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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 January 2016 (28.01.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/013924 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06K 7/14* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/MY2015/050068

(22) International Filing Date:
9 July 2015 (09.07.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI2014002191 25 July 2014 (25.07.2014) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(72) Inventors: **SEA, Chong Seak**; c/o MIMOS Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY). **NG, Kang Siong**; c/o MIMOS Berhad, Technology Park Malaysia, Kuala Lumpur, 57000 (MY).

(74) Agent: **PYPRUS SDN BHD**; Suite 8-02, 8th Floor, Plaza First Nationwide, 161, Jalan Tun H.S. Lee, Kuala Lumpur, 500000 (MY).

(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,

[Continued on next page]

(54) Title: SYSTEM AND METHOD OF MUTUAL AUTHENTICATION USING BARCODE

(57) Abstract: The present invention provides a system and method for mutually authenticating user access and registration. Specifically, the system and method uses barcode as a security token for facilitating user authentication. The barcode is used for encoding user credentials and device registration number therein. The barcode can be obtained through a visual channel.

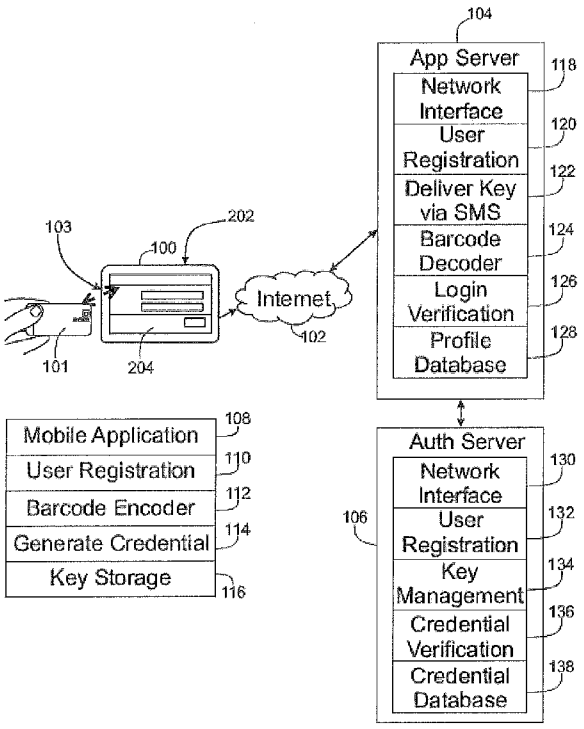

FIG. 1

WO 2016/013924 A1

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:

— *of inventorship (Rule 4.17(iv))*

Published:

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

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

SYSTEM AND METHOD OF MUTUAL AUTHENTICATION USING BARCODE

FIELD OF INVENTION

The present invention is related to authentication mechanisms using a portable communication device and, more particularly, to system and method of mutual authentication mechanisms using barcodes that can be a linear or planar form barcode.

BACKGROUND

Digital identity is an important concern for any individual or company alike. Digital identity refers to all the information about an individual that is digitally available. More number of individuals today perform online activities, for instance, payment transactions, bank login, downloading etc, without paying heed to online security measures, such as private browsing, disabling cookies. As a result, our digital identity is always vulnerable to various privacy threats. And the biggest challenge we face is about losing both – privacy and control over our digital identity.

The most common form of authentication and security measures include usage of usernames and passwords to protect our digital identity online. These usernames and passwords generally comprise complex codes of alphanumeric characters and in some cases, also comprise of special characters or in other instances these characters might also be case sensitive. People often choose common words such as their own name, family members or friends, pets, telephone number, special interests, or some variants that are easy to remember. This makes username and passwords the simplest form of protection yet they are weak and vulnerable as the most common form of attack is password guessing.

Other solutions have been proposed of late, such as One-time Password Authentication (OTP) which generates highly secure one-time password that is valid only for one login session or transaction, ensuring that only properly authenticated users are authorized to access critical applications and data. This type of OTP is currently used by major credit and debit cards users for online authentication.

However, time-synchronized OTPs are subject to problems caused by clock skew, which means that if the authentication server and the user token are not kept at the same time, then the expected OTP value is not generated and the user authentication fails. Also, initial cost requirement is high due to the need of specialized hardware.

Another proposed technique was the challenge-response authentication mechanism (CRAM), whereby an individual is prompted (the challenge) to provide some private information (the response). In security systems, using smart-cards are based on challenge-response. Here, a user is given a code (the challenge) which he enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in. However, the problem arises this may not enough for most of current system required high security implementation.

In recent years, compared to the traditional computers, users now prefer their personal Smartphone mobile devices to access the Internet. Mobile devices are preferred over the traditional stationary computers as the mobile device can be carried from one place to another. Therefore, a secure authentication mechanism that can be easily accessed by a mobile device is needed.

SUMMARY

In accordance with an aspect of the present invention, there is provide a method for mutually authenticating a user through a communication device to access a secured website. The method comprises registering the user with user profile and a registration number of the communication device with the authentication system; requesting access to the secured website through the authentication system with the communication device; rendering a barcode encoded based on user credentials and a user secret key; sending the barcode to the authenticating system for decoding the user credential provided by the user upon requesting access; and comparing the user credential provided by the user against a corresponding user credential stored on the authenticating system. The barcode is rendered as a security token based on a user secret key, wherein the barcode contains user information and credentials.

In one embodiment, a barcode is generated on the user communication device to request for authorization and another barcode is generated on the authentication system for matching the user credentials.

