

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
7 September 2007 (07.09.2007)

PCT

(10) International Publication Number
WO 2007/100202 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/KR2007/000986

(22) International Filing Date:
27 February 2007 (27.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2006-0019452
28 February 2006 (28.02.2006) KR

(71) Applicant (for all designated States except US):
MAZETECH [KR/KR]; #202B IDTVC, 994
Dongchun-dong, Yeonsu-gu, Incheon-si 406-130 (KR).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **LEE, Byung-sung**
[KR/KR]; 203-506 Manhyeon Maeul I Park,
Sanghyeon-dong, Suji-gu, Yongin-si, Gyeonggi-do
448-130 (KR).

(74) Agents: **LEE, Houn-Su** et al.; BYC Bldg. 15Fl., 648-1
Yeoksam-dong, Gangnam-gu, Seoul 135-080 (KR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

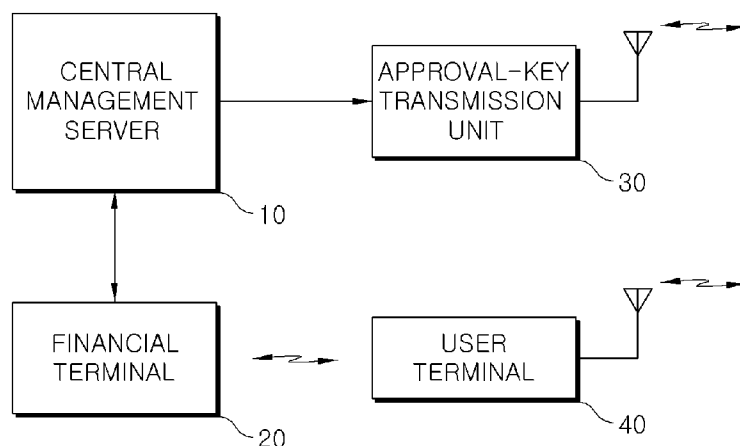
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- with amended claims and statement

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AUTHENTICATION SYSTEM FOR ONLINE FINANCIAL TRANSACTIONS AND USER TERMINAL FOR AUTHENTICATION OF ONLINE FINANCIAL TRANSACTIONS



(57) Abstract: An authentication system for online financial transactions over a communication network is provided, including a central management server which has an approval-key generation unit and an encryption-key generation unit, controls online financial transactions, transmits the approval key to a user terminal over a wireless network, encrypts and decrypts data transmitted and received to and from a financial terminal using the encryption key, a user terminal which is connected to the central management server and a financial terminal over a wireless network, and includes an approval-key receiving unit, an input unit to input a private password, an encryption-key generation unit to generate an encryption key from the approval key and the private password, and a data transceiver unit to transmit the encryption key to a financial terminal, and a financial terminal to encrypt and decrypt data transmitted and received to and from the central management server using the encryption key.

WO 2007/100202 A1

Description

AUTHENTICATION SYSTEM FOR ONLINE FINANCIAL TRANSACTIONS AND USER TERMINAL FOR AUTHENTICATION OF ONLINE FINANCIAL TRANSACTIONS

Technical Field

- [1] The present invention relates to an authentication system for electronic commerce and, more particularly, to an authentication system for online financial transactions and a user terminal for authentication of online financial transactions.

Background Art

- [2] The development of advanced communications technology has enabled users to conduct various kinds of electronic commercial transactions over the Internet and other networks. Most of the electronic commercial transactions involve financial transactions that are conducted online. Examples of the online financial transactions include a simple financial settlement, a wire transfer through a financial computer network, and cash withdrawal, deposit and transfer through a value-added network (VAN) and a financial computer network, such as an automatic teller machine (ATM).
- [3] In general, an authorized authentication key is required to be used to enhance the security of online financial transactions. Besides, an encryption key is required to be entered through an encryption card or the like.
- [4] Recently, there have been developed and widely used methods for enhancing the security of online financial transactions using a mobile communication terminal. Such methods are disclosed in Korean Patent Application Nos. 2001-81122, 2004-75159 and 2003-89125.
- [5] However, the above-mentioned methods cannot offer a full guarantee for the security of online financial transactions since information concerning authentication and encryption is transferred from user terminals over networks.
- [6] Therefore, methods for ensuring the security of online financial transactions are demanded.

