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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2012 (21.06.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/081968 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/MY2011/000163

(22) International Filing Date:
30 June 2011 (30.06.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2010005982 15 December 2010 (15.12.2010) MY

(71) Applicant *(for all designated States except US)*: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MEILANA Siswanto** [ID/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **GUNAWAN Witjaksono** [ID/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ZHARFAN Hamdan** [MY/MY]; 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, 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, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG,

[Continued on next page]

(54) Title: A SYSTEM AND METHOD FOR QUANTUM MOBILE ACCESS VERIFICATION

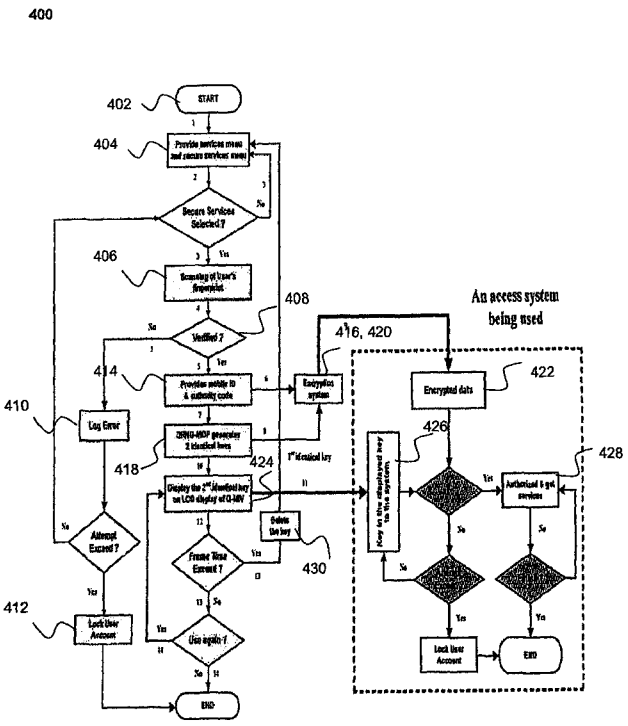

FIG. 4

(57) Abstract: The present invention provides a system (100) for Quantum Mobile Access Verification (Q-MAV) that generates true random identical keys for encryption and decryption of data streaming. The system (100) comprises at least one Quantum Random Number Generator (QRNG) with at least one Multi Output Processor (MOP) (106); at least one Encrypted storage (102); at least one biometric system (101); at least one Encryption system (107); and at least one display system (104), characterized in that the at least one QRNG with at least one MOP (106) generates true random identical keys, known as truly random independent-identical keys or i2 keys, for encryption and decryption of data streaming wherein first key is used to encrypt hardware identification of Q-MAV and authority code, and second key is used to decrypt encrypted data that has been sent, to an access system.

WO 2012/081968 A1

ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, 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))*

Published:

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

A SYSTEM AND METHOD FOR QUANTUM MOBILE ACCESS VERIFICATION

FIELD OF INVENTION

The present invention relates to a system and method for Quantum Mobile Access Verification (Q-MAV) that functions in a variety of verification-authentication processes.

BACKGROUND ART

Increased security features are necessary for securing, for example, buildings, computers, and mobile phones. Conventionally, security systems require static key that requires users to memorize their key or use a random key that is generated by a Random Number Generator (RNG). However, hacking tools, such as, cloning, brute force, phishing, and skimming, make the use of a static key that is susceptible to cracking or theft, which leads to misuse by unauthorized users. Further, the use of a random key based on RNG, which does not have a truly random output.

In the system of the present invention, an authorized biometric-fingerprint identity is recorded from a user of a known identity and stored in the encrypted storage and tampered proof for future reference. The default operation of the device is similar to a mobile phone with additional security features.

The approach and methodology in the present invention satisfies the need of security systems such as secure lock door access, secure computer or laptop access and secure system access verification means using QRNG-MOP which generates true random of independent-identical keys (i2 keys).

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 where some embodiments described herein may be practice.

