise the requests BID is checked against the ET's registered BID (39) to ensure the ET can only be used from one device (38). If the BID is the same, the BID is additionally registered with the AT to allow later direct BID cookie access on the current client device (40) and access is granted (41).

This approach gives each AT two access options: directly via the first used device and via

email with the registered email address.

The BID registrations may have a limited lifetime. When a BID is registered with an AT, the corresponding DB record may be marked with a timestamp. Subsequent BID access can be checked against this timestamp and rejected if expired.

Every AT series can limit access to one or more BIDs per AT. This allows, for instance, for direct access for groups.

The method may include a failure per IP address rate limiter, to protect against brute force attacks. This limiter also allows for shorter ATs, improving the user experience.
Some mobile QR-reader apps automatically send an HTTP request and then open a separate browser when scanning a web URL. As the first request already registers a BID using the QR-reader app identification, the subsequent browser request might be unduly rejected. To prevent this, an interstitial page with user interaction may be displayed so the BID is registered only when the user clicks on a button. This button could be used for e.g. language selection.

# CLAIMS

1- A method for web access control characterized in that it comprises the use of a combination of a unique secure random access-token (AT) and a browser ID (BID) using the following steps:

- creating a content item (1) in a content management system;
- generating a series of unique secure random access tokens (2) and storing them in a database (3);
- generating a file containing the ATs with their corresponding direct link URLs
- when a client device accesses the content with the direct link URL using a browser (11), checking with the server if the request's BID is already registered for this AT;
    - if it is already registered, allowing access to the content;
    - if it is not already registered, checking if a preset limit of allowed registered BIDs for the AT has been reached;
        - if the limit has been reached, denying access to the content;
        - if the limit has not been reached, register the new BID with the AT and allowing access to the content.

2- Method, according to claim 1, characterized in that the code for direct access is printed in a physical medium.

3- Method, according to claim 2, characterized in that the code for direct access to the content is a QR code.

4- Method, according to claim 1, characterized in that the browser (11) accessing the web-app for the content is checked by the server for a browser ID (BID) cookie (12) before checking with the server if the request's BID is already registered for this AT and, if none exists, a new secure unique random number is generated (15) and set as the BID cookie.

5- Method, according to claim 1, characterized in that if the preset limit of allowed registered BIDs for the AT has been reached an opt-in procedure is initialized.

6- Method, according to claim 1, characterized in that the browser (11) accessing the web-app by a non-initial request is checked by the server for a browser ID (BID) cookie (12) and, if none exists, access is denied.

7- Method, according to claim 1, characterized in that the BID registrations are marked with a timestamp and have a limited lifetime.

8- Method, according to claim 1, characterized in that the direct link URL guides to an interstitial page and that the BID is registered after user action.

9- Method, according to claim 1, characterized in that it comprises a failure per IP address rate limiter.

10- A server configured to evaluate a request of a client device for access to created content, with the method of any of the claims 1 to 9, characterized in that it uses a combination of a unique secure random access-token (AT) and a client-device browser ID (BID), wherein the server if the request's BID is already registered for this AT;

if it is already registered, allowing access to the content;

if it is not already registered, checking if a preset limit of allowed registered BIDs for the AT has been reached;

if the limit has been reached, denying access to the content;

if the limit has not been reached, register the new BID with the AT and allowing access to the content.