Disclosure of Invention

Technical Solution

- [7] The present invention provides an authentication system for online financial transactions, which can ensure the security of online financial transactions.
- [8] The present invention further provides a user terminal which can ensure the security of online financial transactions.
- [9] Additional features of the invention will be set forth in the description which follows,

and in part will be apparent from the description, or may be learned by practice of the invention.

Advantageous Effects

- [10] It is possible to provide an authentication system for online financial transactions over a communication network which can greatly enhance the security of online financial transactions, and a user terminal therefor.

Brief Description of the Drawings

- [11] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention, and together with the description serve to explain the principles of the invention.
- [12] Fig. 1 is an authentication system for online financial transactions over a communication network according to an exemplary embodiment of the present invention.
- [13] Fig. 2 is a block diagram of a financial terminal shown in FIG. 1.
- [14] Fig. 3 is a block diagram of a user terminal shown in FIG. 1.
- [15] Fig. 4 is a flow chart for explaining the operation of the authentication system shown in FIG. 1.

Best Mode for Carrying Out the Invention

- [16] The present invention discloses an authentication system for online financial transactions over a communication network, including: a central management server which includes an approval-key generation unit to generate an approval key and an encryption-key generation unit to generate an encryption key from the approval key and a private password, controls online financial transactions, transmits the approval key to a user terminal over a wireless network, encrypts and decrypts data transmitted and received to and from a financial terminal using the encryption key; a user terminal which is connected to the central management server and a financial terminal over a wireless network, and includes an approval-key receiving unit to receive the approval key through the wireless network, an input unit to allow a user to input a private password, an encryption-key generation unit to generate an encryption key from the approval key and the private password, and a data transceiver unit to transmit the encryption key to a financial terminal over the wireless network; and a financial terminal to encrypt and decrypt data transmitted and received to and from the central management server using the encryption key transmitted from the user terminal.
- [17] The present invention also discloses a terminal for authentication of online financial transactions, including: a first communication unit to receive an approval key over a first communication network; a second communication unit to transmit an encryption key over a second communication network; an input unit to allow a user to input a

private password; and an encryption-key generation unit to generate an encryption key from the approval key and the private password.

- [18] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

Mode for the Invention

- [19] The invention is described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure is thorough, and will fully convey the scope of the invention to those skilled in the art. In the drawings, the size and relative sizes of layers and regions may be exaggerated for clarity. Like reference numerals in the drawings denote like elements.
- [20] It will be understood that when an element or layer is referred to as being "on" or "connected to" another element or layer, it can be directly on or directly connected to the other element or layer, or intervening elements or layers may be present. In contrast, when an element is referred to as being "directly on" or "directly connected to" another element or layer, there are no intervening elements or layers present.
- [21] Fig. 1 is an authentication system for online financial transactions over a communication network according to an exemplary embodiment of the present invention.
- [22] The authentication system includes a central management server 10, a financial terminal 20, an approval-key transmission unit 30 and a user terminal 40.
- [23] The central management server 10 controls general online financial transactions. The central management server 10 is linked, for example, to a main computer of a bank over a financial management network. The central management server 10 conducts financial transactions with the financial terminal 20, and transmits transaction data to the main computer over the financial management network.
- [24] The central management server 10 refers to authentication information, such as ID and password, or account information of a user which is input through the financial terminal 20. When the user is a normal user, it generates an approval key for the normal user. The approval key is generated when an authentication procedure is performed, and is used once. The central management server 10 may have an approval-key algorithm to generate an approval key, or receive an approval key from another approval-key generation unit. The central management server 10 stores therein the approval key, together with the authentication information, and transmits them to the approval-key transmission unit 30.