SUMMARY OF INVENTION

The present invention provides a system (100) for Quantum Mobile Access Verification (Q-MAV) that generates true random identical keys for encryption and decryption of data streaming. The system (100) comprises at least one Quantum Random Number Generator (QRNG) with at least one Multi Output Processor (MOP) (106); at least one encrypted storage (102); at least one biometric system (101); at least one Encryption system (107); and at least one display system (104), characterized in that the at least one QRNG with at least one MOP (106) generates true random identical keys, known as truly random independent-identical keys or i2 keys, for encryption and decryption of data streaming wherein first key is used to encrypt hardware identification of Q-MAV and authority code, and second key is used to decrypt encrypted data that has been sent to an access system.

Preferably, the said display is part of mobile device and displays second i2 key. The said i2 keys are used multiple times and are deleted after several attempts for accessing system.

Further, the said encryption system (107) is One Time Pad (OTP) encryption system wherein one bit of key is needed for each data to be encrypted and the said decryption system is decrypted using i2-keys that are changed automatically after every use, wherein the said keys are dynamic, random, and genuinely issued for each verification.

Another aspect of the present invention is a method (400) for generating true random identical keys for encryption and decryption of data streaming. Q-MAV system is first activated (402). Thereafter, at least one secure service and at least one un-secure service is displayed at display of Q-MAV (404). Users fingerprint is scanned if secure service is chosen by user (406) and users fingerprint identify is verified by Q-MAV system (408). Subsequently, log error is displayed and several means is provided to attempt if verification process is unsuccessful (410) and users account is locked when number of attempts is exceeded wherein Q-MAV will function as mobile phone device (412). Hardware identification or Q-MAV and authority code is provided if verification was verified (414) and hardware identification and authority code is sent to encryption system (416). Truly random independent-identical keys, i2-keys is generated as PIN

numbers by QRNG-MOP (418) and hardware identification and authority code is encrypted using first i2-key (420). Thereafter, encrypted data streaming is sent to access system being used via transmitter channel means (422); second i2-key is displayed on display system of Q-MAV system (424) and second i2-key is inserted into access system used to decrypt encrypted data streaming (426). Subsequently, authorization from access system is obtain if decryption process is successful or the key is validated (428) and key is deleted if time frame is exceeded wherein the time frame is determined based on user's preference (430).

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.

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 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 where:

Fig. 1 illustrates internal architecture of Q-MAV system and its components.

Fig. 2 illustrates external architecture of Q-MAV system and its components.

Fig. 3 illustrates communication of Q-MAV system to any secure access system.

Fig. 4 is a flowchart illustrating method for generating true random identical keys for encryption and decryption of data streaming.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for Quantum Mobile Access Verification (Q-MAV) that functions in a variety of verification-authentication processes. Hereinafter, this specification will describe the present invention according to the preferred 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.

Reference is first being made to Figs. 1 and 2 respectively. Fig. 1 illustrates internal architecture of Q-MAV system that is secure mobile communication based on quantum random number generator (QRNG) with multi output processor (MOP), which can be functioned for multi purposes of access system verification-authentication means while Fig. 2 illustrates external architecture of Q-MAV system. As illustrated in Fig. 1 and Fig. 2 respectively, the said Q-MAV system comprises at least one Quantum Random Number Generator (QRNG) with at least one Multi Output Processor (MOP) (106), at least one encrypted storage (102) to store authorized users finger print sample for verification reference, at least one biometric system (101) which represents biometric scanner to scan users finger print to provide secure service, at least one encryption system (107) and at least one display system (104) to display pin number. Other components (103) can be added since only basic minimum components are been described in internal architecture of Q-MAV system.

The said display system (104) displays secure and unsecure services menu and second generated identical key while micro-processor system (105) acts as controller for all components. Quantum random number generator (QRNG) with MOP (106) acts as key generator which will generate truly random independent-identical keys (i2-keys) for encryption and decryption of data streaming wherein first key is used to encrypt hardware identification of Q-MAV and authority code, and second key is used to decrypt encrypted data that has been sent to access system.

The said encryption system (107) is One Time Pad (OTP) encryption system wherein one bit of key is needed for each data to be encrypted while decryption system is

decrypted using i2-keys that are changed automatically after every use as the said keys are dynamic, random and genuinely issued for verification. Transmitter channel (108) and antenna (110) acts as an interface to communicate with external access systems as provided in Q-MAV system.

The said biometric system (101) includes fingerprint scanner and is able to scan fingerprints. Mobile device display (104) is part of mobile device system wherein it displays second i2 key; i2 keys are used multiple times and i2 keys are deleted after several attempts for accessing system. The said encrypted storage (102) is encrypted using any encryption means and is tamper proof.

