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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 September 2016 (09.09.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/139505 A2

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 21/30* (2013.01)

(21) International Application Number:
PCT/IB2015/051518

(22) International Filing Date:
2 March 2015 (02.03.2015)

(25) Filing Language: English

(26) Publication Language: English

(72) Inventor; and
(71) Applicant : **BRADFORD, Dylan** [FR/FR]; 49 Boulevard Raymond Poincare, Le Manet, F-06160 Juan Les Pins - Antibes (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, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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).

Published:

— *with declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority*

WO 2016/139505 A2

(54) **Title**: ICONOGRAPHIC SECURED SYSTEMS

(57) **Abstract**:

Title of invention: ICONOGRAPHIC SECURED SYSTEMS.

Brief Description of the Drawings:

[0004] FIG. 1 shows a system for resident or roaming user being fixed or mobile to securely get access to sensitive stored information whether online or offline according to one or more embodiments of the present disclosure:

[0005] FIG. 2 shows a flow chart of the steps for a user to send credentials request to a web server and get authenticate through 2nd factor protection according to one or more embodiments of the present disclosure.

[0006] FIG. 3 shows a flow chart of the steps for a user to add new entry sensitive information to its account private data list according to one or more embodiments of the present disclosure.

[0007] FIG. 4 shows a flow chart of the steps for a user to select an existing entry from its private data list for update or deletion according to one or more embodiments of the present disclosure.

[0008] FIG. 5 shows a flow chart of the steps for a user to select from personal mailbox an email with crypted sensitive information according to one or more embodiments of the present disclosure.

[0009] Embodiments of the present disclosure and their advantages are best understood by referring to the detailed description that follows. It should be appreciated that reference numerals are used to identify the elements illustrated in one or more figures.

Detailed Description:

[0010] On user's subscription, the information required is user email address as login and password with mandatory strong validation scheme. A 2nd factor protection key is required too, such that only the user is owner of a private key and no reverse deciphering is possible. So the system is unaware of user private data, a token is encrypted using AES 256 bits PCKBS#12 for identifying the user. A proprietary combination of existing and new implemented ciphering algorithm is used to protect both user sensitive private data & stored data in the database. If any intrusion & /or spoofing - phishing on user identity occurs, depending a security level set by the user, the 2nd factor protection prevent anyone to get access to its account information. Of course the system on subscription ask user to accept terms of usage and that it shall not store and / or write down its private key same as a bank card code. No cookies nor cache form data are stored locally on user's devices, if user loses its private key, the account could be locked on its demand and / or a renewal key shall be provided to the user, but all its sensitive data information would be lost. A restoration of lost data could be possible but would require some time to recover.

Once the user authentication through the web server, its preferences, data catalog, private data list, are displayed on its dashboard. The service level selected by the user on subscription impact user preferences such as services being available or not.

[0011] The system and methods described in FIG.2 explain how the user get authenticated through the Authentication Service and Validation Service, and Resource Protection Service. The user provides its credentials using email login and two factor protection keys format being validated by the Validation service. Then the Authentication service checks the user credentials, and checks if the user account is active and / or locked. On successful authentication and active account the user get access to its dashboard being displayed. The notification service based on user preferences and activation may display miscellaneous informations on the top toolbar. The Resource protection service loads the user private data list into its dashboard. No private sensitive data are displayed on the list only informative data. Any resources loaded are referenced by an encoded token to prevent any intrusion to map user private data type to its identity.

[0012] The system and methods described in FIG.3 explain how the user adds a new entry to its list of private data. Based on the browser compatibility and support of Drag & Drop, the user can extend its data catalog with a new private data type through iconic representation. If not a predefined set of data (iconically represented or not) based on user service level subscription could be loaded by the Resource protection service into user's data catalog, then the user can select one type of private data to add a new entry in its list of private data. The Validation service on user preferences and activation applies validation constraints on entered sensitive information, moreover based on the input type such as password text field is not cleared type but in wildcard. The QR Code generator service based on user preferences and activation applies on the new sensitive information. Before submit, the user has the possibility to validate the veracity of the information encrypted under its secured account by reading it with the Qr Code reader. As well the Email service could be used at this step to send to user's subscription email box the new encrypted and ciphered private data with or without a resource mapping such as an icon for quick identification.