- [25] According to an exemplary embodiment of the present invention, a user uses two kinds of passwords; one for user authentication that is conducted by the central management server 10 (hereinafter referred to as 'authentication password', and one for encryption of data that is transmitted between the central management server 10 and the financial terminal 20 (hereinafter referred to as 'private password'). The private password is assigned to a user on initial registration. Thereafter, the private password will not be transmitted between the central management server 10 and the financial terminal 20. An encryption procedure through the private password will be described in detail.
- [26] The central management server 10 includes an encryption/decryption unit to encrypt/decrypt data which is transmitted and received to and from the financial terminal 20. The encryption/decryption unit is made in software or in hardware. The central management server 10 transmits the approval key and generates an encryption key from an authorized authentication key, an approval key and a private password. The central management server 10 encrypts and decrypts the data by the encryption/decryption unit using the encryption key. Any typical encryption/decryption unit may be used in the encryption/decryption procedure.
- [27] The financial terminal 20 enables a user to conduct online financial transactions. The financial terminal 20 may be an automated teller machine (ATM) or a personal computer. When the financial terminal 20 is an ATM, the financial terminal 20 and the central management server 10 are connected to each other, for example, over a value-added network (VAN). When the financial terminal 20 is a personal computer, they are connected to each other over the Internet.
- [28] Fig. 2 is a block diagram of the financial terminal 20.
- [29] The financial terminal 20 includes a controller 21, a network interface 22, an encryption/decryption unit 23, a data transceiver unit 24, an input unit 25 and a monitor 26.
- [30] The controller 21 generally controls the financial terminal 20. The network interface 22 provides an interface with the VAN or Internet. The encryption/decryption unit 23 encrypts data to be transmitted to the central management server 10 and decrypts data received from the central management server 10. The encryption/decryption unit 23 uses an encryption key to encrypt and decrypt the data, in which the encryption key is provided from the controller 21. The encryption/decryption unit 23 is made in software or in hardware.
- [31] The data transceiver unit 24 exchanges data with a user terminal 40. The financial terminal 20 and the user terminal 40 exchanges data with each other through a radio frequency (RF) signal. The data transceiver unit 24 converts an electrical data signal received from the controller 21 into an RF signal, and transmits the RF signal over an

antenna. The RF signal from the user terminal 40 is converted to an electrical signal and provided to the controller 21. The communication between the financial terminal 20 and the user terminal 40 may be made with an infrared signal or in a wireless or wired data communication manner.

[32] The input unit 25 enables a user to input authentication information, such as ID and password, and other transaction information. The monitor 26 displays state information or transaction information to the user.

[33] The approval-key transmission unit 30 receives approval-key information from the central management server 10 and transmits it to the user terminal 40. The approval-key transmission unit 30 is connected to the central management server 10, for example, over a local area network (LAN), and to the user terminal 40 over a wireless communication network. When the user terminal 40 is a mobile communication terminal, the approval-key transmission unit 30 is a short message service (SMS) unit which receives the approval key from the central management server 10 and transmits it to the user terminal 40 in a text message.

[34] The user terminal 40 may be one used only for the above-mentioned financial transactions, or an existing mobile communication terminal.

[35] Fig. 3 is a block diagram of the user terminal 40. The user terminal 40 includes a controller 41, a network interface 42, an input unit 43, an encryption-key generation unit 44, a data transceiver unit 45 and a monitor 46.

[36] The controller 41 generally controls the user terminal 40. The network interface 42 provides an interface between the user terminal 40 and a communication network. When the user terminal 40 is a mobile communication terminal, the network interface 42 provides an interface between the user terminal 40 and the mobile communication network.

[37] The input unit 43 includes, for example, a 10-key keypad. The input unit 43 enables a user to input a private password.

[38] The encryption-key generation unit 44 generates an encryption key by combining an approval key, which is received through the network interface 42, and a private password, which is input through the input unit 43. The encryption-key generation unit 44 may be made in software or in hardware. Any typical encryption-key generation unit may be used in the encryption-key generation procedure.

[39] The data transceiver unit 45 is one for wireless communication between the user terminal 40 and the financial terminal 20. The data transceiver unit 45 converts encryption-key information, which is transmitted from the controller 41 to the financial terminal 20, into, for example, an RF signal, or converts an RF signal, which is received from the financial terminal 20, into an electrical signal and provides it to the controller 41. In this case, any typical data transceiver unit may be used which allows

infrared communication or other wireless or wired communication with the financial terminal 20.

[40] The monitor 46 displays information to users.

