



- (51) **International Patent Classification:**
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)
- (21) **International Application Number:**
PCT/MY2013/000125
- (22) **International Filing Date:**
5 July 2013 (05.07.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
PI 2012003210 13 July 2012 (13.07.2012) MY
- (71) **Applicant:** MIMOS BERHAD [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (72) **Inventors:** SEA Chong Seak; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). NG Kang Siong; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). GALOH Rashidah Haron; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). DHARMADHARSHNI Maniam; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). WONG Hon Loon; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).
- (74) **Agent:** MIRANDAH, Patrick; Patrick Mirandah Co. (Malaysia) Sdn Bhd, Suite 3B-19-3 Plaza Sentral, jalan Stesen Sentral 5, 50470 Kuala Lumpur (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, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

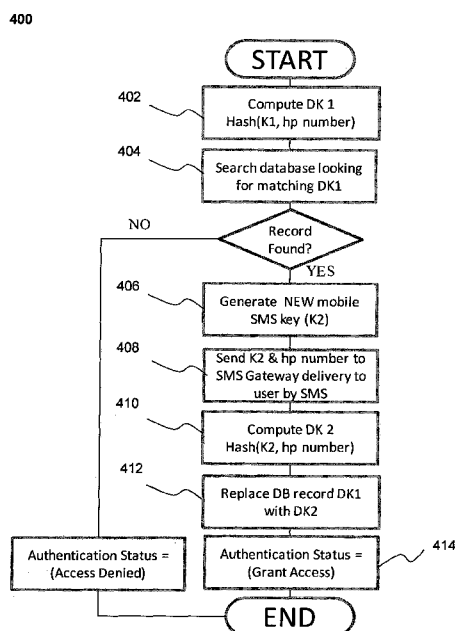
(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,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

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

[Continued on next page]

(54) **Title:** A SYSTEM AND METHOD FOR AUTHENTICATION USING NON-REUSABLE RANDOM GENERATED MOBILE SMS KEY



(57) **Abstract:** The system and method of the present invention proposes user authentication using non-reusable random generated mobile SMS key while retaining user privacy. The system of the present invention comprising at least one user (101) with user mobile phone (106); at least one web application (104); at least one authentication service provider (103); at least one authentication server (102); and at least one database (105). The at least one authentication server (102) further comprising at least one authentication interface module (201); at least one authentication verification module (202); at least one SMS key generation module (203); at least one SMS gateway (204); and at least one database interface module (205). The methodology of the present invention comprises steps of requesting user information for authentication (302); authenticating user information (304); returning authentication status to web application (310); and performing authorization by granting access to user upon successful user authentication (312). Authentication of user information comprises steps of computing hash value (DK1) based on user information (402); searching database for matching hash value (DK1) (404); and generating new mobile SMS key (K2) upon locating matching record in database (406) after mobile SMS key (K1) has been authenticated in the current transaction.



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))

A SYSTEM AND METHOD FOR AUTHENTICATION USING NON-REUSABLE RANDOM GENERATED MOBILE SMS KEY

FIELD OF INVENTION

5

The present invention relates to a system and method for authentication using non-reusable random generated mobile SMS key.

BACKGROUND ART

10

Authentication technologies that are widely used is online form-based authentication using username and password. It uses plaint-text password as credentials and send or forward the password directly on network to server for authentication. Therefore using basic authentication technologies without encryption will reveal any secret credentials to all eavesdroppers. Even with strongest SSL/TLS encryption, online plaintext passwords are vulnerable for man-in-the-middle attacks (web application layer) or called phishing attacks. In Form-based username and password authentication, it requires handling of user's password in a web application layer, which caused many users' password leakage accidents in many commercial and financial web sites.

20

To prevent leakage of reusable weak secret password and some application use unencrypted public channels to forward user's credentials over the network, there is a need to place a strongest protection on authentication credentials and token.

25

One of the solutions would be by using the One time password device, but the device could be costly to deploy due to extra cost required for one time password device (for each users) and software license needed for one time password server. The current OTP system requires synchronization management to manage the synchronization of a token for a specified user or token number, since the current time based OTP very sensitive to time. Complexity of user management between OTP token and user causes lack of user privacy options.

30

The present invention proposes user authentication method to application using non-reusable random generated mobile Short Message System (SMS) Key while retaining user privacy.

35

In the case user needs to access the application website, the website redirects user to authentication server. User must enter user mobile phone number and mobile SMS key (K1) which is retrieved from user mobile via SMS message which was sent by the authentication server. Authentication Server generates hash value which is combination
5 information from user and K1. The hash value is use to search for matching hash value between records in the database If record is found, Authentication server will grant access to the user otherwise authentication server will set the status to "Access Denied" and terminate the authentication process. Upon successful authentication of user, the system will generate new mobile SMS key (K2). Authentication server sends this new
10 generated mobile SMS key (K2) to SMS gateway. Thereafter, the gateway will forward K2 to user for next login INPUT mobile SMS key. Authentication server then computes hash value based on information of user entering mobile phone and K2. Current database record will be replaced with this new generated hash value. The approach of the present invention is to retain user privacy based on authentication using non-
15 reusable random generated mobile SMS key.

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area
20 where some embodiments described herein may be practice.

SUMMARY OF INVENTION

The present invention provides a system and method for authentication using non-reusable random generated mobile SMS key while retaining user privacy. The system comprising at least one user (101) with user mobile phone (106); at least one web application (104); at least one authentication service provider (103); at least one authentication server (102); and at least one database (105). The at least one authentication server (102) further comprising at least one authentication interface module (201); at least one authentication verification module (202); at least one SMS key generation module (203); at least one SMS gateway (204); and at least one database interface module (205). The at least one SMS key generation module (203) having means to generate new mobile SMS key (K2); said new mobile SMS key (K2) is a random number; said random number is a non-reusable mobile SMS key for next login to web application after mobile SMS key (K1) has been authenticated in the current transaction.

The at least one authentication service provider (103) having means to protect web application site from unauthorized user access while the at least one authentication interface module (201) is an interface to other components of the system; said authentication interface module request user information for authentication.

Another aspect of the present invention is the at least one authentication verification module (202) which performs user credential verification by computing hash value (DK1) based on user information and searching database for matching hash value (DK1) to determine successful user authorization in the current transaction. The at least one SMS gateway (204) forwards new mobile SMS key (K2) to user via SMS for next login to web application while the at least one database interface module (205) is a module interface to database for retrieving, inserting and updating user information stored in database.

A further aspect of the present invention is a method (300, 400) for authentication using non-reusable random generated mobile SMS key. The method comprising steps of requesting user information for authentication (302); authenticating user information (304); returning authentication status to web application (310); and performing authorization by granting access to user upon successful user authentication (312). The method for authenticating user information comprises steps of computing hash value

(DK1) based on user information (402); searching database for matching hash value (DK1) (404); and generating new mobile SMS key (K2) upon locating matching record in database (406). The method for requesting user information for authentication further requires user to enter user mobile phone number and mobile SMS key (K1) (306).

5

A further aspect of the present invention is the method for generating new mobile SMS key (K2) upon locating matching record. The said method further comprises steps of forwarding new mobile SMS key (K2) to user via SMS (408); computing hash value (DK2) by hashing newly generated mobile SMS key (K2) with user mobile phone number (410); and replacing database record containing hash value (DK1) with hash value (DK2) (412). The said new mobile SMS key (K2) is a random number; which is a non-reusable mobile SMS key for next login to web application.

10

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

15

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific
5 embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1.0 illustrates the component integration diagram of the present invention.

FIG. 2.0 illustrates the five major modules of the Authentication Server of FIG.1.0.

FIG. 3.0 is a flowchart illustrating a method for authentication using non-reusable
15 random generated mobile SMS key.

FIG. 4.0 is a flowchart illustrating a further method for authentication of user information of the present invention.

20 FIG. 5.0 illustrates the overall system architecture of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for authentication using non-reusable random generated mobile SMS key while retaining user privacy. Hereinafter, this specification will describe the present invention according to the preferred
5 embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

10 Reference is first being made to FIG. 1.0, FIG. 2.0 and FIG. 5.0 respectively. FIG. 1.0 illustrates the component integration diagram of the present invention while FIG. 2.0 illustrates the five major modules of the Authentication Server of FIG.1.0 and FIG. 5.0 illustrates the overall system architecture of the present invention. As illustrated in FIG. 1.0, the present invention comprising at least one user (101) with user mobile phone
15 (106); at least one web application (104); at least one authentication service provider (103); at least one authentication server (102); and at least one database (105). As illustrated in FIG. 2.0, the at least one authentication server (102) further comprising at least one authentication interface module (201); at least one authentication verification module (202); at least one SMS key generation module (203); at least one SMS gateway
20 (204); and at least one database interface module (205).

The system and method for authentication using non-reusable random generated mobile SMS key begins with the authentication service provider (101). The at least one authentication service provider (103) having means to protect web application site from
25 unauthorized user access wherein the authentication service provider (103) will direct user to authentication server (102) for authentication. Thereafter, the authentication interface module (201) which is an interface to other components of the system will request user information for authentication. The system of the present invention also comprises of at least one authentication verification module (202) that performs user
30 credential verification by computing hash value (DK1) based on user information and searching database for matching hash value (DK1) to determine successful user authorization in the current transaction.

Reference is now being made to FIG. 3.0 and FIG. 4.0 respectively. FIG. 3.0 is a
35 flowchart illustrating a method for authentication using non-reusable random generated

mobile SMS key and FIG. 4.0 is a flowchart illustrating a further method for authentication of user information of the present invention. The said methodology begins with the system requesting user information for authentication (302) wherein user is required to enter user mobile phone number and mobile SMS key. Thereafter, authentication server will authenticate user information (304). Authentication of user information further comprises steps of computing hash value (DK1) based on user information (402); searching database for matching hash value (DK1) (404); and generating new mobile SMS key (K2) upon locating matching record in database (406). The new mobile SMS key (K2) is a random number generated by the at least one SMS key generation module (203) of the present invention. The said random number is a non-reusable mobile SMS key for next login of user to web application while retaining user privacy after mobile SMS key (K1) has been authenticated in the current transaction.

Upon generating the new mobile SMS key (K2), SMS gateway (204) forwards new mobile SMS key (K2) to user via SMS for next login to web application (408). Thereafter, hash value (DK2) is computed by hashing newly generated mobile SMS key (K2) with user mobile phone number (410) and database record containing hash value (DK1) is replaced with hash value (DK2) (412). The at least one database interface module (205) is a module interface to database for retrieving, inserting and updating user information stored in the database of the present invention.

As illustrated in FIG. 3.0, upon successful authentication of user information; authentication status is returned to web application (310) wherein user is granted authentication (i.e. access is granted to user) when matching hash value (DK1) is found in the database (414). Else, user access is denied when there is no matching hash value (DK1) in the database.

The system and method of the present invention provides for authentication using non-reusable random generated mobile SMS key. User privacy is retained as the newly generated mobile SMS key (K2) is a random number and is a non-reusable mobile SMS key for next login to web application.

The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all

respects only as illustrative and not restrictive. The scope of the invention is, therefore indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A system (100) for authentication using non-reusable random generated mobile SMS key with at least one user (101) and user mobile phone (106) on at least one web application (104) with at least one authentication service provider (103) to protect web application site from unauthorized user access; at least one authentication server (102); and at least one database (105);

the at least one authentication server (102) further comprising:

at least one authentication interface module (201) is an interface to other components of the system; said authentication interface module request user information;

at least one authentication verification module (202) performs user credential verification by computing hash value (DK1) based on user information and searching database for matching hash value (DK1) to determine successful user authorization in the current transaction;

at least one SMS key generation module (203);

at least one SMS gateway (204); and

at least one database interface module (205)

characterized in that

the at least one SMS key generation module (203) having means to generate new mobile SMS key (K2); said new mobile SMS key (K2) is a random number; said random number is a non-reusable mobile SMS key for next login to web application after mobile SMS key (K1) has been authenticated in the current transaction.

2. A system (102) according to Claim 1, wherein the at least one SMS gateway (204) forwards new mobile SMS key (K2) to user via SMS for next login to web application.

3. A system (102) according to Claim 1, wherein at least one database interface module (205) is a module interface to database for retrieving, inserting and updating user information stored in database.

4. A method (300, 400) for authentication using non-reusable random generated mobile SMS key; the method comprising steps:

requesting user information for authentication (302);
authenticating user information (304);
returning authentication status to web application (310); and
performing authorization by granting access to user upon successful user
authentication (312)

characterized in that

authenticating user information further comprises steps:

computing hash value (DK1) based on user information (402);
searching database for matching hash value (DK1) (404); and
generating new mobile SMS key (K2) upon locating matching
record in database (406) after mobile SMS key (K1) has been
authenticated in the current transaction wherein generating new
mobile SMS key (K2) upon locating matching record further
comprises steps:

forwarding new mobile SMS key (K2) to user via SMS
(408);

computing hash value (DK2) by hashing newly generated
mobile SMS key (K2) with user mobile phone number
(410); and

replacing database record containing hash value (DK1)
with hash value (DK2) (412).

5. A method according to Claim 4, wherein requesting user information for
authentication further requires user to enter user mobile phone number and
mobile SMS key (K1) (306).

6. A method according to Claim 4, wherein generating new mobile SMS key (K2)
upon locating matching record; said new mobile SMS key (K2) is a random
number; said random number is a non-reusable mobile SMS key for next login to
web application.

1/4

100

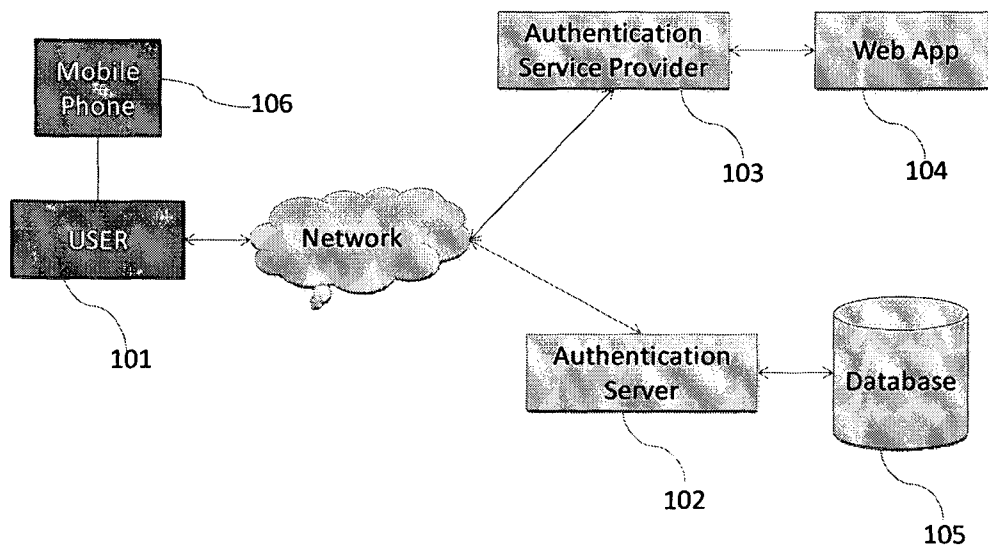


FIG. 1.0

200

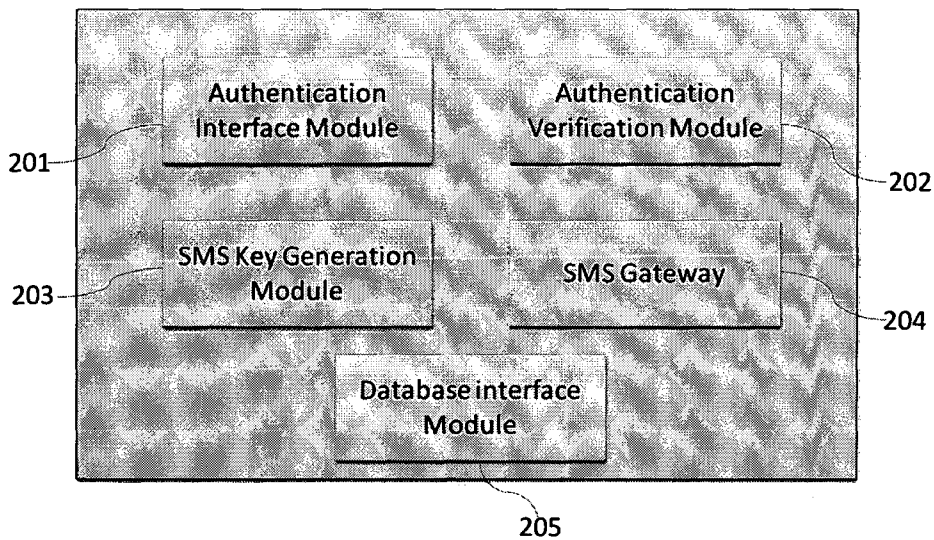


FIG. 2.0

2/4

300

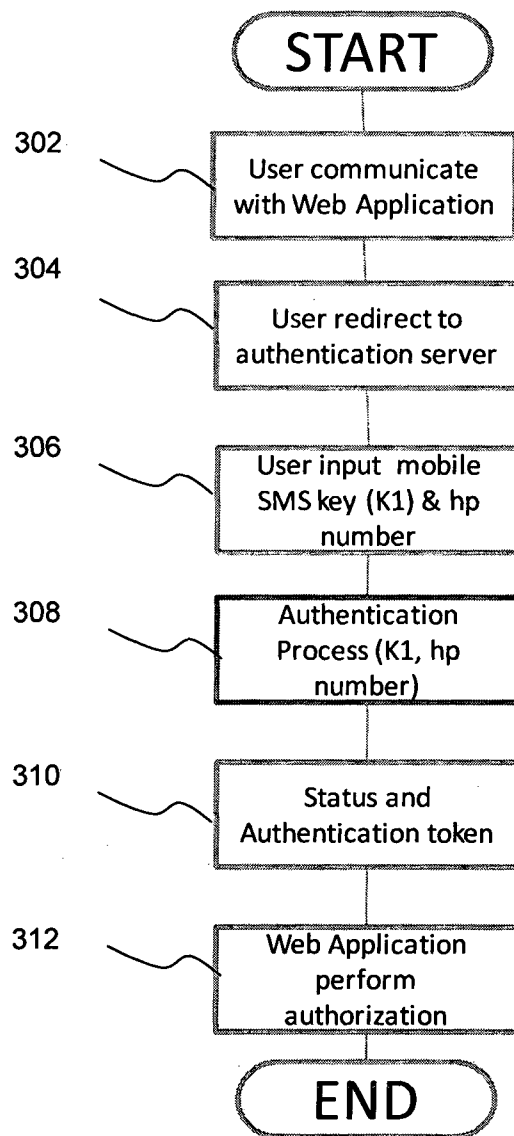


FIG. 3.0

3/4

400

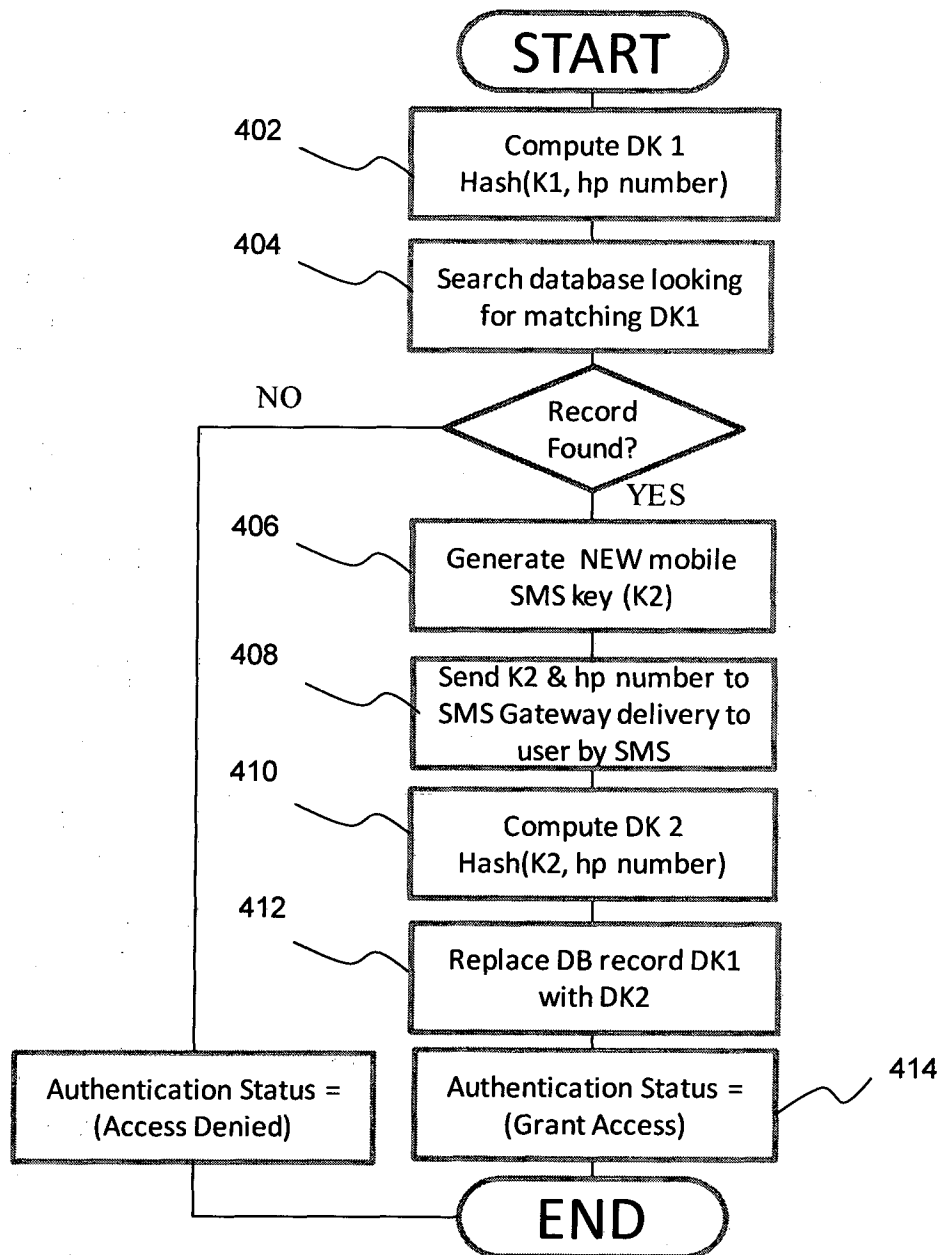


FIG. 4.0

4/4

500

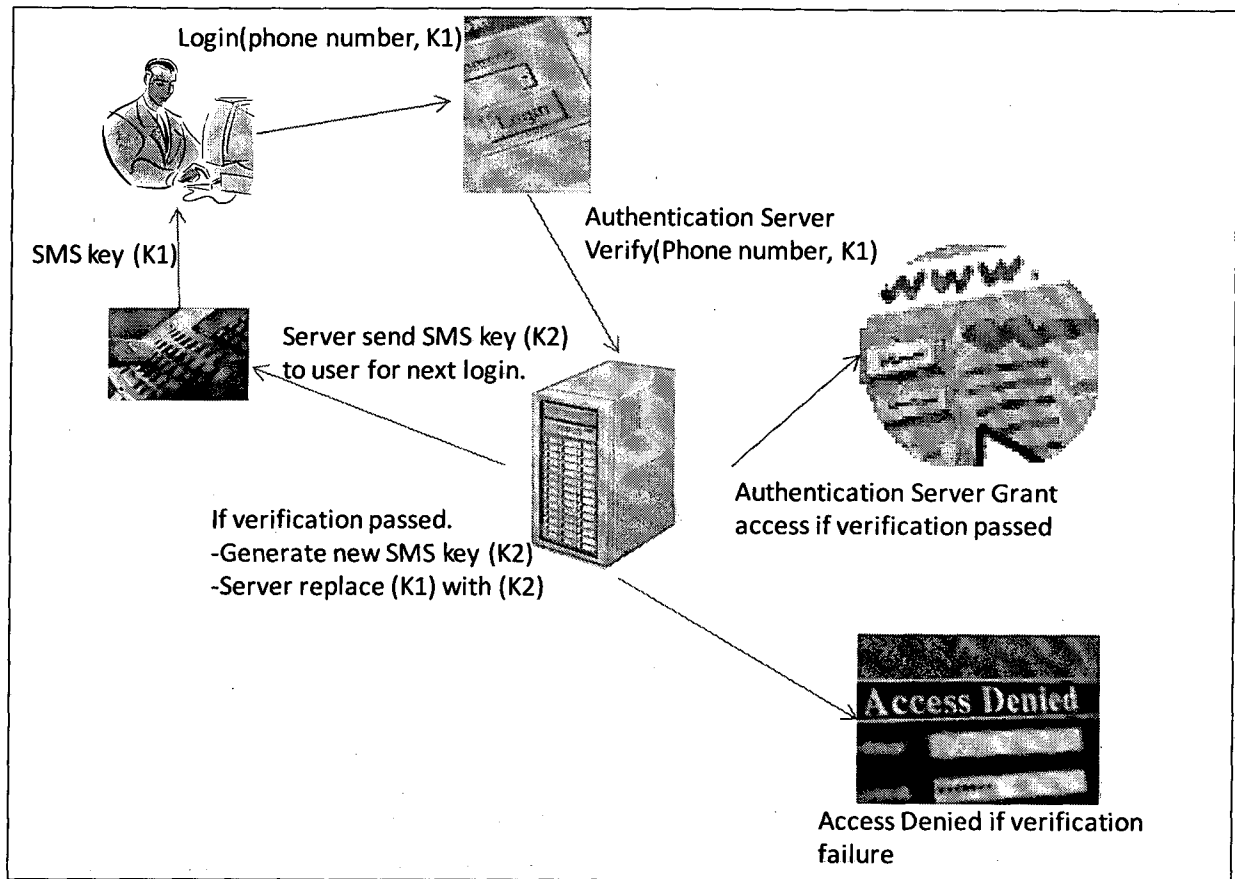


FIG. 5.0

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2013/000125

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04W G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2008/033065 A1 (COMFACT AB [SE]; TOERNQVIST ANDERS [SE]) 20 March 2008 (2008-03-20) figures 1,2 page 6 - page 8 -----	1-3

☐

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

24 October 2013

Date of mailing of the international search report

04/11/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Lamelas Polo, Yvan

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/MY2013/000125

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008033065	A1	20-03-2008	
		AU 2007295134 A1	20-03-2008
		CA 2663256 A1	20-03-2008
		CN 101512576 A	19-08-2009
		EP 2062209 A1	27-05-2009
		US 2009319797 A1	24-12-2009
		WO 2008033065 A1	20-03-2008