# FIGURES

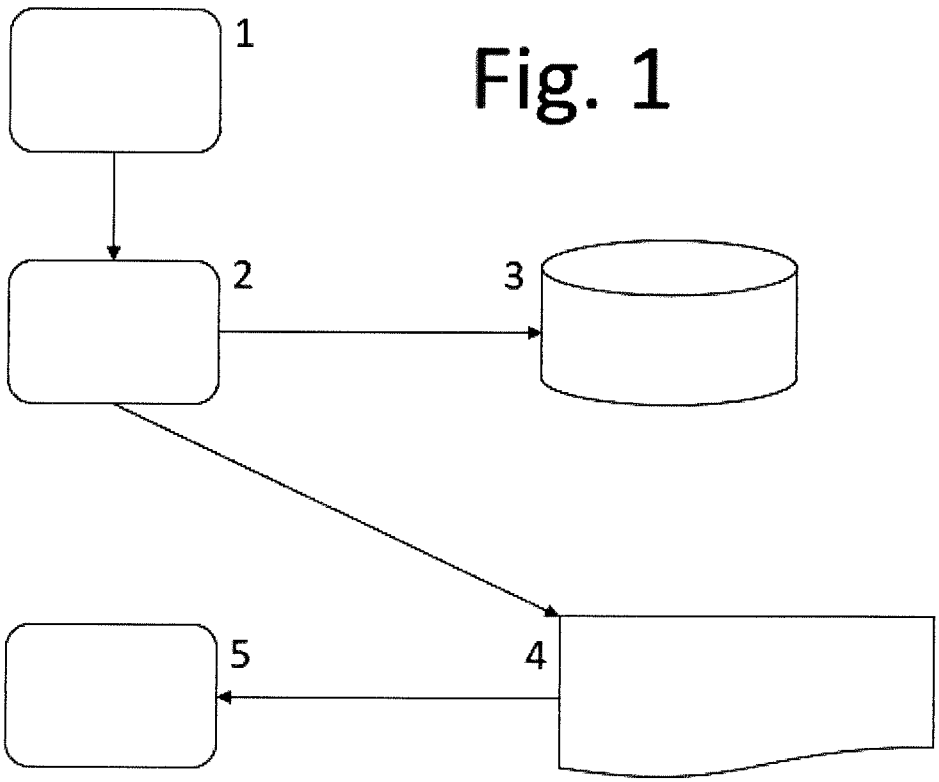



Fig. 1

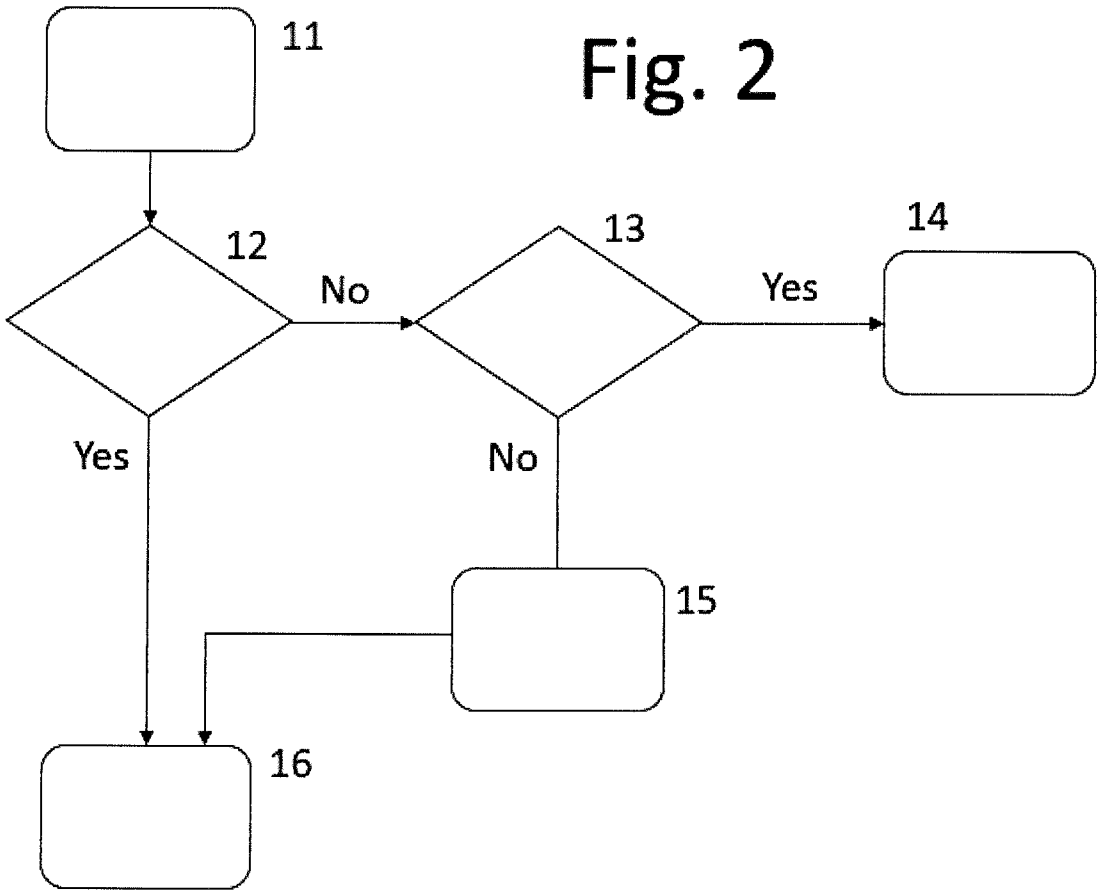