[41] Fig. 4 is a flow chart for explaining the operation of an authentication system according to an exemplary embodiment of the present invention.

[42] When a user conducts a financial transaction, the user accesses the central management server 10 through the financial terminal 20 and selects a desired financial transaction. The central management server 10 requests the user to enter ID and authentication password through the financial terminal 20. The central management server 10 may request the user to further enter information such as a user name or a bank account. The user enters the authentication information according to a typical online financial transaction procedure.

[43] When the user enters information requested by the central management server 10 to log in, the central management server 10 conducts a typical authentication procedure to determine whether or not the user is genuine.

[44] When the user is determined to be genuine, the central management server 10 generates an approval key for a current financial transaction. The approval key, together with user information, is stored and transmitted to the approval-key transmission unit 30. The user information includes an access number of the user terminal 40.

[45] The approval-key transmission unit 30 transmits the approval-key information received from the central management server 10 to the user terminal 40 over the wireless communication network.

[46] In Fig. 3, when the user terminal 40 receives the approval-key information through the network interface 42, the controller 41 outputs on the monitor 46 a message to enter a private password. When a user enters the private password through the input unit 43, the controller 41 provides both the approval key information received through the network interface 42 and the private password entered through the input unit 43 to the encryption-key generation unit 44, and drives the encryption-key generation unit 44 to generate an encryption key.

[47] The controller 41 transmits the encryption key to the financial terminal 20 through the data transceiver unit 45. The encryption key may be automatically transmitted or selectively transmitted by the input unit 43.

[48] The central management server 10 transmits the approval key through the approval-key transmission unit 30, and generates an encryption key in the same manner as the user terminal 40.

[49] Referring to Fig. 2, when the financial terminal 20 receives the encryption key through the data transceiver unit 24, it notifies the central management server 10 that

the encryption key has been received. The financial terminal 20 uses the encryption key received from the user terminal 40 to initialize the encryption/decryption unit 23. When the central management server 10 receives from the financial terminal 20 a message indicating that the encryption key has been received, it uses the encryption key to initialize an encryption/decryption unit. Subsequently, the central management server 10 and the financial terminal 20 encrypt data with the encryption key and make communications.

- [50] When the central management server 10 transmits the approval key to the user terminal 40 and is not acknowledged by the financial terminal 20 in a predetermined time that the encryption key has been received, the central management server 10 determines that the current financial transaction is not normal, and initializes the current financial transaction.
- [51] In the above-mentioned exemplary embodiment, the central management server 10 and the financial terminal 20 individually generate an encryption key. When the encryption key is generated, a private password, which is not transmitted through a network, is used between the central management server 10 and the financial terminal 20. The central management server 10 and the financial terminal 20 encrypt and decrypt information which is transmitted with the encryption key. Thus, even though a third party has intentionally obtained information transmitted between the central management server 10 and the financial terminal 20, the third party cannot recognize the information. Therefore, it is possible to greatly enhance the security of financial transactions.
- [52] In the present embodiment of the invention, the user terminal 40 generates and provides an encryption key to the financial terminal 20. However, the user terminal 40 may store an authorized authentication key for a current financial transaction, and provide an encryption key, together with the authorized authentication key, to the financial terminal 20.
- [53] As a result, the user can conduct a secure financial transaction only with the user terminal 40.
- [54] When the user terminal 40 stores the authorized authentication key, the user terminal 40 and the central management server 10 may generate an encryption key by combining the approval key, authorized authentication key, and private password.
- [55] It will be apparent to those skilled in the art that various modifications and variation can be made in the present invention without departing from the spirit or scope of the invention. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

Industrial Applicability

- [56] The present invention can efficiently be applied to an authentication system for online financial transactions, which can ensure the security of online financial transactions, and a user terminal which can ensure the security of online financial transactions.