In another embodiment, scanning the barcode through the user communication device via a visual channel. It is possible that scanninng the barcode comprises displaying the barcode on another communication device, wherein the barcode is rendered on a mobile application deployed on the another communication device, and the barcode is rendered based on the user credential sent from the authentication system.

In a further embodiment, the barcode is use as the security token for authenting user registration and user access.

In another aspect, there is also provided an authentication system for mutually authenticating a user through a communication device. The authentication system comprises an application server in communication with the user portable communication device, the application server has a database of user profiles that includes a user ID and a registration number of the user portable communication device; an authentication server for rendering a barcode encoded with a secret key that based on the user profiles; a mobile application for deploying on the user portable communication device, wherein the mobile application operable to communicate with the application server to facilitate user authentication. The system operationally authenticates the user through matching the user credential decoded from the barcode against a corresponding user credential stored on the authentication server.

In one embodiment, the visual channel includes optical means for acquiring the barcode. In another embodiment, the barcode is displayed on another communication device, wherein the barcode is rendered on a mobile application deployed on the another communication device, and the barcode is rendered based on the user credential sent from the authentication server. The barcode maybe a matrix barcode or more specifically, a two-dimensional barcode.

BRIEF DESCRIPTION OF THE DRAWINGS

The detailed description is described with reference to the accompanying figures. The drawings form an integral part of the description and illustrate the preferred embodiments of the invention, which should not be interpreted as restricting the scope of the invention, but just as an example of how the invention can be embodied.

FIG. 1 illustrates an authentication system in accordance with an embodiment of the present invention;

FIG. 2 illustrates a schematic block diagram of a user device **200** in accordance with an embodiment of the present invention;

FIG. 3 illustrates a sequence diagram of a user registration process in accordance with an embodiment of the present invention;

FIG. 4 illustrates an authentication process as the user is accessing a secured website through the application server in accordance with an embodiment of the present invention; and

FIG. 5 illustrates a block diagram of the authentication system in accordance with another embodiment of the present invention.

DETAILED DESCRIPTION

In the following detailed description, a reference is made to the accompanying drawings that form a part hereof, and in which the specific embodiments that may be practiced is shown by way of illustration. These embodiments are described in sufficient detail to enable those skilled in the art to practice the embodiments and it is to be understood that the logical, mechanical and other changes may be made without departing from the scope of the embodiments. The following detailed description is therefore not to be taken in a limiting sense.

One embodiment provides a system and method for two factor mutual authentication methods through a barcode as a security token for providing more effective

secure solution, especially implementation for authenticated users to the systems with minimum data transmitted over the network (via visual channel, i.e. optical means).

It is an object of the invention to use barcode as a security authentication token to establish secure authentication. The barcode provides digital information flow only in one-direction from a portable communication device. According to one object of the invention, when two communicating devices, where one of the communicating device is a portable device that is capable of encoding a precise information into a barcode. The other device, referred to herein as the user portable communication device that can be a portable communicating device, capable of scanning the barcode and decoding the relevant information. The user portable communication device, according to another embodiment of the invention communicates with the portable communication device via a visual channel.

Embodiments of the invention will now be described with reference to the accompanying drawings. The invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein.

FIG. 1 illustrates an authentication system in accordance with an embodiment of the present invention. The authentication system includes a user portable communication device **101**, a portable communication device **100**, a visual channel **103,** a communication network **102**, and an authentication source which include an application server **104** and an authentication server **106**.

The user portable communication device **101** and the portable communication device **100** are communication devices that are able to connect to the authentication source via the communication network **102**, such as Internet. The communication devices may be

any computing devices that are able to establish data communication through the communication network **102**, which include smartphone, tablet PC and etc. Preferably, the user portable communication device **101** and the portable communication device **100** may in someway establish the visual channel **103** for capturing image from one to another, wherein the captured image can be decoded for extracting authentication information. The visual channel **103** may be established through a camera and a display unit, which are respectively integrated on the user portable communication device **101** and the portable communication device **100**. As shown in **FIG. 1**, the visual channel **103** is established through a display unit on the portable communication device **100** and an integrated camera on the user portable communication device **101**, wherein the display unit displays the authentication information encoded in a form of barcode and the integrated camera captures an image of the barcode. It is understood to a skilled person that the visual channel may be established through may other means, for example, the means for capturing authentication information may be a connected camera or a dedicated barcode scanner, whilst the means for displaying the barcode may be a monitor screen or even a piece of printed material with the barcode printed thereon.

It is well understood that the barcode can be any matrix barcode or any two-dimensional (2D) code, such as TOF417, C0DE49, CODE 16K, tQR Code, Data Matrix, Maxi Code, Code One and so on. The type of code used can be selected depending on the requirement and information to be embedded therein. QR code is now favorably adapted as it has relatively large capacity, high reliability, can represent characters and images, and other information, confidentiality, security and etc. It can also have 360-degree recognition ability and represent characteristics of Chinese characters, and become easy to implement.

The authentication system further includes a mobile application **108,** which includes a user registration module **110**, and barcode encoder **112**, a credential generator **114**, and a key storage **116**. Preferably, the mobile application **108** is a trusted application obtained from a trusted source. The trusted source can be any trusted source mobile apps depository center, such as Apple App Store, Google Play or any app marketplace, or directly from the application server **104** of the authentication source. Preferably, either one or both of user portable communication device **101** and the portable communication device **100** are deployed with the mobile application **108** for realizing the authentication.