Fig. 2

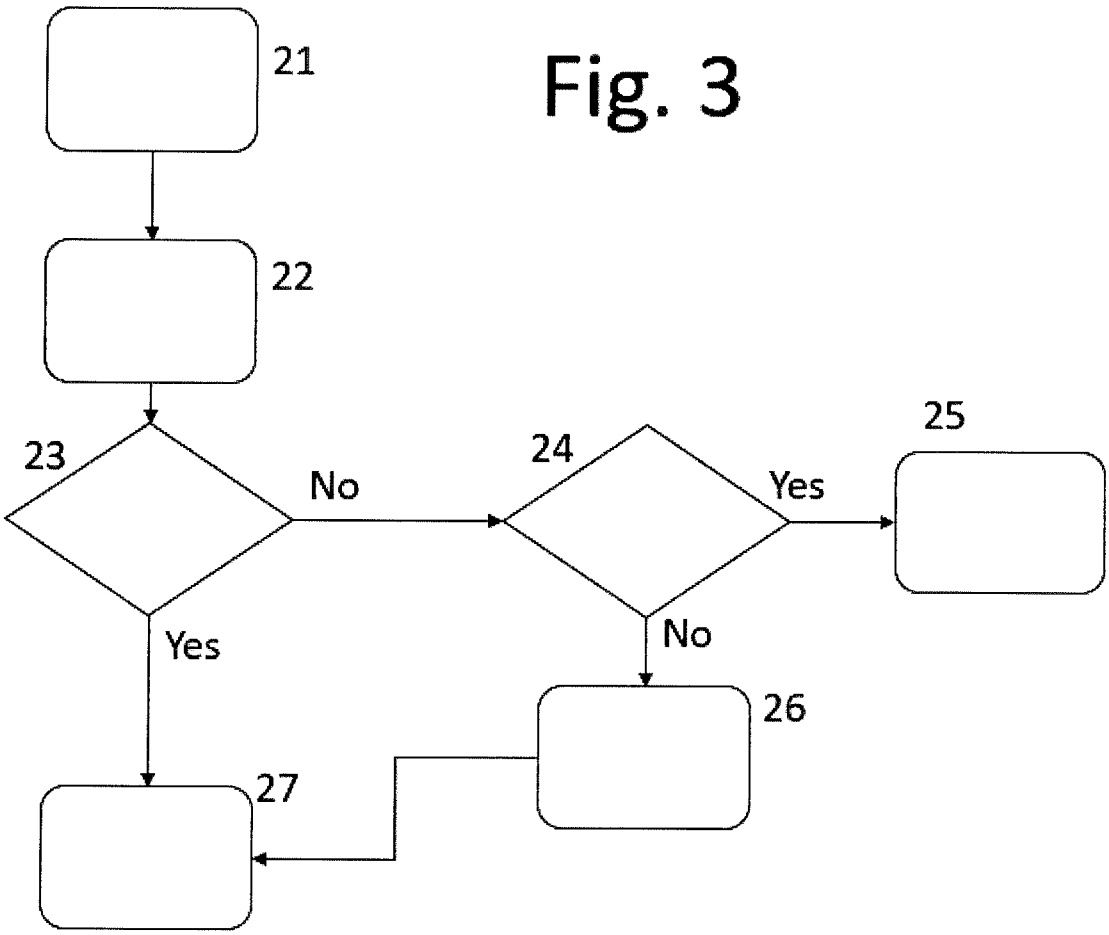



Fig. 3