Claims

- [1] An authentication system for online financial transactions over a communication network, comprising:
a central management server which comprises an approval-key generation unit to generate an approval key and an encryption-key generation unit to generate an encryption key from the approval key and a private password, controls online financial transactions, transmits the approval key to a user terminal over a wireless network, encrypts and decrypts data transmitted and received to and from a financial terminal using the encryption key;
a user terminal which is connected to the central management server and a financial terminal over a wireless network, and comprises an approval-key receiving unit to receive the approval key through the wireless network, an input unit to allow a user to input a private password, an encryption-key generation unit to generate an encryption key from the approval key and the private password, and a data transceiver unit to transmit the encryption key to a financial terminal over the wireless network; and
a financial terminal to encrypt and decrypt data transmitted and received to and from the central management server using the encryption key transmitted from the user terminal.
- [2] The authentication system of claim 1, wherein the user terminal and the financial terminal transmit and receive an encryption key to and from each other over a wireless network.
- [3] The authentication system of claim 1, wherein the user terminal further comprises a storage unit to store an authorized authentication key, and the authorized authentication key is provided, together with an encryption key, to the financial terminal.
- [4] A terminal for authentication of online financial transactions, comprising:
a first communication unit to receive an approval key over a first communication network;
a second communication unit to transmit an encryption key over a second communication network;
an input unit to allow a user to input a private password; and
an encryption-key generation unit to generate an encryption key from the approval key and the private password.
- [5] The terminal of claim 4, further comprising an authorized authentication-key storage unit to store an authorized authentication key.

AMENDED CLAIMS received by the International Bureau on 16 July
2007 (16.07.2007)

Claim Amendments

1. An authentication system for online financial transactions over a communication network, comprising: a central management server which comprises an approval-key generation unit to generate an approval key and an encryption-key generation unit to generate an encryption key from the approval key and a private password, controls online financial transactions, transmits the approval key to a user terminal over a wireless network, encrypts and decrypts data transmitted and received to and from a financial terminal using the encryption key; a user terminal which is connected to the central management server and a financial terminal over a wireless network, and comprises an approval-key receiving unit to receive the approval key through the wireless network, an input unit to allow a user to input a private password, an encryption-key generation unit to generate an encryption key from the approval key and the private password, and a data transceiver unit to transmit the encryption key to a financial terminal over the wireless network; and a financial terminal to encrypt and decrypt data

transmitted and received to and from the central management server using the encryption key transmitted from the user terminal.

2. The authentication system of claim 1, wherein the user terminal and the financial terminal transmit and receive an encryption key to and from each other over a wireless network.

3. The authentication system of claim 1, wherein the user terminal further comprises a storage unit to store an authorized authentication key, and the authorized authentication key is provided, together with an encryption key, to the financial terminal.