Reference is now made to Fig. 3. Fig. 3 illustrates communication of Q-MAV system to any secure access system. The said Q-MAV system is capable of communicating to any secure access systems such as secure door lock access, secure computer or laptop access, and other secure equipment physical access systems means using some kinds of connections (*i.e*, wired, wireless, or no connection to communicate with third party or a head quarter).

The present invention focuses only on communication between Q-MAV with secure access systems. Communication between access parties to third parties or their headquarters with its policy requirements is beyond of the scope of the present invention.

Reference is now made to Fig. 4. Fig. 4 is a flowchart illustrating method for generating true random identical keys for encryption and decryption of data streaming. As illustrated in Fig. 4, Q-MAV system is first activated (402). At least one secure service and at least one un-secure service is displayed at display of Q-MAV (404). User needs to select secure service and scan user's fingerprint on biometric system of Q-MAV system (406). Device will functioned as normal mobile phone if secure service is not selected.

Thereafter, users scanned fingerprint will be verified with stored authorized users data reference in Q-MAV system (408). Q-MAV will provide and send its hardware ID and authority code to encryption system if scanned user's fingerprint matches stored authorized user's data reference (414). QRNG-MOP will be activated to generate two

identical keys. If verification fails, Q-MAV system display log error (410) and return to secure services menu until failed attempts have exceeded, then the system will block users account wherein Q-MAV will functioned as mobile phone device (412). Subsequently, hardware identification and authority code is sent to encryption system (416) and QRNG- MOP generates truly random independent-identical keys (418). The two identical keys generated are truly random of independent-identical keys (i2-keys). It is generated by QRNG-MOP as PIN numbers which is first identical key and second identical key. The said first identical key will be used to encrypt Q-MAV's hardware identification (ID) and authority code using One Time Pad (OTP) encryption method (420). Thereafter, the encrypted streaming data will be sent to an access system being used via a transmitter channel (422).

Second identical key will be displayed at display of Q-MAV system, wherein user is required to decrypt the encrypted streaming data by keying-in the appeared key on the display of Q-MAV system to the access system being used (424). Displayed key can be used several times or for several accesses within time frame, if exceeded, displayed key will be deleted and Q-MAV will function as mobile phone. This security protocol is used to avoid misused of the authorization by non-authorized users. Second i2-key is inserted into access system used to decrypt encrypted data streaming (426). Thereafter, authorization is obtained from access system if decryption process is successful or when key is validated (428).

If both keys are matched, an authorized user is able to access system within the time frame. If the time frame has exceeded, the access system will end the process by deleting key as time frame is determined based on users preference (430) and the process will restart at secure services menu. If both keys are not matched, system will provide log error and return to secure services menu until failed attempts have exceeded. Thereafter, the system will block the user's account. The numbers of failed attempts depends on third parties rule or specification.

The system and methodology of the present invention provides for independent-identical keys (i2-keys) generated by QRNG-MOP wherein the mobile device system transmits encrypted streaming data which consists of hardware identification and authority code.

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 Quantum Mobile Access Verification (Q-MAV) that generates true random identical keys for encryption and decryption of data streaming, comprising:

   at least one Quantum Random Number Generator (QRNG) with at least one Multi Output Processor (MOP) (106);

   at least one encrypted storage (102);

   at least one biometric system (101);

   at least one Encryption system (107); and

   at least one display system (104),

   characterized in that the at least one QRNG with at least one MOP (106) generates true random identical keys, known as truly random independent- identical keys or i2 keys for encryption and decryption of data streaming wherein first key is used to encrypt hardware identification of Q-MAV and authority code, and second key is used to decrypt encrypted data that has been sent to access system.

2. A system (100) according to Claim 1, wherein biometric system is fingerprint scanner.

3. A system (100) according to Claim 1, wherein i2 keys are used multiple times.

4. A system (100) according to Claim 1, wherein encrypted data is sent via transmitter channel.

5. A system (100) according to Claim 1, wherein display system is part of mobile device.

6. A system (100) according to Claim 1, wherein display system displays second i2 key.

7. A system (100) according to Claim 1, wherein i2 keys are deleted after several attempts for accessing system.

8. A system (100) according to Claim 1, wherein encrypted storage (102) is encrypted using any encryption means and is tamper proof.