[0013] The system and methods described in FIG.4 explains what user can do on entry selection. The entry is loaded from the private data

list, where its representation in the list is completely informative, no sensitive information is displayed to prevent eye sneaking over the shoulders. The entry information being displayed are not in clear and resolution of Qr Code could not allow long distance reader to scan it. The Notification service based on user preferences and activation provides the possibility for the user to set the expiration date or being notified either through alert under its secured account and / or email. The QR Code generator service based on user preferences and activation applies on update over sensitive information. The system provides an easy switching between data type through a combo box representing all user's data catolog so that the user can update not only the sensitive information but change its type. An optional version information field is handled too that is global in the catalog and different in the entry. The Validation service based on user preferences and activation applies validation constraints to updated sensitive information before submit. An URL input field is provided with its format constraints for the Automatic Secured Login service system (ASL) with optional conjunction with the QR Code generator service (ASLQ). The data entry input fields can be extended on demand with proper sets of validation constraints. The Email service based on user preferences and activation can send to user's subscription email box the new encrypted and ciphered private data with or without a resource mapping such as an icon for quick identification.

[0014] Refer to the figures wherein the drawings are for purposes of illustrating embodiments of the present disclosure only, and not for purposes of limiting the same. FIG. 1 shows a system for a user to use a trusted device to scan QR code displayed on a display of an untrusted device to supply sensitive information to an identity provider for the identity provider to broker a login to a Website according to one or more embodiments of the present disclosure.

[0015] A user 100 carries a trusted device 102. Trusted device 102 may be a smart phone (e. g., iPhone, Google phone, or other phones running Android, Window Mobile, or other operating systems), a tablet computer (e.g., iPad, Galaxy), personal digital assistant (PDA), a notebook computer, or various other types of Wireless or Wired computing devices. It should be appreciated that trusted device 102 may be referred to as a mobile device without departing from the scope of the present disclosure. Trusted device 102 may have a camera. Trusted device 102 may communicate over a net Work 106 with an identity provider 108. A Website server 116 hosts a Website and may also communicate with identity provider 108 over network 106. The Website may be operated by a financial institution, a merchant, or other entities providing secured access to authorized users. In one embodiment, identity provider 108 may broker a login session to Website server 116 by user 100.

Technical field

[0002] The present disclosure relates generally to systems and methods for user to access securely sensitive personal data offline & online. More precisely the present disclosure relates to methods and systems providing resident & roaming user being fixed or mobile to get access to their private secured sensitive information data from a certified website server.

Background

[0003] Users from internet inherently have many accounts or applications to login daily and many situations prevent them from an easy and secure access experience depending on which ecosystem they use (devices, operating systems, security level) and their status towards secure or unsecure internet access. Recent studies revealed that most user create a weak level of credentials and / or re-use of them for all accounts or applications, increasing inherently the risk of intrusion & hijacking of user accounts. The presence of smartphones & tablets applications increasing exponentially requires more than ever a high security level on sensitive information access that could be at risk with malwares or key-logger spywares. Moreover distributed and shared informations through cloud solutions increase the access to sensitive information if a one of the user devices is stolen and stores login credentials or caches ciphering shared keys. Finally protection can be expired per accounts and / or applications thus making it more difficult to handle in an agenda. Herein methods and systems provide a solution to the latter enumerated issues:

The weakness on user credentials is resolved by a 2nd factor protection with a mandatory high strength level validation of the main system user account through secured web server HTTPS. Then the second level once authenticated of applications' protection goes through the same 2nd factor protection and optional strength level validation. From main system user account, some sensitive information can be sent to its mailbox in one click, therefore user being offline through its email client mailbox can get access to sensitive information that was set with lower level of protection on QR Code scanning, if highest level was setup then user must be online for 2nd factor protection authentication. Therefore the user can setup per account and / or applications the level of security in a centralized way, and setup the notification service level before data access expires. Therefore no security keys are stored on user's device nor on server as based on unreversed 2nd factor protection mixed new ciphering algorithm, if devices are stolen or mail box intruded based on highest level of protection setup by the user, access will be protected by the 2nd factor protection.

We claim:

1. A system comprising:

   a transactional ciphered solid storage system of user private sensitive data; wherein the user private sensitive data includes user credentials for authentication; wherein authentication service receiving the user credentials for login provides access to user's resources; wherein user mandatory 2nd factor protection is required for the resource protection service to display each user resources on the Website on any devices being used;

2. The system of claim 1, wherein user login session is protected with 2nd factor protection on the Website on any devices but requires secured HTTP over SSL (HTTPS).

3. The system of claim 2, wherein authentication service on the Website provides user login session creation after evaluating the level of trust for the user based on the credential information, comprises an internal security token for accessing user private sensitive data as resources from ciphered database.

4. The system of claim 1, wherein resource protection service to the Website provides the deciphering list of user resources requires system of claim 2 and additional security token based on system of claim 3.