Operationally, the mobile application **108** communicates with the authentication source through the communication network **102**. The user registration module **110** facilitates means for registering a new user on the communication devices directly. The user registration information is sent to the authentication source. The barcode encoder **112** adapted for encoding and decoding barcode to extract authentication information. The credential generator **114** generates user credentials based on the preset inputs, which include time, location, login factors and etc. The key storage **116** stores the keys that are used to generate the user credential through credential generator **114**. The generated credential can be a one-time password (OTP) that are typically used as a secondary authentication factor. The key storage **116** stores all the keys generated for user authentication.

Over at the authentication source side, the application server comprises a network interface **118**, a user registration module **120**, key delivery module **122**, barcode decoder **124**, a login verification module **126** and a profile database **128**. The authentication server

106 also comprises a network interface **130**, a user registration module **132**, a key manager **134**, a credential verification module **136**, and a credential database **138**.

The application server **104** is connected to the authentication server **106** for activating user account and authenticating it after performing validation and verification of user credentials. It manages the creation and distribution of user's secret key to the user portable communication device **101**. The application server **104** and the authentication server **106** are network of servers or computers working in a coordinated manner, of which respective network interfaces **118** and **130** are adapted to connecting the two servers **104** and **106**.

The user registration module **120** is adapted to register user for mapping the same with the application user profile. The key delivery module **122** delivers user secret key generated by authentication server **106** to the user portable communication device **101**. Preferably, the secret key is delivered via a messaging channel, such as SMS gateway. The barcode decoder **124** is adapted for decoding a barcode or any matrix barcode for extracting authentication information. The barcode is transmitted from the user portable communication device **101**, of which the user portable communication device **101** optically obtains/captures the barcode from the portable communication device **100** via the visual channel. The login verification module **126** operationally validates user profile for authentication. These user profiles are stored on the profile database **128**.

The authentication server **106** uses its user registration module **132** to associate user with secret key generated. The key management module **134** generates and manages user secret key. The credential verification module **136** operationally validates the credential

submitted by user and the supplied user's credentials are stored on the credential database **138**.

Through the mobile application **108**, the user is able to carryout a user registration through the user registrations mobile on either the user portable communication device **101** or the portable communication device **100**. The user registration particulars, as mentioned, are sent to the authentication source. All the registered users are able to utilize the mobile application **108** to perform authentication with the authentication source.

FIG. 2 illustrates a schematic block diagram of a user device **200** in accordance with an embodiment of the present invention. The communication device **200** can be adapted on either one or both of the user portable communication device **101** and portable communication device **100** of **FIG. 1**. The user device **200** comprises a camera **202**, a display screen **204** and programs **206**. The camera **202** is facilitated as an optical means for scanning a barcode encoded with user authentication information or credential that is generated based on an input secret key. The display screen **204** on the other hand is used for displaying or showing the matrix barcode for scanning by the camera on the other communication device. The program **206** that comprises the mobile application **108** that operationally facilitates the user authentication process based on the key **208**.

FIG. 3 illustrates a sequence diagram of a user registration process in accordance with an embodiment of the present invention. The current figure is herein after described in conjunctions with the features of **FIG. 1**, though it is understood to a skilled person that the process can be adapted in different setup and configuration. The user registration process involves a user **302**, the communication device **100**, the user communication device **101**, the application server **104** and the authentication server **106** of **FIG. 1**. User registration process

is required for all new users who have not yet register with the authentication system. It is to be noted that the communication device **100** may be a portable device, or a desktop computer having a display screen and a camera.

At step **311**, the user **302** uses the communication device **100** to request for registration. The request is sent through the mobile application **108** to the application server **104** at step **312** through a communication network, such as Internet.

At step **314**, the application server **104** reverts with a registration form on a web browser on the communication device **100** to acquire necessary details from the user **302**. The registration form can be presented in a HTML form on a web browser and display on the communication device **100** to user **302** at step **313**. The details may include user personal particulars, registration number of the user communication device **101**, specifications of the user portable communication device **101** or other associated or required information therefor.

At step **315**, the user **302** enters all the required details on the form displayed on the communication device 100, and submits to the application server **104** at step **316**.

At step **318**, the application server **104** creates a user profile based on the details provided by the user. The user profile includes a user ID, among other information. The user ID may include the user's name, user's email address or registration number of the user communication device (such as IMEI, IMSI, and MSISDN).

At step **320**, the application server **104** forwards the user ID to the authentication server **106** for user registration.

At step **322**, the Authentication Server **106** generates a user secret key and associates the user secret key with the user ID. The user secret key is generated through applying cyptography function on a random data. The user ID and the associated user secret key are stored in the credential database **138** of the authentication server **106**.

At step **324**, the authentication server **106** sends the user secret key **208** to the application server **104**. At step **326**, the user secret key is being encrypted at the application server **104** through pre-arranged encryption key. Any open or proprietary encryptions may be used for such encryption, including but not limited to AES (Advanced Encryption Standard) or DES (Digital Encryption Standard), or any other suitable encryption methods.

At step **328**, the application server **104** delivers the encrypted user secret key to the user trusted mobile application **108** on the user portable communication device **101** via Short Message Service (SMS) as an activation SMS for validation of authentication process. This process is provided for establishing the ownership of the communication device **100**. As illustrated above, the trusted mobile application **108** is deployed as means for facilitating the authorization. It is adapted to receive the activation SMS, which allows the mobile application **108** to process the activation SMS. While processing the activation SMS, the mobile application **108** verifies the source of the SMS and the decrypts contents of the activation SMS. Specifically, the secret key will be recovered from the activation SMS and stored on the mobile device in a secured formed. The secret key may be protected for recovering therefrom through any one or more of the user password, device serialization and sensor input.