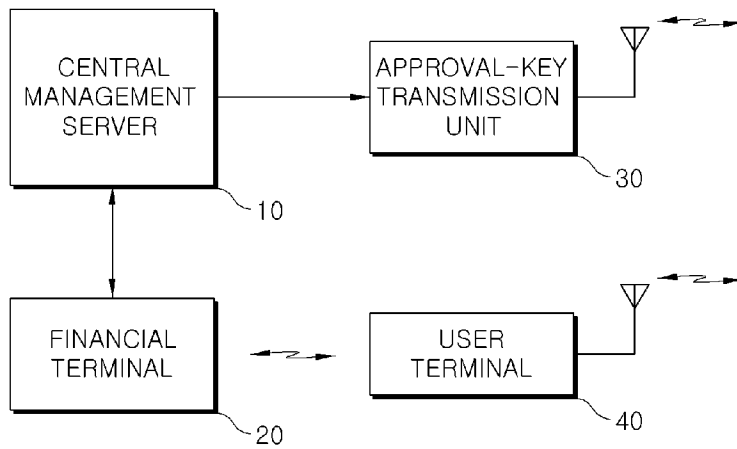
STATEMENT

International application No. PCT/KR2007/000986

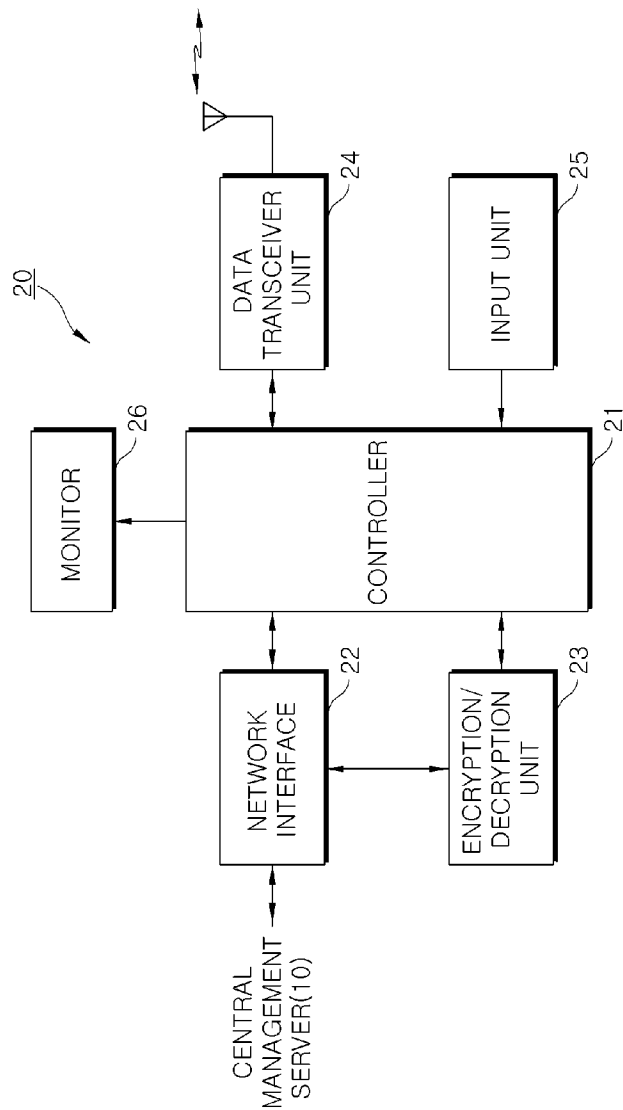
Applicant: MAZETECH

The amended claims of the present invention do not at all affect the description and the drawings of the present invention.

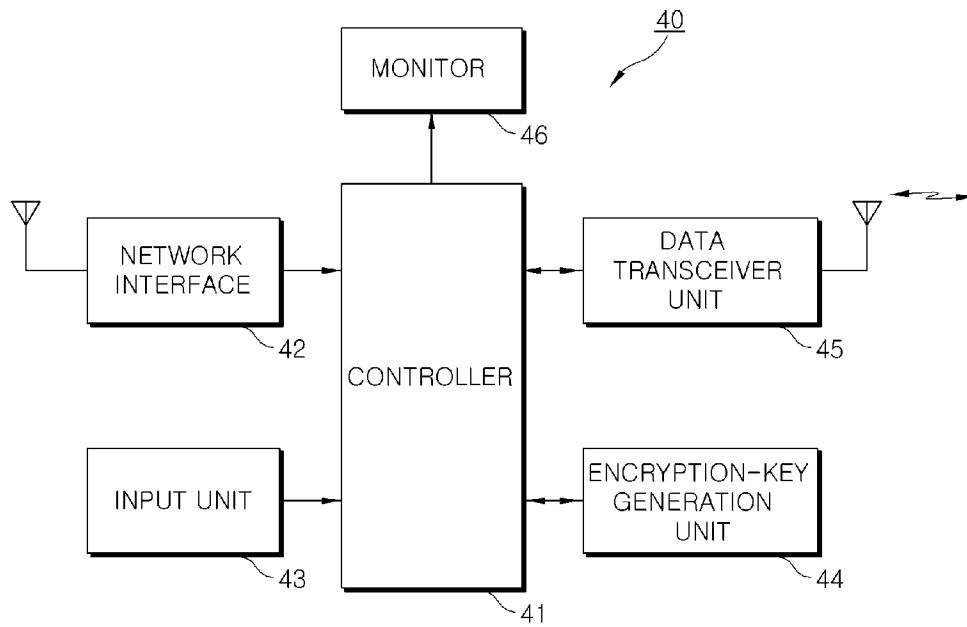
[Fig. 1]



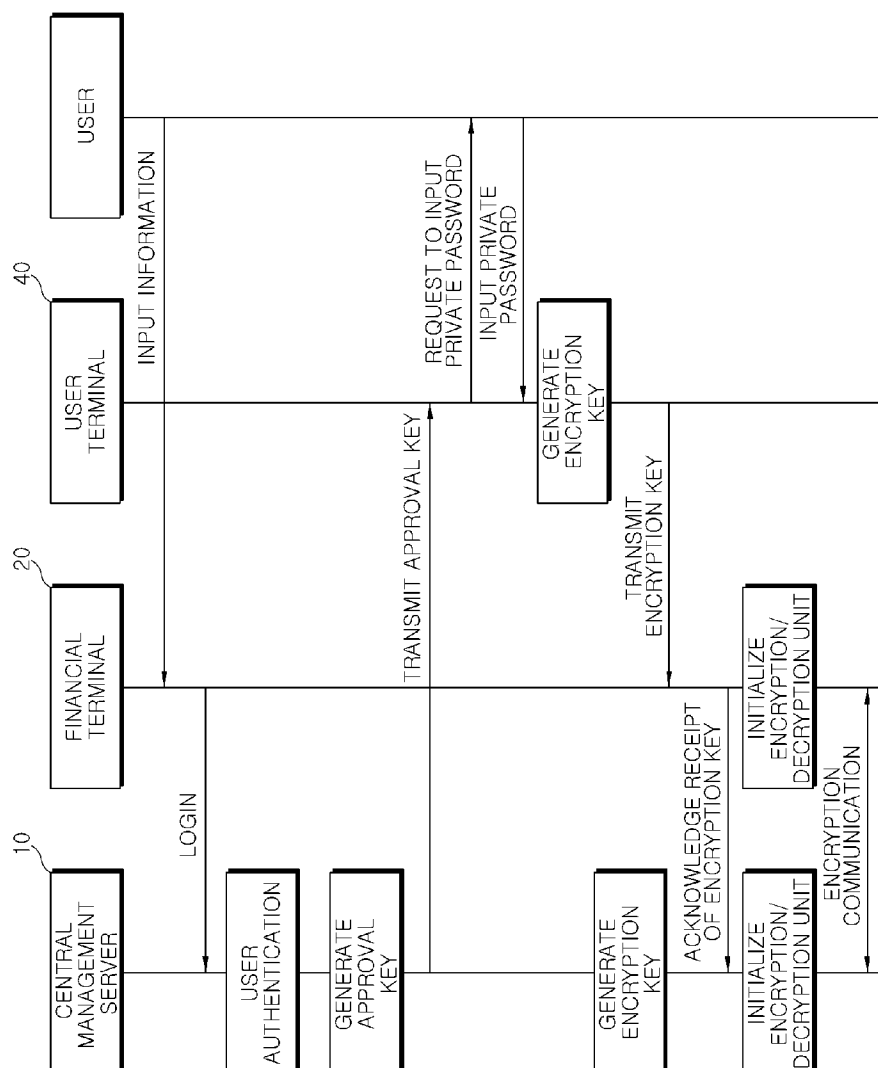
[Fig. 2]



[Fig. 3]



[Fig. 4]



A. CLASSIFICATION OF SUBJECT MATTER**G06Q 20/00(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)

IPC8 G06Q 20/00; G06Q 40/00; H04L 9/08

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 since 1975.

Japanese utility models and application for utility models since 1975.

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

e-KIPASS "SESSION, KEY, GENERATION, PASSWORD"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2001-0026309 A (SMART CARD TECHNOLOGY INC.) 6 April 2001 See English abstract; fig. 8	1-5
Y	US 06230269 B1 (SPIES, T. R. et al.) 8 May 2001 See abstract; fig. 4	1-5
A	US 06539479 B1 (WU T. J.) 25 March 2003 See abstract	1-5
A	KR 10-2003-0005986 A (BIZMODEL LINE CO., LTD.) 23 January 2003 See abstract	1-5



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 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

11 JUNE 2007 (11.06.2007)

Date of mailing of the international search report

11 JUNE 2007 (11.06.2007)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

YUK, SEONG WON

Telephone No. 82-42-481-8213



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/000986Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

KR1020010026309A

06.04.2001

None

US06230269B1

08.05.2001

None

US06539479B1

25.03.2003

None

KR1020030005986A

23.01.2003

None