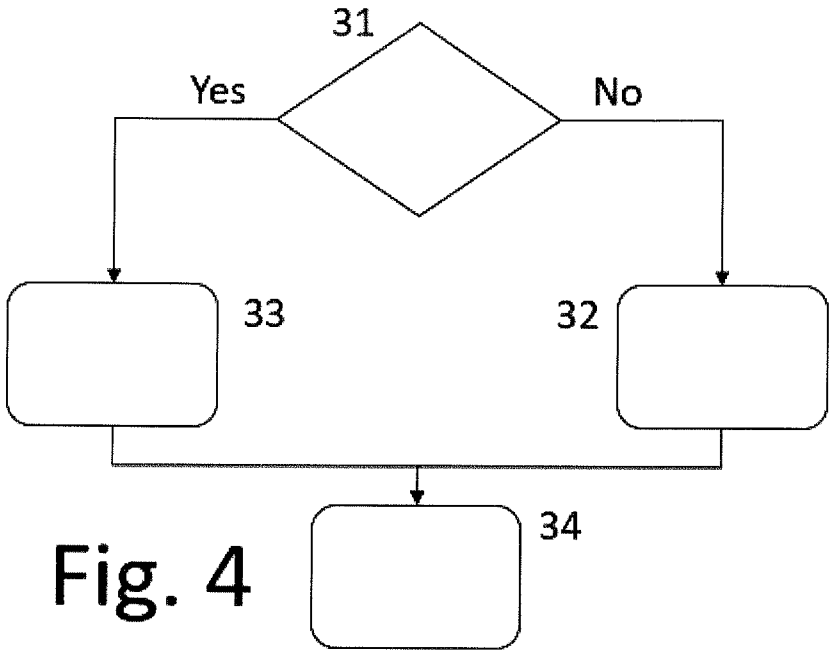
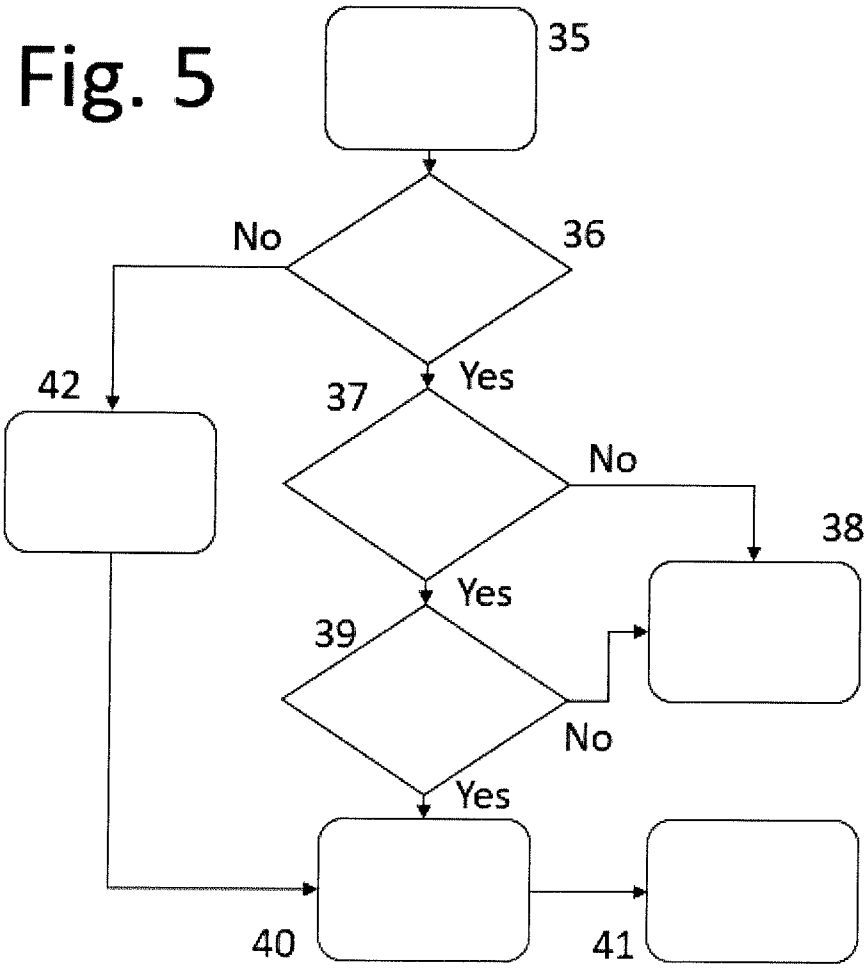