It is well known in the art that although the secret key stored on the key database is encrypted before sending to the device, user may opt for additional protection to secure the

secret key on the device. One of the most common protections is user password and pattern lock. In addition to the password, the mobile application may utilize some of the unique identities assigned to the device for protecting the secret key. These unique identities include a device serial number, Wi-Fi MAC address, and other unique number available to the device. Further, the device may also facilitate sensor for acquiring biometric of the user for protecting the secret key. These biometric may include audio, fingerprint, and etc.

At step **331**, the user is notified and at step **332**, the user **302** clicks on the trusted mobile application **108** on the user portable communication device **101**, and at step **334** the user communication device **101** generates a first credential (C1) by applying cryptographic techniques on the secret key and some input factors, such as time location, etc. The first credential C1 is then encoded to a 2-dimensional (2D) barcode as a security token. The barcode encoder **112** of the mobile application **118** is responsible for encoding the relevant information to the 2D barcode format. The barcode security token generated is then forwarded to the application server **104** using communication device **100** via visual channel **103** at step **336.** At step **337**, the barcode is decoded.

At step **338**, the application server **104** receives and decodes the 2D barcode security token to recover the User ID and user credentials C1. At step **340**, the user ID along with user credentials C1 are pushed to the authentication server **106** for credential authentication.

At step **342**, once the first user credentials C1 reach the authentication server **106** then the authentication server **106** looks up for the relevant user information by using the user ID. The authentication server **106** searches in its credential database **138** and retrieve

the user information stored in its database. At step **344**, the authentication server then generates a second user credential (C2) based on the user secret key for comparing the first user credentials C1. The secret key is processed with certain required factors, such as time, location and etc. to generate another credential for comparing with that in the one encoded in the barcode.

Once they are matched, at step **346**, the authentication server **106** informed the application server **104** of the authentication status. At step **348**, application server **104** activates the user account and confirmation is sent to the communication device **100** and in turn the user **302**. User may then use the communication device **100** to carry out authentication accordingly at step **350**.

The cryptographic or encryption/decryption techniques used may be, but not limited to, hashing, symmetric and asymmetric cryptography.

FIG. 4 illustrates an authentication process as the registered user **306** is accessing a secured website throught the application server **104** in accordance with an embodiment of the present invention.

At step **411**, the user **302** requests to access the secured website through the user communication device **100**. At step **412**, the communication device 100 connects to send the request to the application server **104**, which in some case, can be a proxy server for handing authentication. The application server **104** returns with a HTML pages at step **414** to request for user login credentials, the registered user ID and credential. At step **415**, the login page is displayed to the user **302**. The user **302** clicks the mobile application **108** to initiate the login process at step **416**. At step **418**, the mobile application **108** installed on

the user communication device 101 is used to generate a user credential based on user secret key and input factor such as time, location and etc. and applies with cryptographic function to encode the same into barcode as a security token.

At step **420**, the user communication device 100 captures or scans the barcode from the user communication device **101** via visual channel or any out-of-band channel, and send to the application server **104.** At step **422**, the application server 104 received the decoded barcoded. At step **424**, the application server **104** lookup for the corresponding user profile based on the recovered a first user credentials (C1). Once the user profile is identified, at step **426**, the user ID and credentials are sent to the authentication server **106** for credential validation.

At step **428**, once the first user credentials (C1) reach the authentication server **106**, the authentication server **106** looks up for the relevant user information. The authentication server **106** searches in its credential database **138** and retrieve the user information stored in its database. The authentication server **106** then generates the user secret key. The secret key is then processed with certainly required factors, such as time, location and etc. to generate another credential (C2) for comparing with that in the one encoded in the barcode.

Once they are matched, at step **432**, the authentication server **106** informed the application server **104** of the authentication status. At step **434**, application server **104** complete the authentication process and allowing the user to access the secured website, only when authentication server return a status of validation and comparison result showing both credentials are identical. At step 436, the user 302 is authenticated and allow to access.

It is well understood to a skilled person that the authentication method of the present invention may adapt any type of barcode that is designed so that reading and decoding is feasible and efficient using the built-in camera **202** and the computer power available in a portable communication device **100**. Examples of barcode may include Data matrix, QR code, Sema code or may other codes available.

The exemplary architecture **500** of the application server **104** and the authentication server **106** is as shown in **FIG. 5**. The application server **104** and the authentication server **106** include processor(s) **502**, Input - Output circuitry **504**, computer readable media, such as, but not limited to, memory **506**, and network interface (not shown). The application server **104** and the authentication server **106** may be connected to the portable communication device **100** via communication network **102**. The computer readable media **506** stores application program modules **508** and data **510**. Application program modules **508** contain instructions, which when executed by processor(s) **502**, cause the processor(s) **502** to perform actions of a method described herein in **FIG. 3** and **FIG. 4**.

The method described above with reference to **FIG. 3** and **FIG. 4** may be embodied on a computer program comprising computer programming codes for performing the server-side parts of the method when the computer program code is executed by a processor **502**, for instance embodied in any of the application server **104** and the authentication server **106** in **FIG. 1**. The method may also be embodied as executable instructions on a computer readable medium having stored there on a computer program comprising computer program code for performing the method when the computer program code is executed by a processor **502**. Again the processor **502** may, for instance, be embodied in any of the servers **104** or **106** as shown in **FIG. 1**. The computer readable

medium may, for instance, be memory **506** or any another plausible medium including, but not limited to, an optical disc (e.g. CD or DVD), a portable semiconductor memory (e.g. USB stick), a magnetic disc, or a file server accessible in a computer network such as the Internet.