5. A system comprising:

   a transactional ciphered solid storage system of user private sensitive data; wherein each resource is associated with a pre-defined and customizable set of private data type with an optional add new type action by drag & drop facility depending on browser support; wherein each listed resource provides either a code by qrcode generator service code or HTTPS URL encoded encapsulating either user private sensitive data or HTTPS URL encoded access to it; wherein the code and / or secured HTTPS URL could be sent by email service to user's private mailbox; wherein an editable form could be displayed on resource selection with automatic re-evaluation of its input fields from qrcode & HTTPS URL encoded to expiration date; wherein on expiration of the private sensitive data is sent by the notification service to the user's private mailbox.

6. The system of claim 9, wherein resource protection service to the Website provides a user pre-defined and customizable set of private data with optional add new type action by drag & drop facility depending on browser support is loaded.

7. The system of claim 8, wherein the selection on any listed resource triggers the display of an editable form, provides

either a code by qrcode generator service code or HTTPS URL encoded encapsulating either the latter user private sensitive data or HTTPS URL encoded access to it. The resource is displayed in an editable form where user can update or delete from the list, any private sensitive data updated triggers re-evaluation of either qrcode or HTTPS URL encoded.

8. The system of claim 7, wherein an expiration date input field is editable in the form displayed, provides information for the notification service. The notification service provides either or both alerts and email notifications.

9. The system of claim 7, wherein email service by the Website provides sending to user's private mailbox either the qrcode or HTTPS URL encoded.

10. A method comprising:

validating & authenticating the user credentials by Validation & Authentication Service for a Website to grant user access to its private sensitive data;

deciphering user resources through a transactional ciphered solid storage by Resource Protection Service;

generating qrcode on demand per resource by the Generartor Service with combining 2nd factor protection;

delivering to user private mail box different level of secured HTTPS URL & qrcode by Email Service;

alerting &/or delivering notification on user resource expiration by Notification Service.

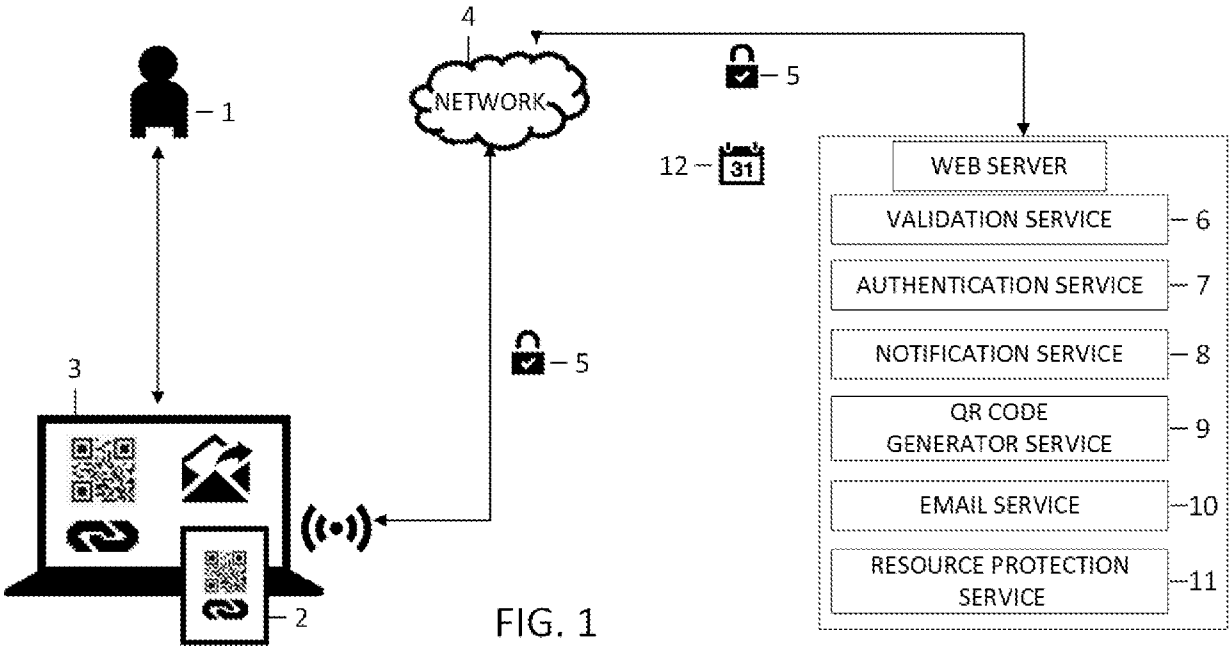

4
NETWORK
1
5
12
31
WEB SERVER
VALIDATION SERVICE
6
AUTHENTICATION SERVICE
7
NOTIFICATION SERVICE
8
QR CODE GENERATOR SERVICE
9
EMAIL SERVICE
10
RESOURCE PROTECTION SERVICE
11
3
5
2