9. A system (100) according to Claim 1, wherein biometric system (101) is able to scan fingerprints.

10. A system (100) according to Claim 1, wherein encryption system (107) is One Time Pad (OTP) encryption system wherein one bit of key is needed for each data to be encrypted.

11. A system (100) according to Claim 1, wherein decryption system is decrypted using i2-keys that are changed automatically after every use, the said keys are dynamic, random, and genuinely issued for each verification.

12. A system (100) according to Claim 1, wherein Q-MAV system has at least a time frame to maintain the key or without a time frame based on security level of mobile device.

13. A system (100) as claimed in Claim 1, wherein Q-MAV system is implemented in hardware system and device-based access verification.

14. A method (400) for generating true random identical keys for encryption and decryption of data streaming comprising steps of:

activating Q-MAV system (402);

displaying at least one secure service and at least one un-secure service at display of Q-MAV (404);

scanning users finger print, if secure service is chosen by user (406);

verifying users fingerprint identify by Q-MAV system (408);

displaying log error and providing means to attempt for several times if verification process is unsuccessful (410);

locking users account when number of attempts is exceeded wherein Q-MAV will function as mobile phone device (412);

providing hardware identification or Q-MAV and authority code, if verification was verified (414);

sending hardware identification and authority code to encryption system (416);

generating truly random independent-identical keys, i2-keys as PIN numbers by QRNG-MOP (418);

encrypting hardware identification and authority code using first i2-key (420);

sending encrypted data streaming to access system being used via transmitter channel means (422);

displaying second i2-key on display system of Q-MAV system (424);

inserting second i2-key into access system used to decrypt encrypted data streaming (426);

obtaining authorization from access system if decryption process is successful or the key is validated (428); and

deleting key if time frame is exceeded wherein the time frame is determined based on user's preference (430).

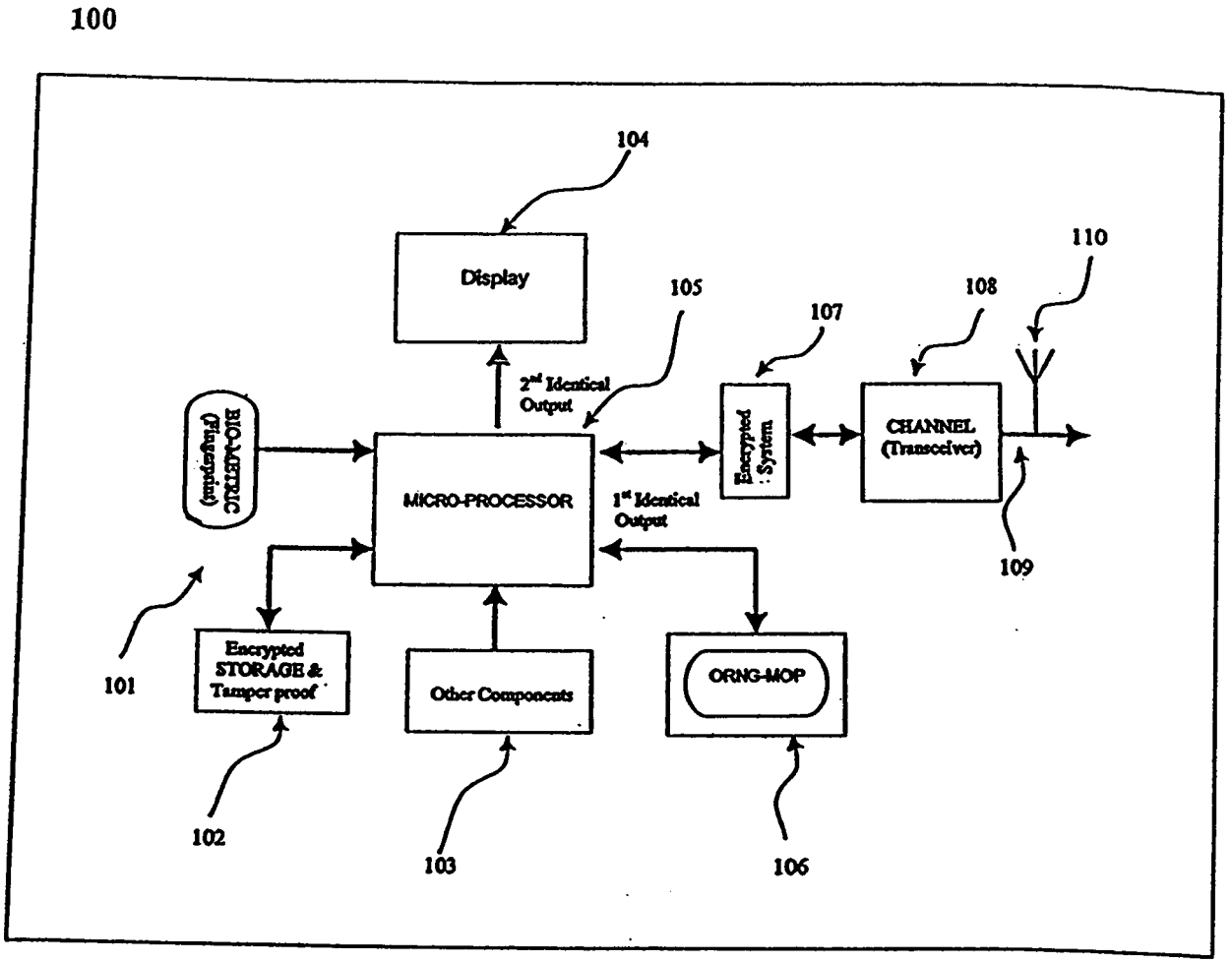
100
104
Display
105
107
108
110
2nd Identical Output
BIO-METRIC (Fingerprint)
MICRO-PROCESSOR
1st Identical Output
Encrypted System
CHANNEL (Transceiver)
109
101
Encrypted STORAGE & Tamper proof
Other Components
ORNG-MOP
102
103
106