Furthermore, the method described above with reference to **FIG. 3** and **FIG. 4** may also be embodied as a computer program, also known as app, comprising computer program code for performing the portable communication device **100** parts of the method when the computer program code is executed by a processor on the portable communication device **100**. The method may also be embodied as a computer readable medium having stored there on a computer program comprising computer program code for performing the method when the computer program code is executed by a processor in the portable communication device **100**. The computer readable medium may be any plausible medium including, but not limited to, an optical disc CD or DVD, a portable semi-conductor memory USB stick, a magnetic disc, or a file server accessible in a computer network such as the Internet.

The user device **100** on the other hand is equipped with a barcode scanner, which can be integrated or externally attached as an input peripheral, for capturing the barcode for carrying out the authentication. In one embodiment, the barcode is presented or outputted on a display unit of a separate device, which is also adapted to operationally communicate with the application server **104**.

In another embodiment, the barcode can be sent to the device seeking for the authentication itself, and once the barcode is received, the device seeking for the authentication may process the acquired barcode on the mobile application **108** as defined above.

In yet a further alternative, the barcode can be printed out in a physical medium, whereby the barcode can be scanned through the user device **100** to perform the authentication as described above.

The foregoing description of the specific embodiments will fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify and/or adapt for various applications such specific embodiments without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. Therefore, while the embodiments herein have been described in terms of preferred embodiments, those skilled in the art will recognize that the embodiments herein can be practiced with modification within the spirit and scope of the appended claims.

Although the embodiments herein are described with various specific embodiments, it will be obvious for a person skilled in the art to practice the disclosure with modifications. It is to be noted that invention is not limited to one communication device or one user, but can authenticate multiple users at one period of time. However, all such modifications are deemed to be within the scope of the claims.

Claims:

1. A method for mutually authenticating a user through a communication device to access a secured website, the method comprising:

registering the user with user profile and a registration number of the communication device with the authentication system;

requesting access to the secured website through the authentication system with the communication device;

rendering a barcode as a security token, the barcode containing user credentials is encoded based on a user secret key;

sending the barcode to the authentication system for decoding the user credential provided by the user upon requesting access; and

comparing the user credential provided by the user against a corresponding user credential stored on the authentication system.

2. The method of claim 1, wherein a barcode is generated on the user communication device (101) to request for authorization and another barcode is generated on the authentication system for matching the user credentials.

3. The method of claim 1, further comprises scanning the barcode through the user communication device (101) via a visual channel.

4. The method of claim 3, wherein scanninng the barcode comprises displaying the barcode on another communication device, wherein the barcode is rendered on a mobile application (108) deployed on the another communication device, and the barcode is

rendered based on the user secret key and the barcode include the user credentials sent from the authentication system.

5. The method of claim 1, wherein the barcode is use as the security token for authenting user registration and user access.

6. An authentication system for mutually authenticating a user through a communication device, the authentication system comprising:

an application server (104) in communication with the user portable communication device (101), the application server (104) has a database of user profiles that includes a user ID and a registration number of the user portable communication device (101),

an authentication server (106) for rendering a barcode encoded with a secret key that based on the user profiles;

a mobile application (108) for deploying on the user portable communication device, wherein the mobile application (108) operable to communicate with the application server (104) to facilitate user authentication;

wherein the system operationally authenticates the user through matching the user credential decoded from the barcode against a corresponding user credential stored on the authentication server (106).

7. The system according to claim 6, wherein the visual channel includes optical means for acquiring the barcode.

8. The system according to claim 6, wherein the barcode is displayed on another communication device device, wherein the barcode is rendered on a mobile application

(108) deployed on the another communication device, and the barcode is rendered based on the user secret key, and the barcode include the user credentials sent from the authentication server (106).

9. The system according to claim 6, wherein the barcode is a matrix barcode.

10. The system according to claim 6, wherein the barcode is a two-dimensional barcode, which include either planar or linear form barcode.

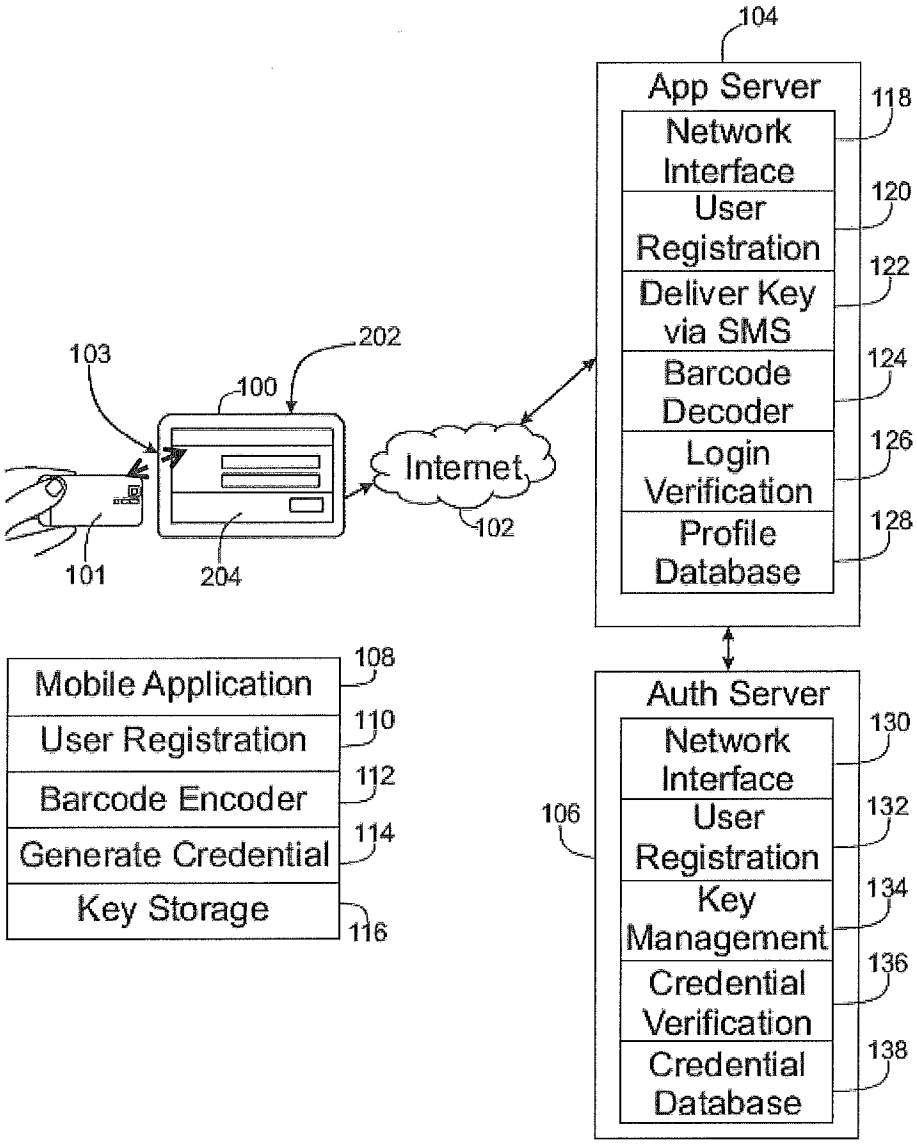
104
App Server
118
Network Interface
120
User Registration
122
Deliver Key via SMS
124
Barcode Decoder
126
Login Verification
128
Profile Database
103
202
100
Internet
102
101
204
Mobile Application
108
User Registration
110
Barcode Encoder
112
Generate Credential
114
Key Storage
116
Auth Server
106
130
Network Interface
132
User Registration
134
Key Management
136
Credential Verification
138
Credential Database

FIG. 1

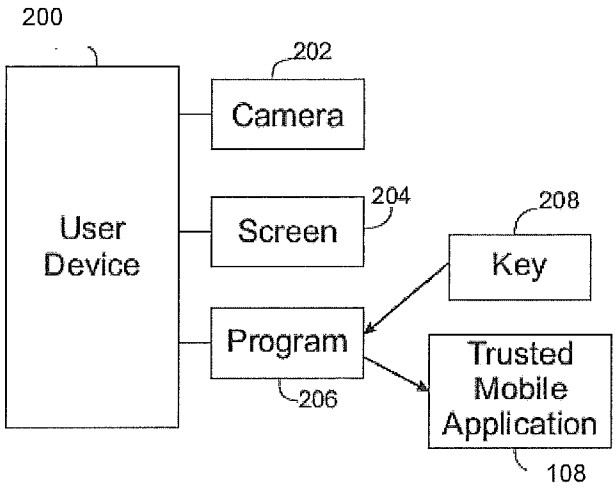
200
User Device
202
Camera
204
Screen
206
Program
208
Key
Trusted Mobile Application
108

FIG. 2

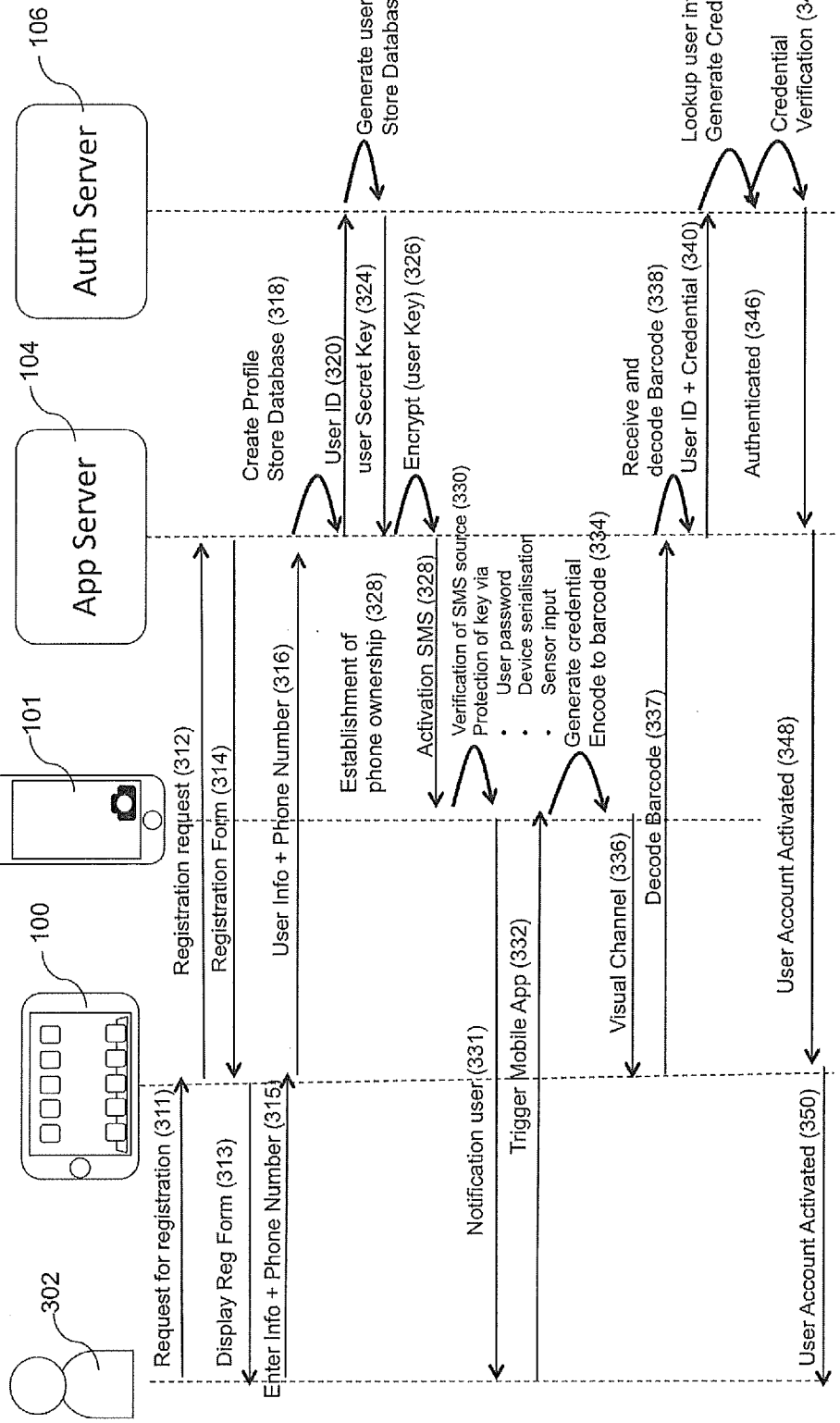
302
100
101
App Server
104
Auth Server
106
Request for registration (311)
Display Reg Form (313)
Enter Info + Phone Number (315)
Registration request (312)
Registration Form (314)
User Info + Phone Number (316)
Create Profile
Store Database (318)
User ID (320)
Generate user key
Store Database (322)
user Secret Key (324)
Encrypt (user Key) (326)
Establishment of
phone ownership (328)
Activation SMS (328)
Verification of SMS source (330)
Protection of key via
• User password
• Device serialisation
• Sensor input
Generate credential
Encode to barcode (334)
Notification user (331)
Trigger Mobile App (332)
Visual Channel (336)
Decode Barcode (337)
Receive and
decode Barcode (338)
User ID + Credential (340)
Lookup user info
Generate Credential (342)
Credential
Verification (344)
Authenticated (346)
User Account Activated (348)
User Account Activated (350)