FIG. 1

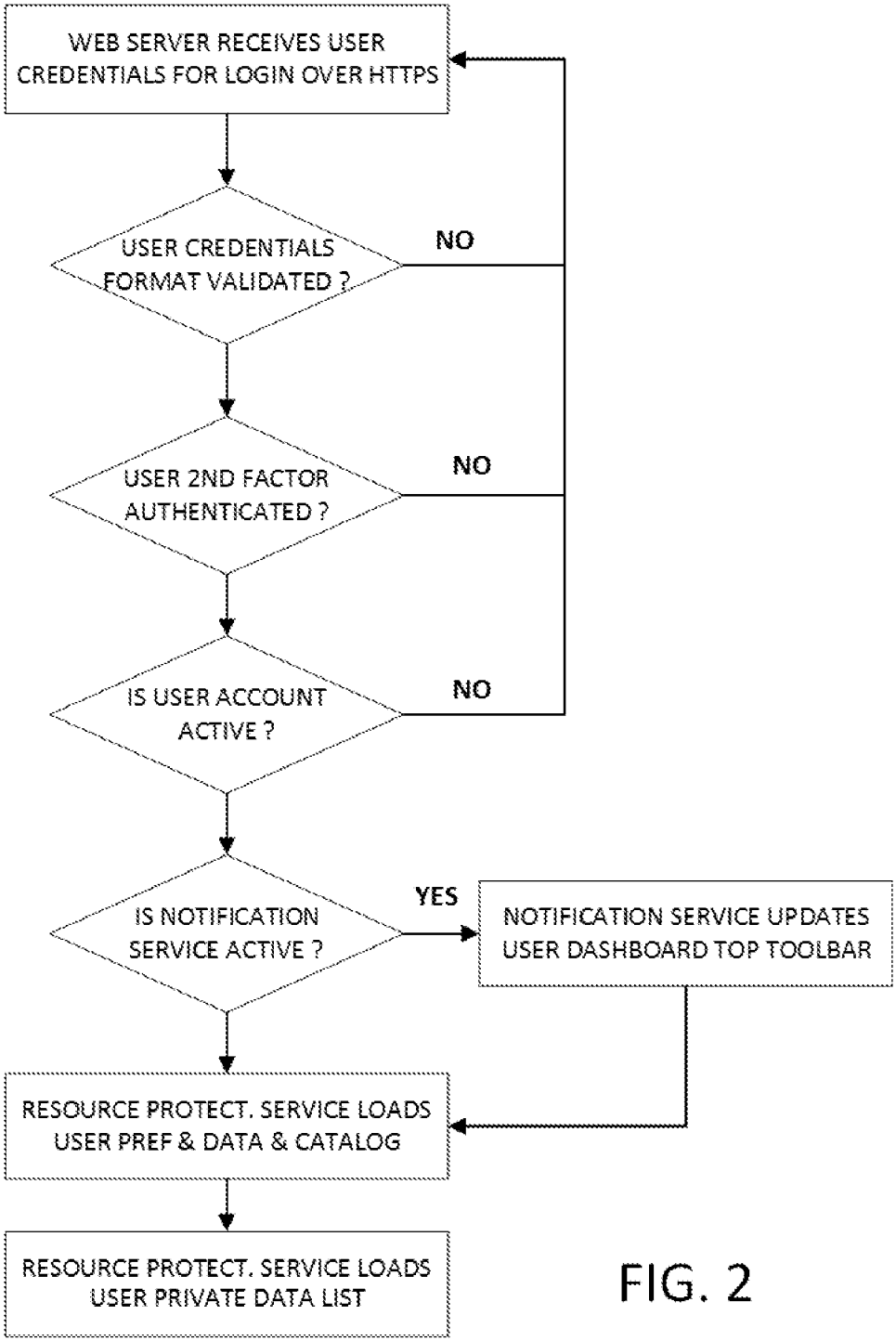

WEB SERVER RECEIVES USER CREDENTIALS FOR LOGIN OVER HTTPS
USER CREDENTIALS FORMAT VALIDATED ?
NO
USER 2ND FACTOR AUTHENTICATED ?
NO
IS USER ACCOUNT ACTIVE ?
NO
IS NOTIFICATION SERVICE ACTIVE ?
YES
NOTIFICATION SERVICE UPDATES USER DASHBOARD TOP TOOLBAR
RESOURCE PROTECT. SERVICE LOADS USER PREF & DATA & CATALOG
RESOURCE PROTECT. SERVICE LOADS USER PRIVATE DATA LIST

FIG. 2

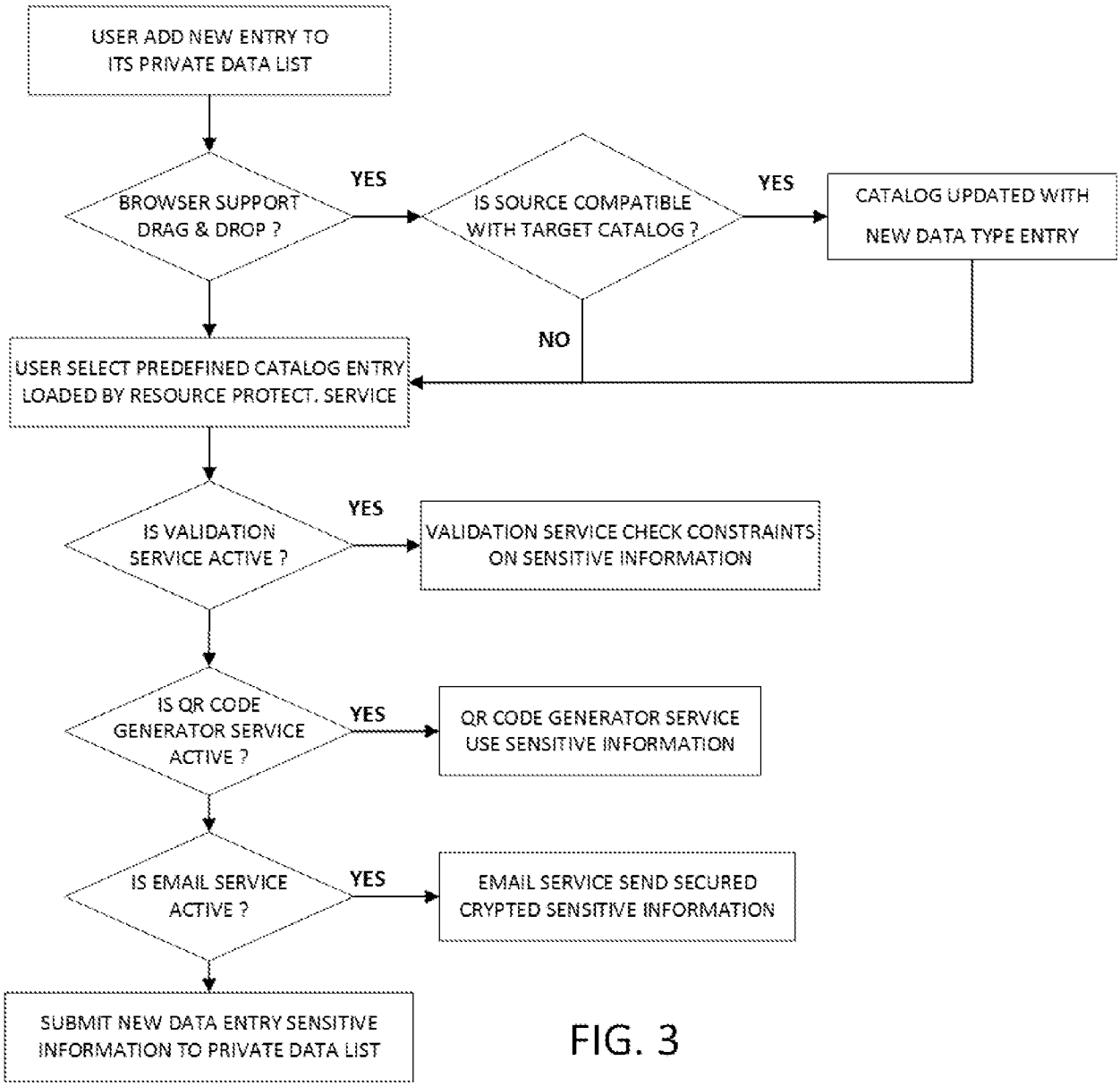

USER ADD NEW ENTRY TO ITS PRIVATE DATA LIST
BROWSER SUPPORT DRAG & DROP ?
YES
IS SOURCE COMPATIBLE WITH TARGET CATALOG ?
YES
CATALOG UPDATED WITH NEW DATA TYPE ENTRY
NO
USER SELECT PREDEFINED CATALOG ENTRY LOADED BY RESOURCE PROTECT. SERVICE
IS VALIDATION SERVICE ACTIVE ?
YES
VALIDATION SERVICE CHECK CONSTRAINTS ON SENSITIVE INFORMATION
IS QR CODE GENERATOR SERVICE ACTIVE ?
YES
QR CODE GENERATOR SERVICE USE SENSITIVE INFORMATION
IS EMAIL SERVICE ACTIVE ?
YES
EMAIL SERVICE SEND SECURED CRYPTED SENSITIVE INFORMATION
SUBMIT NEW DATA ENTRY SENSITIVE INFORMATION TO PRIVATE DATA LIST

