



- (51) **International Patent Classification:**
G06F 21/36 (2013.01)
- (21) **International Application Number:**
PCT/CN2014/081588
- (22) **International Filing Date:**
3 July 2014 (03.07.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/842,386 3 July 2013 (03.07.2013) US
- (71) **Applicant:** MPAYME LTD. [CN/CN]; 51 Floor, Hopewell Centre, 183 Queen's Road East, Wan Chai, Hong Kong (CN).
- (72) **Inventor:** GADOTTI, Alessandro; Flat 30A, Block 1, The Zenith, 3 Wan Chai Road, Hong Kong (CN).
- (74) **Agent:** CHINA PAT INTELLECTUAL PROPERTY OFFICE; 2nd Floor, Zhongguancun Intellectual Property Building, Block B, No.21 Haidian South Road, Haidian, Beijing 100080 (CN).

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

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

Published:

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

(54) **Title:** METHOD AND SYSTEM FOR AUTHENTICATING USER USING OUT-OF-BAND CHANNEL

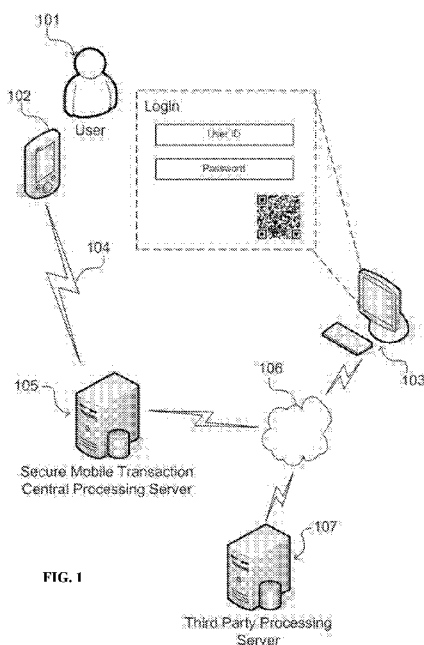


FIG. 1

(57) **Abstract:** The user authentication method comprises : a central processing server generates an encoded data, such as a QR code, from encoding a session number, which can be randomly generated; a first client computing device displays a login page that includes the QR code to a user for authentication; the user uses a mobile communication that has already been registered and paired with the user account stored in the central processing server to image-capture the QR code, and sends the decoded QR code data to the central processing server; the central processing server validates the decoded QR code data against the session number; upon a positive validation, the user may need to enter his/her security PIN according to configuration in the second mobile communication and be sent to the central processing server for validation; and upon a positive validation, the user authentication is completed.

METHOD AND SYSTEM FOR AUTHENTICATING USER USING OUT-OF-BAND CHANNEL

5 **Claim for Domestic Priority:**

[0001] This application claims priority under 35 U.S.C. § 119 to the United States Provisional Patent Application No. 61/842,386, filed July 3, 2013, the disclosure of which is incorporated herein by reference in its entirety.

10 **Cross-references to Related Applications:**

[0002] This application is a continuation-in-part application of the United States Patent Application No. 13/602,197 filed September 2, 2012, the disclosure of which is incorporated herein by reference in its entirety.

15 **Field of the Invention:**

[0003] The present invention relates generally to methods and systems of online user authentication. Particularly, the present invention relates to online user authentication techniques that utilize out-of-band channels.

20 **Background:**

[0004] Many online activities, such as making online purchases and payments, which involve accessing personal and protected information often require user authentication. The most common form of user authentication is the use of a login challenge for a user identifier and password. However, there are a number of
25 drawbacks in this form of user authentication, which include forgotten password, stolen user identifier and/or password, and too simple password, resulting in weak security. Other multi-factor and strong authentication methods and systems have been developed; but most could not uphold strong security without sacrificing user

convenience. Therefore, there is a need for a user authentication method and system that can support strong security and yet demand minimal efforts on the part of the users.

5 **Summary:**

[0005] It is an objective of the present invention to provide a method and system for online user authentication using a mobile communication device. Since the mobile communication device is pre-registered in the user authentication authority system and that the mobile communication device can uniquely identify the authenticating user, it serves as the out-of-band channel for authenticating the user. It is a further objective of the present invention to provide such a method and system that support strong security and require the user to memorize and supply only a security personal identification number for authentication.

10 [0006] In accordance with various embodiments, the present invention can be implemented as an extension to the secure mobile payment system described in United States Patent Application No. 13/602,197.

15 [0007] In accordance with various embodiments, the present invention comprises a central processing server accessible through a communication network, such as the Internet; a plurality of users; mobile communication devices and client computing devices that can access the central processing server; and a third party computing processor that can access the central processing server.

20 [0008] In accordance with various embodiments, the functionalities of the central processing server comprises user authentication, user account management for managing user accounts, wherein the user accounts contain user identification and authentication credentials, and are stored securely in a database.

25 [0009] In accordance with various embodiments, the central processing server includes a plurality of user interfaces for user interaction using various types of computing devices and mobile communication devices running web browser

applications. In addition, the central processing server also includes server backend APIs for machine-to-machine integration enabling specially-developed applications running in the third party computing processor to communicate with the central processing server. These user interfaces and server backend APIs facilitate the functionalities including, but are not limited to, user authentication, user account management and online shopping by users, system administration by administrators, online shopping inventory, payment, and fulfillment management by users.

[0010] In accordance with various embodiments, each of the mobile communication devices is equipped with a camera or scanner for optically capturing images of computer-generated encoded data such as barcodes. In accordance with various embodiments, the mobile communication device is configured to process the captured encoded data image and exchange data with the central processing server for facilitating various aforementioned functionalities such as user authentication.

[0011] The central processing server with its database, user interfaces and server backend APIs, and the mobile communication devices running the secure mobile transaction mobile application constitute a secure mobile transaction system. In accordance with various embodiments, each user account in the secure mobile transaction system may associate (pair) with only a single mobile communication device at any one time.

[0012] In one aspect of the present invention, a user who has already been registered and created a valid user account in the secure mobile transaction system may use his/her mobile communication device that has already been registered and paired in the secure mobile transaction system to authenticate for accessing a protected third party application, such as a third party web site, provided by the third party processing server, or one or more protected user interfaces provided by the central processing server. The user authentication method comprises: the central processing server generates an encoded data, such as a QR code, from encoding a session number, which can be randomly generated; a first mobile communication device or a first client

computing device displays a login page that includes the QR code to the user for authentication; the user uses a second mobile communication that has already been registered and paired in the secure mobile transaction system to image-capture the QR code, and sends the decoded QR code data to the central processing server; the central processing server validates the decoded QR code data against the session number; upon a positive validation, the user enters his/her security PIN in the second mobile communication and be sent to the central processing server for validation; and upon a positive validation, the user authentication is completed.

Brief Description of the Drawings:

[0013] Embodiments of the invention are described in more detail hereinafter with reference to the drawings, in which

[0014] FIG. 1 shows a block diagram illustrating an embodiment of the presently claimed secure mobile transaction system; and

[0015] FIG. 2 depicts a user activity diagram illustrating an embodiment of user authentication process using the secure mobile transaction system; and

[0016] FIG. 3 shows an exemplary embodiment of the transitioning user interface being displayed during the user authentication process using the secure mobile transaction system.

Detailed Description:

[0017] In the following description, methods and systems of online user authentication using out-of-band channels and the like are set forth as preferred examples. It will be apparent to those skilled in the art that modifications, including additions and/or substitutions may be made without departing from the scope and spirit of the invention. Specific details may be omitted so as not to obscure the invention; however, the disclosure is written to enable one skilled in the art to practice the teachings herein without undue experimentation.

[0018] System:

[0019] Referring to FIG. 1. In accordance with various embodiments the presently claimed invention comprises a central processing server **105** accessible through a first communication network **104**, which can be the Internet, a telecommunication network, or any network supporting the TCP/IP protocol; a plurality of users **101** each associating with a user account; mobile communication devices **102** that can access the central processing server **105** through the first communication network **104**; client computing devices **103** that can access the central processing server **105** and a third party processing server **107** through a second communication network **106**, which can be the same as the first communication network **104** or a separate communication network that can be the Internet, a telecommunication network, or any network supporting the TCP/IP protocol.

[0020] In accordance with various embodiments, the functionalities of the central processing server **105** comprises user authentication and user account management for managing user accounts, wherein a data record of a user account comprises the user's identification and authentication credential.

[0021] In accordance with various embodiments, the central processing server **105** includes at least one group of user interfaces for users accessible by the mobile communication devices **102** and the client computing devices **103**. The group of user interfaces include interactive transactional web pages that can be displayed in web browser applications running in the mobile communication devices **102** and the client computing devices **103**, and user interfaces that are specifically designed for specifically-developed mobile applications running in the mobile communication devices **102**. One exemplary embodiment of such user interface is a mobile application (App) running on the iOS[®] operating system developed by Apple[®] Inc. Another exemplary embodiment of such user interface is a mobile application (App) running on the Android[®] operating system developed by Google[®] Inc. The central

processing server also provides another group of user interfaces for system administrative users.

[0022] In addition to the groups of user interfaces, the central processing server **105** also includes server backend APIs for machine-to-machine integration, enabling specifically-developed software applications running in the third party processing server **107** to communicate with the central processing server **105**. In accordance to various embodiments, the machine-to-machine data interchanges via the server backend APIs supports industry standards including, but are limited to, XML and JSON.

[0023] These user interfaces and server backend APIs facilitate the functionalities including, but are not limited to, user authentication, user account management, and online shopping by users, system administration by administrators, online shopping inventory, payment, and fulfillment management by users.

[0024] In accordance with various embodiments, the central processing server **105** includes a database for preserving data records of the user accounts, system configuration data, and other meta data. The database can be implemented in the same physical computer server of the central processing server **105**, or in a separate physical computer server. Exemplary embodiments of the database are various commercially available relational database management systems such as Oracle[®] Database and Microsoft[®] SQL Server.

[0025] In accordance with various embodiments, each of the mobile communication devices **102** is equipped with a camera or scanner for optically capturing images of computer-generated encoded data such as barcodes. In accordance with various embodiments, the mobile communication device is configured to process the captured encoded data image and exchange data with the central processing server for facilitating various aforementioned functionalities such as user authentication. In accordance with various embodiments, the mobile communication device configuration for processing the encoded data and executing a

mobile transaction is accomplished by installing and executing mobile application software and/or firmware specifically designed for the mobile communication device (hereinafter referred to as secure mobile transaction mobile application). Optionally, the operating system (OS) of the mobile communication device is modified and/or configured to accomplish portions or all of the aforementioned functionalities.

[0026] The central processing server **105** with its database, user interfaces and server backend APIs, and the mobile communication devices **102** running the secure mobile transaction mobile application constitute a secure mobile transaction system. In accordance with various embodiments, each user account in the secure mobile transaction system may associate (pair) with only a single mobile communication device **102** at any one time. Each of the users **101** may also be required to define a security personal identification number (PIN) for his/her user account according to the system configuration. A user account is created in the central processing server and its record data is stored in the database of the central process server when a new user is registered in the secure mobile transaction system. The user registration process includes steps for registering and pairing his/her mobile communication device. In accordance with various embodiments, the user registration process adopts that of the secure mobile payment system as disclosed in United States Patent Application No. 13/602,197.

[0027] In accordance with various embodiments, the computer-generated barcode is a matrix or two-dimensional barcode such as a Quick Response (QR) code. The barcode can be generated by the central processing server **105**. The barcode contains at least an identity data, which is unique to each barcode at least within the secure mobile transaction system if not globally. The barcode can be electronically displayed on the screen of a client computing device **103** or mobile communication device **102**. The barcode can also be printed and displayed on various portable articles including, but not limited to, a paper ticket and a carrying card.

[0028] In accordance with various embodiments, all communications between the mobile communication devices **102** and the central processing server **105** are PKI encrypted using, for example, AES, and the data communication messages are transmitted over Secure Socket Layer (SSL).

5 [0029] User Authentication:

[0030] In accordance to one embodiment, a user who has already been registered and created a valid user account in the secure mobile transaction system may use his/her mobile communication device that has already been registered and paired in the secure mobile transaction system to authenticate for accessing a protected
10 third party application, such as a third party web site, provided by the third party processing server, or one or more protected user interfaces provided by the central processing server.

[0031] Referring to FIG. 2. The user authentication method comprises the following steps:

15 [0032] 1. **(201)** A user requesting to access the protected third party application provided by the third party processing server or the one or more protected user interfaces provided by the central processing server, wherein the protected third party application can be a third party web site that is protected by access control and requires user authentication for its access and which can be accessed through a web
20 browser application running in a first mobile communication device or a first client computing device, and wherein the protected user interfaces provided by the central processing server can be interactive transactional web pages that are protected by access control and require user authentication for their accesses and which can be accessed through a web browser application running in a first mobile communication
25 device or a first client computing device.

[0033] 2. **(202)** The user is redirected to a login page, wherein the login page can be served from the third party processing server or the central processing server. The login page includes an encoded data such as a barcode that is displayed on

the screen of the first mobile communication device or the first client computing device. The barcode can be a QR code. The encoded data is dynamically generated by the central processing server during the rendering of the login page.

[0034] In one embodiment, the generation of the encoded data comprises the central processing server generating a random number, wherein the random number can be 32 characters (30 characters + 2 checksum) in length; and encoding the random number into a QR code for the encoded data. The random number is a session number for later associating with the user's logon session. In an alternative embodiment, the generation of the encoded data comprises the central processing server encoding one of its previously generated and preserved session numbers into a QR code for the encoded data. A record of the session number is preserved in the database of the central processing server for later validation purposes.

[0035] If the login page is served by the third party processing server, the third party processing server requests and receives the encoded data from the central processing server by invoking the central processing server backend APIs.

[0036] 3. **(203)** The login page with the encoded data is displayed on the screen of the first mobile communication device or the first client computing device. The user, using a second mobile communication device that has already been registered and paired in the secure mobile transaction system, image-captures the encoded data.

[0037] In an alternative embodiment, instead of being displayed on the screen of the first mobile communication device or the first client computing device, the encoded data can also be printed on a physical media, such as a paper ticket or a carrying card, to be presented to the user to image-capture the encoded data using the second mobile communication device.

[0038] 4. **(204)** The second mobile communication device, running the secure mobile transaction mobile application, decodes the image-captured encoded data and extracts the session number.

[0039] 5. (205) The second mobile communication device sends the extracted session number along with the identification data of the second mobile communication device to the central processing server.

[0040] 6. (206) The central processing server receives the session number and the identification data of the second mobile communication device; and validates the session number by matching the previously preserved record of the session number in its database. Upon positive validation, the central processing server retrieves the user account record by matching the identification data of the second mobile communication device. The central processing server associates the session number to the user account.

[0041] 7. (207) If the login page is served by the central processing server, when the web browser application displaying the login page is refreshed under auto-reload (polling) or manual reload, the login page is re-rendered by the central processing server with visual cue for the user to proceed to the next step of the user authentication.

[0042] If the login page is served by the third party processing server, the third party processing server is notified of the successful association of the session number to the user account by way of the central processing server backend API callback or response, or repeated invocations (polling) of the central processing server backend APIs by the third party processing server. Once the notification is received, when the web browser application displaying the login page is refreshed under auto-reload (polling) or manual reload, the login page is re-rendered by the third party processing server with visual cue for the user to proceed to the next step of the user authentication.

[0043] 8. (208) The user enters his/her security PIN in the user interface of the secure mobile transaction mobile application running in the second mobile communication device.

[0044] 9. (209) The second mobile communication device cryptographically encrypts the security PIN and sends the encrypted security PIN along with its identification data to the central processing server.

[0045] 10. (210) The central processing server receives the encrypted security PIN and the identification data of the second mobile communication device; retrieves the user account record by matching the identification data of the second mobile communication device; decrypts the encrypted security PIN and validates the decrypted security PIN against the security PIN stored in the user account record. Upon a possible validation, the user is considered authenticated and the session number is now associated with the user's login session.

[0046] 11. (211) If the login page is served by the central processing server, when the web browser application displaying the login page is refreshed under auto-reload (polling) or manual reload, the web browser application is redirected to the target protected third party application or protected user interfaces provided by the central processing server.

[0047] If the login page is served by the third party processing server, the third party processing server is notified of the successful user authentication by way of the central processing server backend API callback or response, or repeated invocations (polling) of the central processing server backend APIs by the third party processing server. Once the notification is received, when the web browser application displaying the login page is refreshed under auto-reload (polling) or manual reload, the web browser application is redirected to the target protected third party application or protected user interfaces provided by the central processing server.

[0048] In another embodiment, the central processing server and the second mobile communication device, through the secure mobile transaction mobile application, are configured as such that the security PIN to be provided by the user is optional in the user authentication. Thus, the abovementioned steps 7 to 10 may be opted out, and in this case the user authentication is completed upon the positive

validation of the session number and the identification data of the second mobile communication device received by the central processing server.

[0049] The embodiments disclosed herein may be implemented using general purpose or specialized computing devices, mobile communication devices, computer processors, or electronic circuitries including but not limited to digital signal processors (DSP), application specific integrated circuits (ASIC), field programmable gate arrays (FPGA), and other programmable logic devices configured or programmed according to the teachings of the present disclosure. Computer instructions or software codes running in the general purpose or specialized computing devices, mobile communication devices, computer processors, or programmable logic devices can readily be prepared by practitioners skilled in the software or electronic art based on the teachings of the present disclosure.

[0050] In some embodiments, the present invention includes computer storage media having computer instructions or software codes stored therein which can be used to program computers or microprocessors to perform any of the processes of the present invention. The storage media can include, but are not limited to, floppy disks, optical discs, Blu-ray Disc, DVD, CD-ROMs, and magneto-optical disks, ROMs, RAMs, flash memory devices, or any type of media or devices suitable for storing instructions, codes, and/or data.

[0051] Exemplary embodiments of mobile communication devices include, but are not limited to, mobile telephones, mobile telephones with personal computer like capability (commonly referred to as “smartphones”), electronic personal digital assistants (PDAs), portable computers with wired or wireless wide-area-network and/or telecommunication capability such as tablet personal computers and “netbook” personal computers. Examples of mobile communication devices include, but not limited to, the Apple[®] iPhone[®], Google[®] Nexus[™] 10, HTC[®] One[™], Nokia[®] Lumia[™], Samsung[®] Galaxy[™], and Sony[®] Xperia[™].

[0052] The foregoing description of the present invention has been provided

for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations will be apparent to the practitioner skilled in the art.

5 [0053] The embodiments were chosen and described in order to best explain the principles of the invention and its practical application, thereby enabling others skilled in the art to understand the invention for various embodiments and with various modifications that are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the following claims and their equivalence.

Claims:

1. A computer processor implemented method for online user authentication, comprising:

5 generating an encoded data, by a central processing server, wherein the encoded data is encoded for a data comprising a session number stored in the central processing server;

presenting the encoded data to a user for user authentication;

10 image-capturing the encoded data, by a mobile communication device equipped with a camera or optical scanner, wherein the mobile communication device is associated with a user account associated with the user, wherein the user account record is stored in the central processing server, and wherein the user account record comprises an identification data of the mobile communication device;

15 decoding the image-captured encoded data, by the mobile communication device, to extract the session number;

sending, by the mobile communication device, the extracted session number and an identification data of the mobile communication device to the central processing server; and

20 authenticating the user, by the central processing, by matching the extracted session number and the identification data of the mobile communication device received from the mobile communication to the session number stored in the central processing and the identification data of the mobile communication device in the user account record.

25 2. The method of claim 1, wherein the encoded data is a quick response (QR) code.

3. The method of claim 1, further comprising:

capturing, by the mobile communication device, a security personal identification number (PIN) provided by the user, wherein the user account record further comprises a saved security PIN pre-defined by the user;

5 sending, by the mobile communication device, the security PIN to the central processing server; and

authenticating the user, by the central processing server, by matching the security PIN received from the mobile communication device with the saved security PIN pre-defined by the user in the user account record in addition to matching the extracted session number and the identification data of the mobile communication
10 device received from the mobile communication to the session number stored in the central processing and the identification data of the mobile communication device in the user account record.

4. The method of claim 1, wherein the presentation of the encoded data to a user
15 for user authentication is by displaying a login user interface that includes the encoded data on a screen of a client computing device.

5. The method of claim 1, wherein the presentation of the encoded data to a user
20 for user authentication is by presenting a physical media imprinted with the encoded data.

6. A system for online authenticating a user, comprising:
a central processing server configured to:

25 generate an encoded data, wherein the encoded data is encoded for a data comprising a session number stored in the central processing server; and

authenticate the user by matching the extracted session number and an identification data of an mobile communication device received from the mobile communication to the session number stored in the central processing

and the identification data of the mobile communication device in an user account record associated with the user;

the mobile communication device, which is equipped with a camera or optical scanner, is configured to:

5 image-capture the encoded data when the encoded data is presented for user authentication;

 decode the image-captured encoded data to extract the session number;

and

 send the extracted session number and an identification data of the
10 mobile communication device to the central processing server;

 wherein the mobile communication device is associated with the user account, wherein the user account record is stored in the central processing server, and wherein the user account record comprises an identification data of the mobile communication device.

15

7. The system of claim 6, wherein the encoded data is a quick response (QR) code.

8. The system of claim 6, wherein:

20 the mobile communication device is further configured to:

 capture a security personal identification number (PIN) provided by the user, wherein the user account record further comprises a saved security PIN pre-defined by the user; and

 send the security PIN to the central processing server; and

25 the central process server is further configured to:

 authenticate the user by matching the security PIN received from the mobile communication device with the saved security PIN pre-defined by the user in the user account record in addition to matching the extracted session

number and the identification data of the mobile communication device received from the mobile communication to the session number stored in the central processing and the identification data of the mobile communication device in the user account record.

5

9. The system of claim 6, wherein the presentation of the encoded data for user authentication is by displaying a login user interface that includes the encoded data on a screen of a client computing device.

10

10. The system of claim 6, wherein the presentation of the encoded data for user authentication is by presenting a physical media imprinted with the encoded.

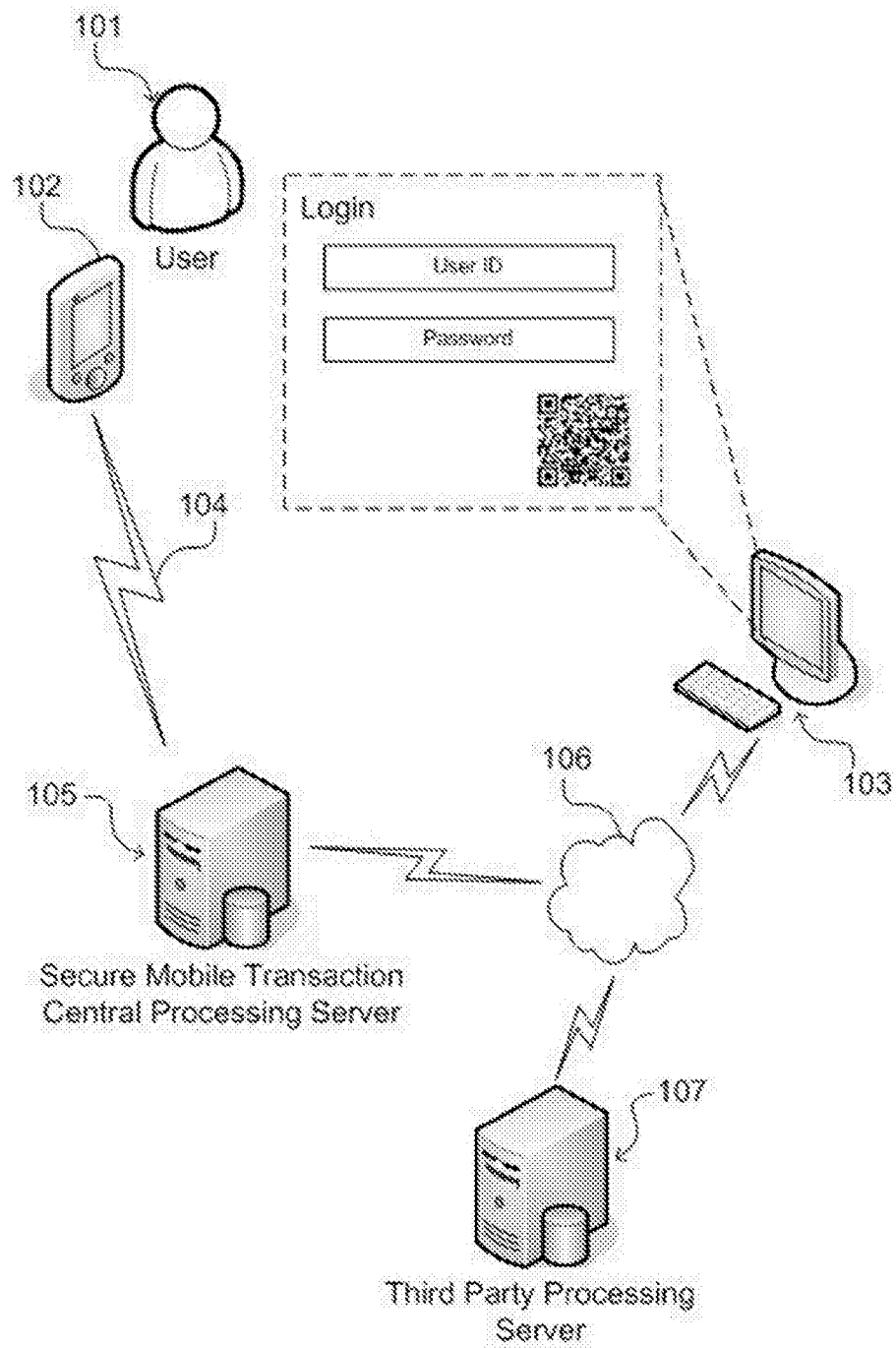


FIG. 1

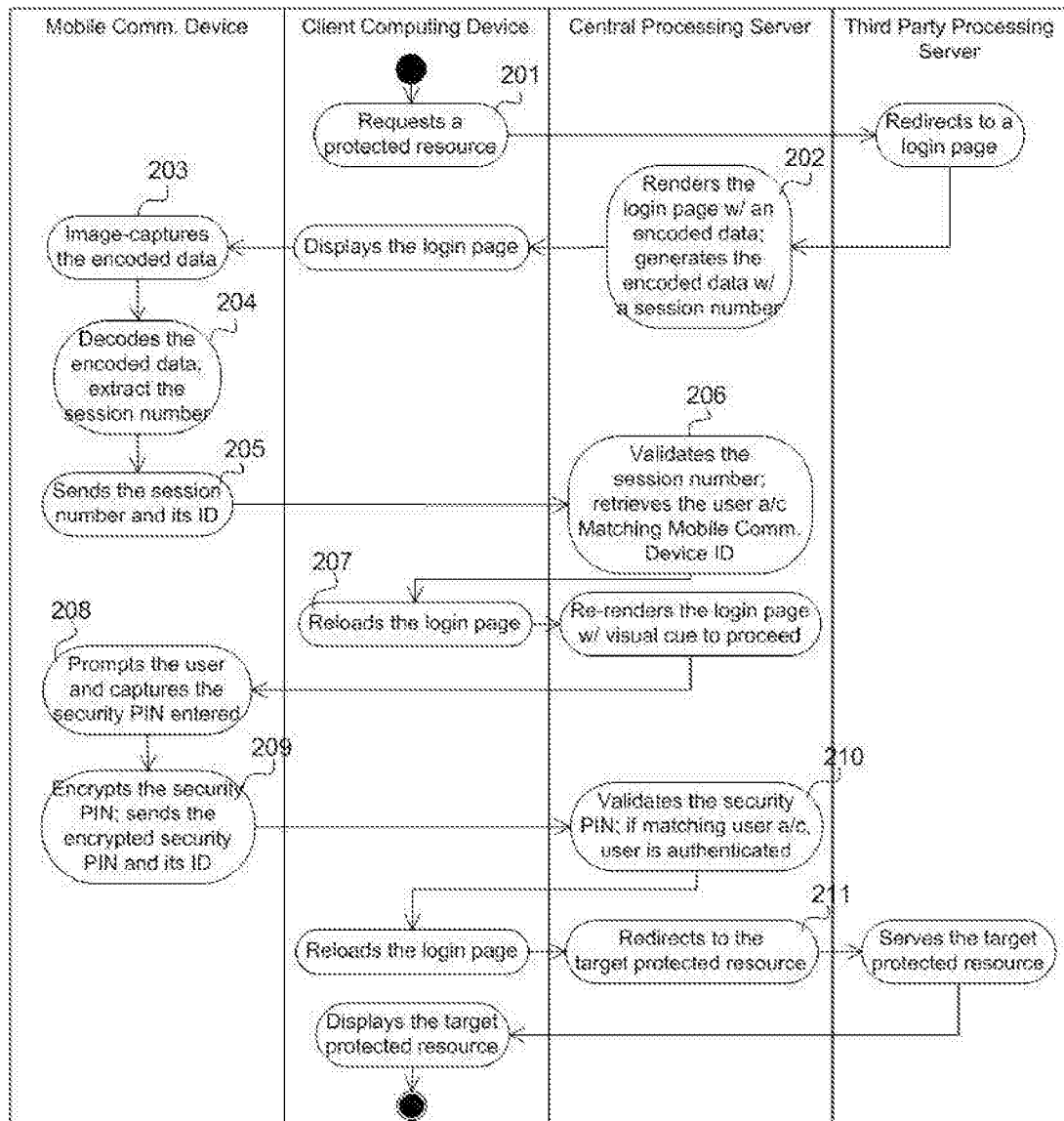
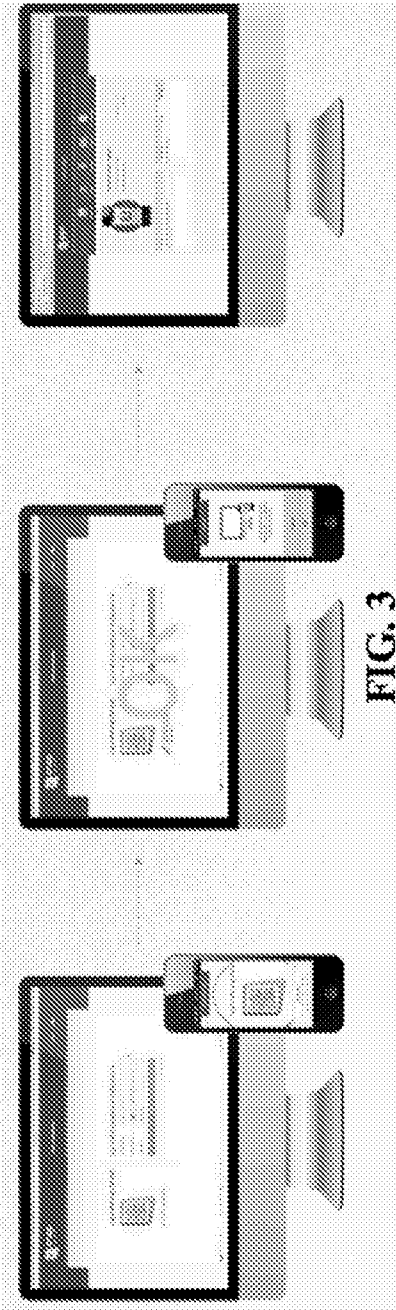


FIG. 2



INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/081588

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/36(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; H04N

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)

CNPAT,WPI,EPODOC,CNKI,IEEE:personal, response, QR, camera, match+, number, data, user, captur+, account, quick, code, identification, encoded, decod+, PIN, session, optical, image, authenticat+, scanner

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013167208 A1 (SHI, JIAZHENG) 27 June 2013 (2013-06-27) description, paragraphs [0012] to [0031] and figure 2	1-10
A	WO 2012135563 A1 (SONY MOBILE COMMUNICATIONS AB) 04 October 2012 (2012-10-04) the whole document	1-10
A	CN 102939613 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 20 February 2013 (2013-02-20) the whole document	1-10
A	CN 102595643 A (LOGITECH EUROPE L.L.C.) 18 July 2012 (2012-07-18) the whole document	1-10

☐ 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	“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
“E”	earlier application or patent but published on or after the international filing date	“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
“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)	“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
“O”	document referring to an oral disclosure, use, exhibition or other means	“&”	document member of the same patent family
“P”	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

16 September 2014

Date of mailing of the international search report

10 October 2014

Name and mailing address of the ISA/

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA(ISA/CN)
6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088 China

Authorized officer

GAO,Xu

Facsimile No. (86-10)62019451

Telephone No. (86-10)62413259

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/081588

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2013167208	A1	27 June 2013	Non e			
WO	2012135563	A1	04 October 2012	CN	103563346	A	05 February 2014
				US	2014197232	A1	17 July 2014
				EP	2692125	A1	05 February 2014
				JP	2014518597	A	31 July 2014
CN	102939613	A	20 February 2013	AU	2011261259	A1	04 October 2012
				US	2012030047	A1	02 February 2012
				WO	2011153505	A1	08 December 2011
				WO	2012118870	A1	07 September 2012
				AU	2012223415	A1	12 September 2013
				US	2012221421	A1	30 August 2012
CN	102595643	A	18 July 2012	DE	102011086678	A1	24 May 2012
				US	8823494	B1	02 September 2014