FIG. 3

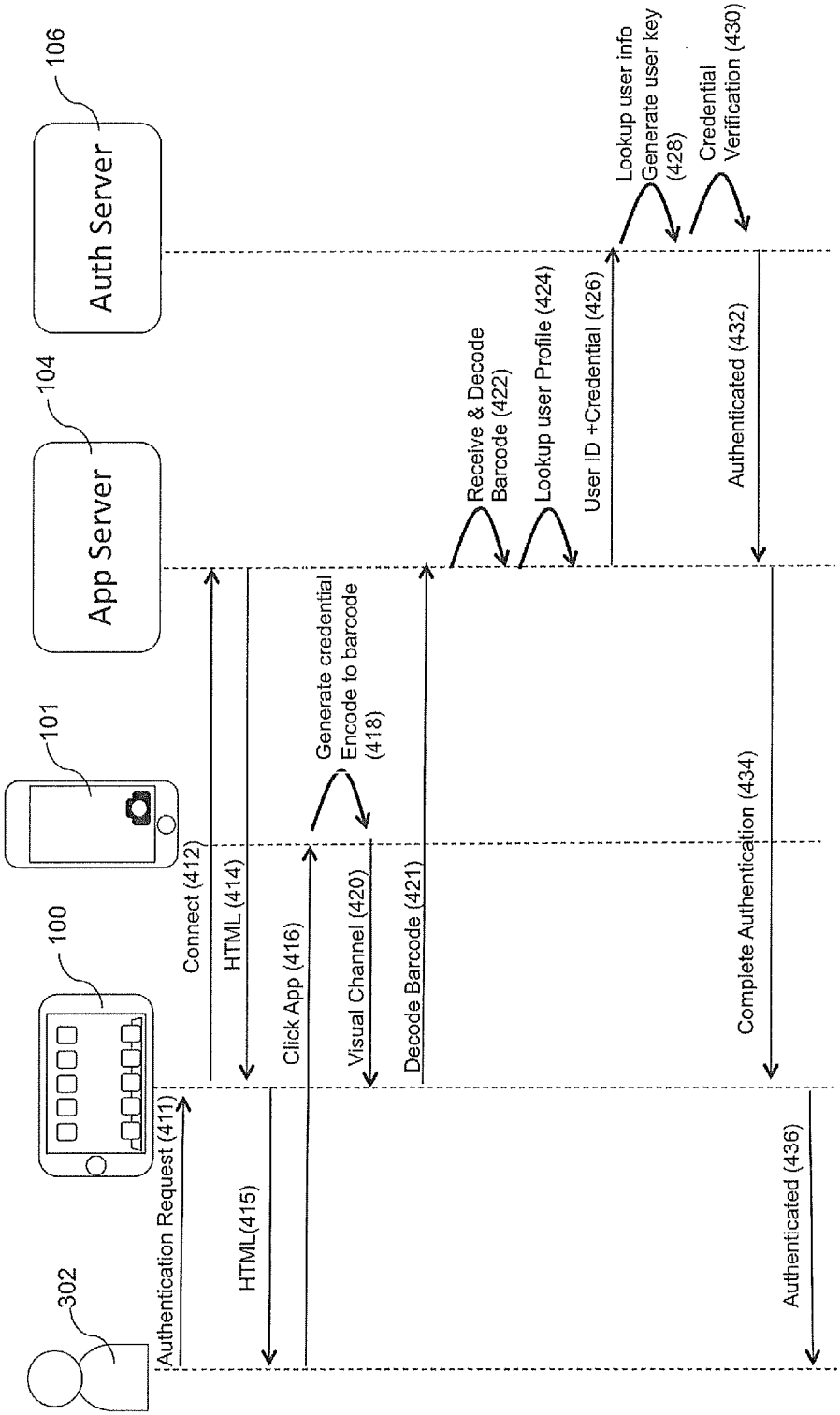
302
100
101
104
106
App Server
Auth Server
Authentication Request (411)
Connect (412)
HTML (414)
HTML(415)
Click App (416)
Generate credential
Encode to barcode
(418)
Visual Channel (420)
Decode Barcode (421)
Receive & Decode
Barcode (422)
Lookup user Profile (424)
User ID +Credential (426)
Lookup user info
Generate user key
(428)
Credential
Verification (430)
Authenticated (432)
Complete Authentication (434)
Authenticated (436)