FIG. 3

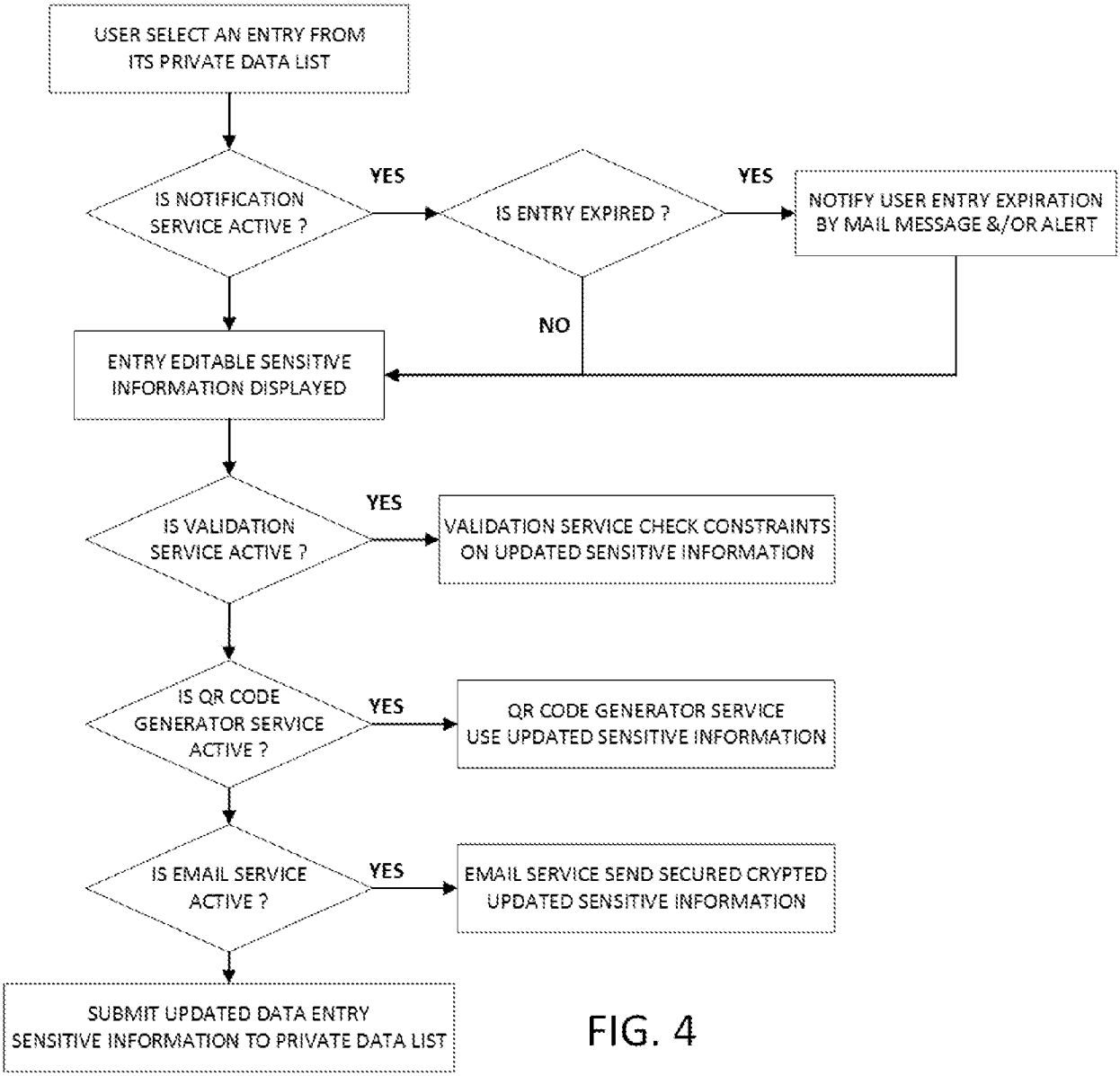

USER SELECT AN ENTRY FROM ITS PRIVATE DATA LIST
IS NOTIFICATION SERVICE ACTIVE ?
YES
IS ENTRY EXPIRED ?
YES
NOTIFY USER ENTRY EXPIRATION BY MAIL MESSAGE &/OR ALERT
NO
ENTRY EDITABLE SENSITIVE INFORMATION DISPLAYED
IS VALIDATION SERVICE ACTIVE ?
YES
VALIDATION SERVICE CHECK CONSTRAINTS ON UPDATED SENSITIVE INFORMATION
IS QR CODE GENERATOR SERVICE ACTIVE ?
YES
QR CODE GENERATOR SERVICE USE UPDATED SENSITIVE INFORMATION
IS EMAIL SERVICE ACTIVE ?
YES
EMAIL SERVICE SEND SECURED CRYPTED UPDATED SENSITIVE INFORMATION
SUBMIT UPDATED DATA ENTRY SENSITIVE INFORMATION TO PRIVATE DATA LIST

FIG. 4

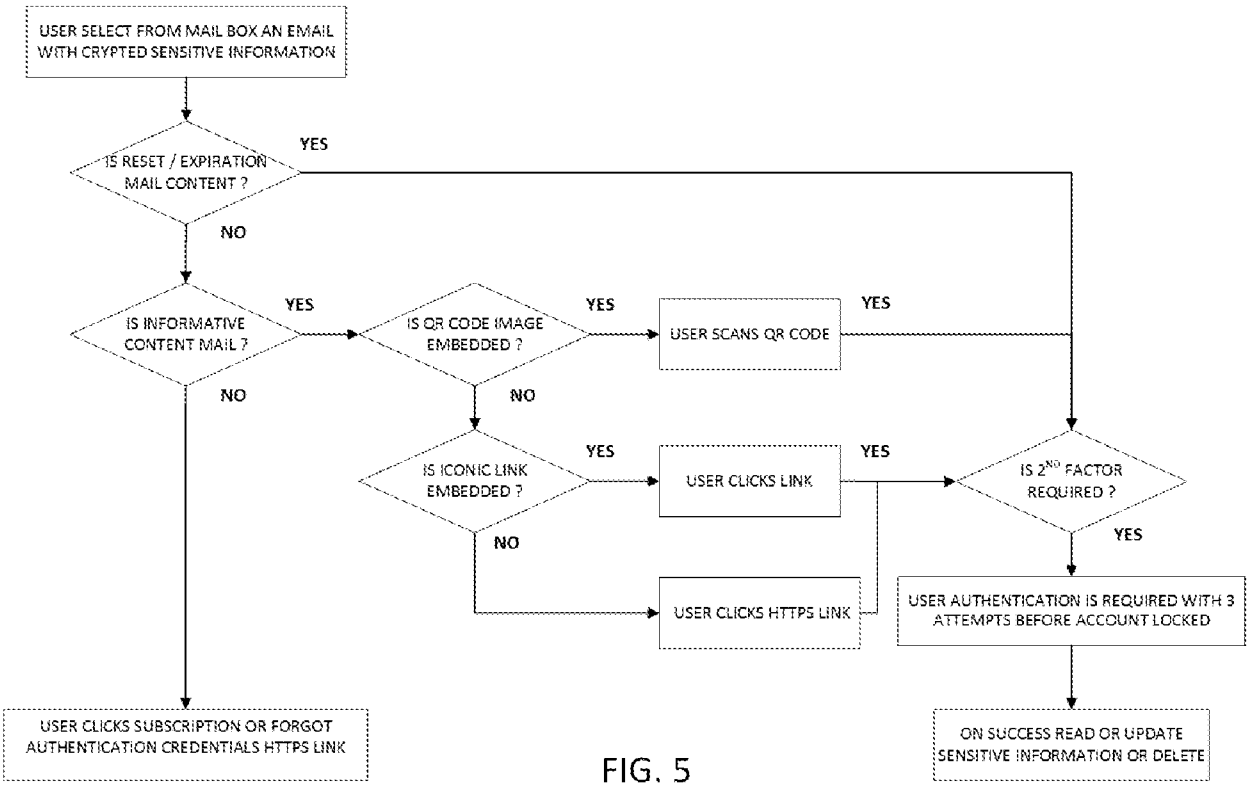

USER SELECT FROM MAIL BOX AN EMAIL WITH CRYPTED SENSITIVE INFORMATION
IS RESET / EXPIRATION MAIL CONTENT ?
YES
NO
IS INFORMATIVE CONTENT MAIL ?
YES
NO
IS QR CODE IMAGE EMBEDDED ?
YES
NO
USER SCANS QR CODE
YES
IS ICONIC LINK EMBEDDED ?
YES
NO
USER CLICKS LINK
YES
USER CLICKS HTTPS LINK
IS 2ND FACTOR REQUIRED ?
YES
USER AUTHENTICATION IS REQUIRED WITH 3 ATTEMPTS BEFORE ACCOUNT LOCKED
USER CLICKS SUBSCRIPTION OR FORGOT AUTHENTICATION CREDENTIALS HTTPS LINK
ON SUCCESS READ OR UPDATE SENSITIVE INFORMATION OR DELETE

FIG. 5

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and Rule 39)

Applicant's or agent's file reference Iconographic	IMPORTANT DECLARATION	Date of mailing *(day/month/year)* 10 August 2015 (10-08-2015)
International application No. PCT/IB2015/051518	International filing date *(day/month/year)* 2 March 2015 (02-03-2015)	(Earliest) Priority date *(day/month/year)*
International Patent Classification (IPC) or both national classification and IPC H04L63/08		
Applicant BRADFORD, DYLAN		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below

1. ☐ The subject matter of the international application relates to:
   - a. ☐ scientific theories.
   - b. ☐ mathematical theories
   - c. ☐ plant varieties.
   - d. ☐ animal varieties.
   - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. ☐ schemes, rules or methods of doing business.
   - g. ☐ schemes, rules or methods of performing purely mental acts.
   - h. ☐ schemes, rules or methods of playing games.
   - i. ☐ methods for treatment of the human body by surgery or therapy.
   - j. ☐ methods for treatment of the animal body by surgery or therapy.
   - k. ☐ diagnostic methods practised on the human or animal body.
   - l. ☐ mere presentations of information.
   - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.

2. ☐ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
   ☐ the description ☐ the claims ☐ the drawings

3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:
   - ☐ the written form has not been furnished or does not comply with the standard.
   - ☐ the computer readable form has not been furnished or does not comply with the standard.

4. Further comments:

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	KOESTEL, Gilbert Tel: +31 (0)70 340-3544

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 203

1 Claims 1-10 do not meet the requirements of Art. 6 PCT (clarity) for, at least, the reasons set out below.
- Independent claim 1, though drafted as a system-claim ('A system comprising ...'), only comprises one feature which unambiguously relates to a system-component, namely a 'solid storage system' (line 2). The remaining features of the claim are defined in terms of method-steps rather than system-components, namely: 'authentication service' (l.5-6), 'receiving credentials' (l.5), 'providing access' (l.5), 'requiring 2nd factor protection' (l.6), 'to display resources' (l.7-8).
It is not clear which devices perform these method-steps and how they relate to each other. For example, lines 2-4 relate to a storage system which stores sensitive data including user credentials. In lines 4-5, these credentials are received by an authentication service. When read in combination, these passages imply that the credentials are somehow transferred from the storage system to the system which implements the authentication service, but the claim does not provide any indication as to how this is implemented.
- In claim 1, lines 6-7 state that a 2nd factor protection is 'required'. It is not clear whether such a method is actually implemented, between which entities, and how it is implemented.
- In claim 1, line 7, it is not clear what 'each' relates to: each user or each resource.
- In claim 1, line 8, the term 'the Website' has no antecedent.
- In claim 1, line 8, it is not clear which devices are implied.
- In claim 2, it is not clear what contradiction is implied by the word 'but'.
- In claim 3, it is not clear what the subject is with the verb 'comprises'.
- In claim 3, the expression 'internal security token' is not clear: it is not clear how it is created, by which entity it is created and which entity has access to it.
- In claim 5, line 3, the expression 'each resource' has no antecedent.
- The dependencies of claims 6-9 are not clear, especially because claim 7 depends on claim 8 and vice versa. As a result, the set of claims 6-9 only comprises dependent claims.
- In claim 10, line 3, it is not clear which entity is implied by the impersonal term 'its', in other words, which entity is the owner of the 'private sensitive data' of line 4.
- In claim 10, line 3, the term 'for' implies a relationship between 'Website' (line 3) and 'private sensitive data' (line 4). It is not clear which relationship. For example the website might actually store these data or it might be a login page providing access to another place where the private data are actually stored.
- In claim 10, lines 5-6, the expression 'decyphering [...] through a [...] storage' is not clear.
- In claim 10, lines 7-8, the expression 'Generator Service' has no antecedent.
- In claim 10, lines 7-8, it is not clear how a QR-code is generated and on the basis of which data.
- In claim 10, line 9, it is not clear how the term 'level' should be interpreted.
- In claim 10, lines 9-10, it is not clear how 'different level of secured HTTPS URL & qrcode' are generated, and on the basis of which data.
- In claim 10 as a whole, it is not clear which entities carry out the

different method-steps and how they interact with each other.

2 As a result of the deficiencies indicated above, it is presently not possible to carry out a meaningful search.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guidelines C-IV, 7.2), should the problems which led to the Article 17(2) declaration be overcome.