Fig. 4

Fig. 5



# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/076982

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD. H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
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 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. |
|---|---|---|
| X | US 2008/115227 A1 (TOUTONGHI MICHAEL J [US]) 15 May 2008 (2008-05-15) abstract, paragraphs 13-22 ----- | 1-10 |
| A | Anonymous: "Kindle Book License Limit Explained ¦ The eBook Reader Blog", , 1 June 2018 (2018-06-01), XP055658376, Retrieved from the Internet: URL:https://web.archive.org/web/20180601084955/http://blog.the-ebook-reader.com/2018/01/27/kindle-book-license-limit-explained/ [retrieved on 2020-01-15] the whole document ----- | 1-10 |

-/--

[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 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 |
|---|---|
| 17 January 2020 | 27/01/2020 |

| 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 | Murgan, Tudor A. |

1

Form PCT/ISA/210 (second sheet) (April 2005)

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/076982

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 2013/232563 A1 (ACHE MARC [US] ET AL) 5 September 2013 (2013-09-05) abstract | 1-10 |
| A | US 2018/218145 A1 (HUSSAIN MUJTABA [US] ET AL) 2 August 2018 (2018-08-02) abstract | 1-10 |
| A | US 2013/219458 A1 (RAMANATHAN VASUDEVAN [US]) 22 August 2013 (2013-08-22) abstract | 1-10 |
| A | Ms Rina ET AL: "Guide 2013 Edition Managing Intellectual Property for Museums", , 31 December 2013 (2013-12-31), XP055658386, Retrieved from the Internet: URL:https://www.wipo.int/edocs/pubdocs/en/copyright/1001/wipo_pub_1001.pdf [retrieved on 2020-01-15] sections 4 and 6 | 1-10 |

1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2019/076982

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2008115227 A1 | 15-05-2008 | NONE | |
| US 2013232563 A1 | 05-09-2013 | AU 2006249478 A1 | 30-11-2006 |
| | | BR PI0613299 A2 | 28-12-2010 |
| | | CA 2608692 A1 | 30-11-2006 |
| | | CN 101185100 A | 21-05-2008 |
| | | EP 1891599 A2 | 27-02-2008 |
| | | JP 2008542877 A | 27-11-2008 |
| | | KR 20080041150 A | 09-05-2008 |
| | | NZ 563336 A | 29-07-2011 |
| | | US 2006272031 A1 | 30-11-2006 |
| | | US 2008134312 A1 | 05-06-2008 |
| | | US 2013232563 A1 | 05-09-2013 |
| | | WO 2006127359 A2 | 30-11-2006 |
| US 2018218145 A1 | 02-08-2018 | NONE | |
| US 2013219458 A1 | 22-08-2013 | US 2013219458 A1 | 22-08-2013 |
| | | WO 2013123399 A1 | 22-08-2013 |