FIG. 1

200

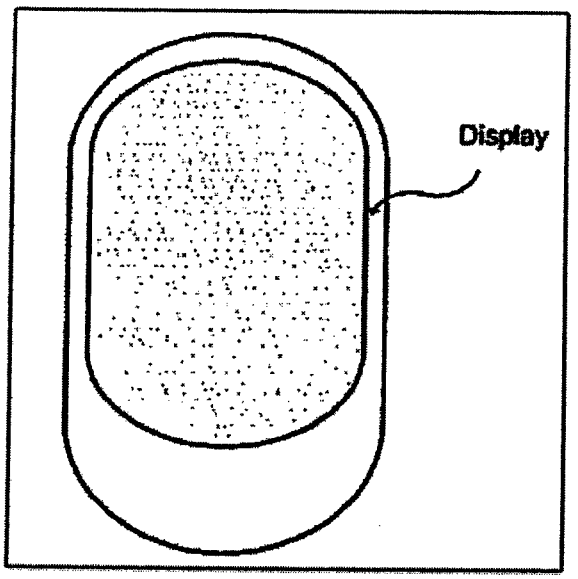

FIG. 2

300

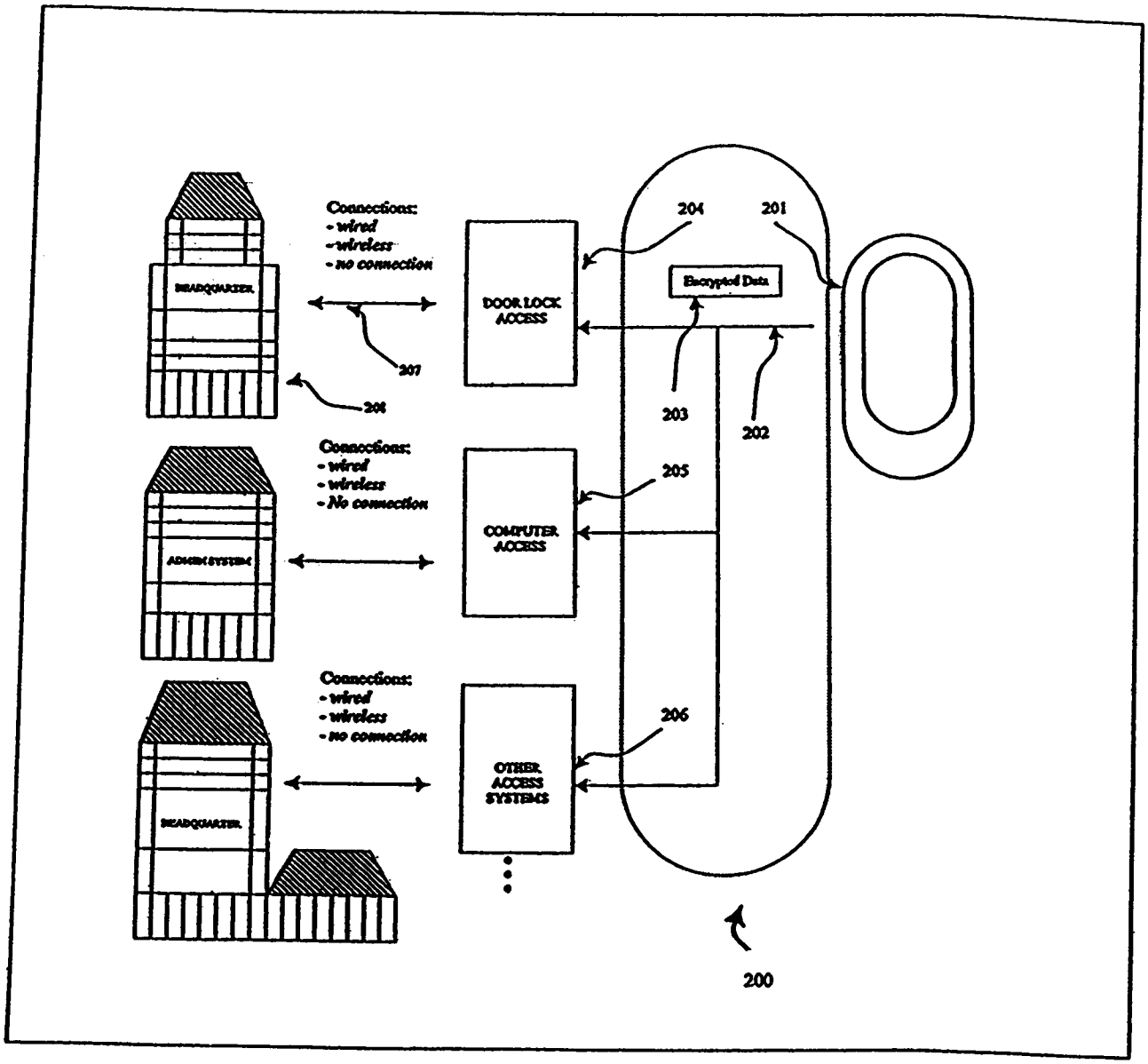
Connections:
- wired
- wireless
- no connection
207
208
DOOR LOCK ACCESS
204
201
Encrypted Data
203
202
Connections:
- wired
- wireless
- No connection
205
COMPUTER ACCESS
Connections:
- wired
- wireless
- no connection
206
OTHER ACCESS SYSTEMS
200