FIG. 4

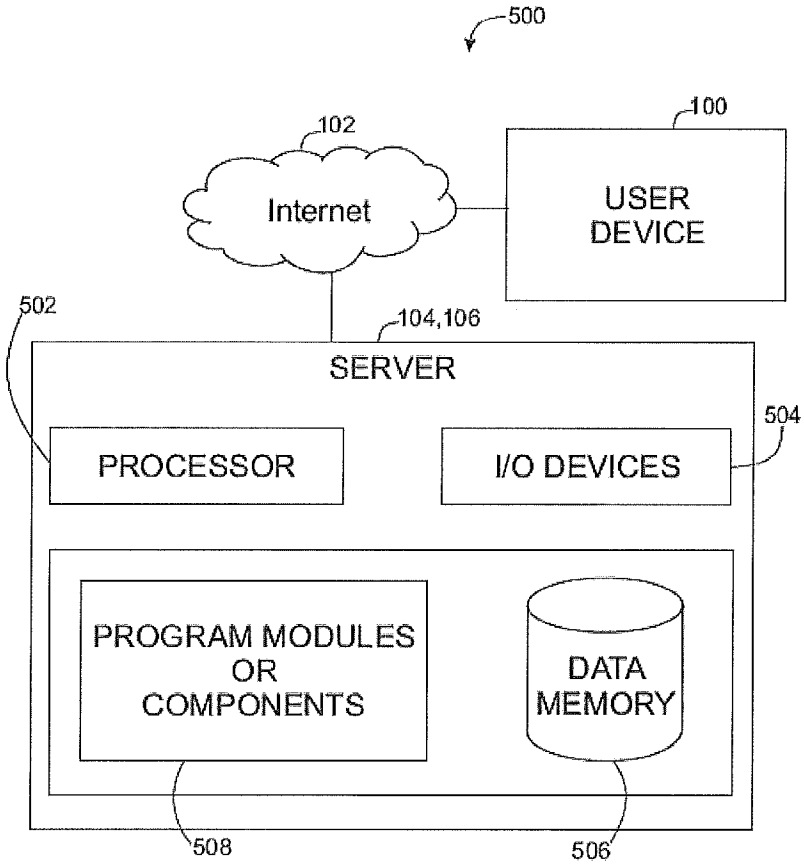
500
100
102
Internet
USER DEVICE
502
104,106
SERVER
504
PROCESSOR
I/O DEVICES
PROGRAM MODULES OR COMPONENTS
DATA MEMORY
508
506

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2015/050068

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04L 9/08(2006.01)i, G06K 7/14(2006.01)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)
H04L 9/32; G06F 15/16; G06T 11/00; G06Q 30/00; G06Q 20/22; H04L 9/00; G06F 21/00; H04L 9/08; G06K 7/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: barcode, mutual authentication, credential, token

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012-0240204 A1 (PIYUSH BHATNAGAR et al.) 20 September 2012 See paragraphs [0038]-[0049], [0053], [0055]; claim 25; and figures 1-5, 10.	1-10
A	US 2011-0219427 A1 (GENT HITE et al.) 08 September 2011 See paragraphs [0012]-[0020]; and figures 1, 2.	1-10
A	US 2013-0278622 A1 (NETSPECTRUM INC.) 24 October 2013 See paragraphs [0065]-[0091]; and figures 1-4.	1-10
A	US 2012-0089519 A1 (PRASAD PEDDADA) 12 April 2012 See paragraphs [0041], [0042]; and figures 3, 4.	1-10
A	US 2006-0088166 A1 (KIYOKO KARUSAWA) 27 April 2006 See paragraphs [0064]-[0095]; and figures 1-3.	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
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 December 2015 (14.12.2015)	**15 December 2015 (15.12.2015)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-472-7140

Authorized officer
KIM, Do Weon
Telephone No. +82-42-481-5560

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2015/050068

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0240204 A1	20/09/2012	US 8763097 B2	24/06/2014
US 2011-0219427 A1	08/09/2011	None	
US 2013-0278622 A1	24/10/2013	WO 2013-163217 A1	31/10/2013
US 2012-0089519 A1	12/04/2012	WO 2012-048015 A1	12/04/2012
US 2006-0088166 A1	27/04/2006	CN 100591009 C	17/02/2010
		CN 1764115 A	26/04/2006
		DE 602005026239 D1	24/03/2011
		EP 1650894 A1	26/04/2006
		EP 1650894 B1	09/02/2011
		JP 04736398 B2	27/07/2011
		JP 2006-121497 A	11/05/2006