FIG. 3

400

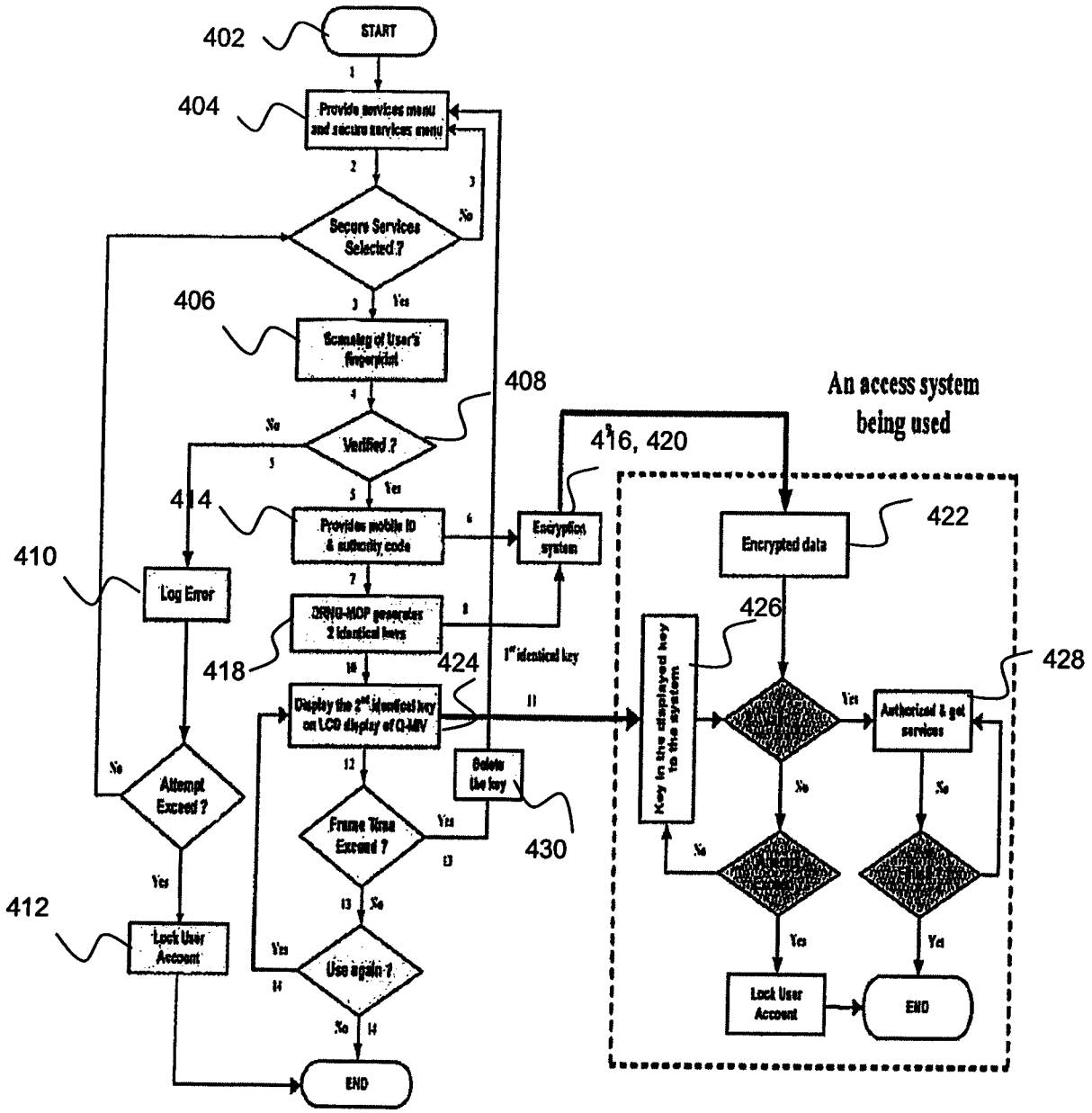
402
START
404
Provide services menu and secure services menu
Secure Services Selected ?
No
Yes
406
Scanning of User's fingerprint
408
Verified ?
No
Yes
An access system being used
416, 420
414
Provides mobile ID & authority code
Encryption system
422
Encrypted data
410
Log Error
426
428
1st identical key
418
424
Display the 2nd identical key on LCD display of O-MIV
Key in the displayed key to the system
Authorized & get services
Attempt Exceed ?
Delete the key
Frame Time Exceed ?
430
412
Lock User Account
Use again ?
Lock User Account
END
END

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2011/000163

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/08 (2006.01) ***H04L 9/00*** (2006.01) ***H04L 9/32*** (2006.01)

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)

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)
WPI, EPODOC, INSPEC, TXTUS0, TXTUS1, TXTUS2, TXTUS3, TXTUS4, TXTEP1, TXTGB1, TXTWO1 with keywords mobile access verification, symmetric cryptography, quantum, random number, biometric, hardware identification, authority code, OTP and similar terms.
Google Patents, Google Scholar, Google, and IEEE Xplore searched with similar terms as above.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/0211787 A1 (BUKSHPUN et al.) 19 August 2010 See the whole document.	1-14
A	US 2010/0046755 A1 (FISKE) 25 February 2010 See the whole document.	1-14
A	US 2007/0014407 A1 (NARENDRA et al.) 18 January 2007 See the whole document.	1-14

☐ 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
08 September 2011	20/09/2011
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **Dr. RASIKA PERERA** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 3116

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2011/000163

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2010211787	NONE					
US	2010046755	EP	1834438	US	2006129811	US	7657033
		US	2007129188	WO	2007075156		
US	2007014407	WO	2007011992				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX