



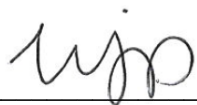
City of New York, State of New York, County of New York

I, Jacqueline Yorke, hereby certify that the document “**4 WO2002-008981**” is, to the best of my knowledge and belief, a true and accurate translation from Japanese into English.

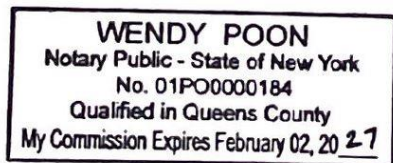


Jacqueline Yorke

Sworn to before me this
December 5, 2023



Signature, Notary Public



Stamp, Notary Public

(19) Japan Patent Office (JP)	Re-published Japanese Translation of a PCT Application (A1)	(11) International publication number WO2002/008981
Date of issue January 8, 2004 (01.08.2004)	(43) International publication date	January 31, 2002 (01.31.2002)

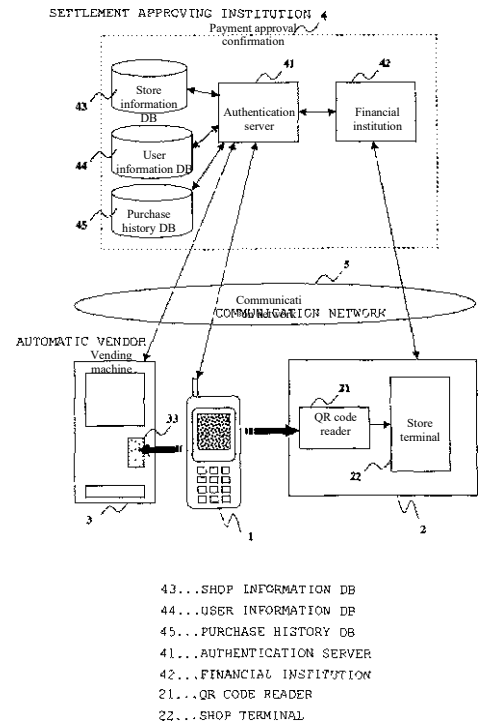
(51)Int.Cl.⁷	FI
G06F 17/60	G06F 17/60 414
G06K 17/00	G06F 17/60 422
G06K 19/06	G06F 17/60 506
G06K 19/07	G06F 17/60 512
H04Q 7/38	G06F 17/60 ZEC
Request for examination Yes Number of preliminary claims (Total of 47 pages)	
Continued on last page	

Application Number (21) International application number (22) International application date (31) Priority claim number (32) Priority date (33) Priority claim country (81) Designated country: EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), CN, JP, KR, US	Japanese Patent Application 2002-514614 (P2002-514614) PCT/JP2001/004223 May 21, 2001 (05.21.2001) Japanese Patent Application 2000-223658 (P2000-223658) July 25, 2000 (07.25.2000) Japan (JP)	(71) 500344688 Applicant Image Media Design Co., Ltd. 5-9-2 Nishigotanda, Shinagawa-ku, Tokyo (74) 100088720 Agents Patent attorney Shinichi Ogawa (72) Yuji Kano Inventor 4-9-19 Nishigotanda, Shinagawa-ku, Tokyo
--	--	--

(54) [Title of the Invention] Commercial transaction method and network terminal and commercial transaction system

(57) [Summary]

To provide secure authentication and payments. At the time of purchase, the owner of the network terminal, for example, the mobile phone (1), enters the purchase information such as the identity of the seller, the payment amount, and the PIN, and sends it to the authentication server (41), and receives the payment certificate as a QR payment certification key that can be displayed as a 2-D barcode on the mobile phone display based on the results of authentication and credit inquiry. The store terminal (22) reads this displayed code by the reader (21), and also reads the serial number and the phone number of the mobile phone that is externally marked as a barcode, and sends it to the authentication server. The authentication server checks whether this code has been previously issued and whether the serial number is legitimate.



[Scope of Patent Claims]

[Claim 1]

A commercial transaction method comprising of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the commercial transaction method is characterized in that it comprises the steps of receiving the payment certification key information related to the commercial transaction from a payment authorization institution, causing the payment certification key information received to be displayed in the display means, forwarding the payment certification key information displayed on the network terminal to a payment terminal installed at the purchaser of goods, and performing payment of the selected goods by the purchaser using the payment terminal of the purchaser of goods.

10

[Claim 2]

A commercial transaction method comprising of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the commercial transaction method is characterized in that it comprises the steps of receiving the payment certification key information related to a commercial transaction and a certificate of trust issued by a product purchase source from a payment approval institution, causing the received certificate of trust with the payment certification key information to be displayed on the display means, forwarding the payment certification key information displayed on the network terminal to a payment terminal installed at the purchaser of goods, and performing payment of the selected goods by the purchaser using the payment terminal of the purchaser of goods.

20

[Claim 3]

A commercial transaction method according to any one of Claims 1 or 2, characterized in that a mobile device is used as the network terminal.

[Claim 4]

A commercial transaction method according to any one of the Claims 1 to 3, characterized in that the network terminal receiving the payment certification key information and the ordering party network terminal in the commercial transaction are different terminals.

30

[Claim 5]

A commercial transaction method according to any one of the Claims 1 to 4, characterized in that the payment certification key information displayed in the display means is configured with a code character information image.

[Claim 6]

A commercial transaction method according to any one of the Claims 1 to 5, characterized in that the payment certification key information displayed in the display means is configured with an encrypted code character information image.

[Claim 7]

A commercial transaction method according to any one of the Claims 1 to 6, characterized in that the network terminal has a sign that records the identification information of each terminal device, and further comprises the steps of causing the payment terminal to read the identification sign, transmitting some or all of the payment certification key information transferred to the payment terminal and the identification sign information to the payment authorization institution, and authenticating whether the identification sign information is legitimately registered in advance with the payment authorization institution, and transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the payment terminal from which the item was purchased.

40

[Claim 8]

A commercial transaction method according to any one of the Claims 1 to 6, characterized in that the network terminal has an identification sign that records the identification information of either the IC card or the owner of the network terminal, and further comprises the steps of causing the payment

50

terminal to read the identification sign, transmitting some or all of the payment certification key information transferred to the payment terminal and the identification sign information to the payment authorization institution, and authenticating whether the identification sign information is legitimately registered in advance with the payment authorization institution, and transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the payment terminal from which the item was purchased.

[Claim 9]

A commercial transaction method according to any one of the Claims 1 to 8, characterized in that the identification sign is composed of a mark that emits the identification information recorded on the identification sign with reflected light of a predetermined wavelength in response to irradiation light of a predetermined wavelength.

10

[Claim 10]

A commercial transaction method according to any one of the Claims 1 to 9, characterized in that it further comprises of a step of displaying the information regarding the purchaser included in the payment certification key information on a display unit of the payment terminal from which the product was purchased.

[Claim 11]

A commercial transaction method according to any one of the Claims 1 to 10, characterized in that it further comprises of a step of transmitting the content of the transaction that has completed the payment from the payment terminal of the item purchaser to the payment authorization institution and updating the purchase history information of the purchaser.

20

[Claim 12]

A commercial transaction method according to any one of the Claims 1 to 11, characterized in that it further comprises of a step of transmitting the content of the transaction completed by the payment authorization institution to the network terminal of the purchaser and displaying the content of the transaction.

[Claim 13]

A commercial transaction method comprising of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the commercial transaction method is characterized in that it comprises the steps of receiving the payment certification key information relating to the transaction from the payment authorization institution and a certificate of trust issued by the product purchaser at the network terminal, printing the received certificate of trust with the payment certification key information with the code character information image, reading the signed certificate of trust with the payment certification key information to the payment terminal installed at the product purchaser, and performing payment of the selected goods by the purchaser at the payment terminal of the product purchaser.

30

[Claim 14]

A commercial transaction method according to Claim 13, characterized in that the code character information image is printed with a printing material mixed with crystalline powder that emits the payment certification key information by the reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength.

40

[Claim 15]

A commercial transaction method according to Claims 1 to 13, characterized in that the network terminal has an input means for inputting the information on the commercial transaction, which further comprises the steps of inputting the information on a transaction of a product including at least the product provider or the product identification information, the payment method, the purchase amount and the purchaser's own PIN from the input means, and transmitting the input payment information to a payment authorization institution and receiving the payment certification key information generated in response to the authentication of the product provider and the purchaser's own authentication and credit results.

50

[Claim 16]

A commercial transaction method according to Claims 1 to 15, characterized in that the network terminal has an input means for inputting the information on the commercial transaction, which further

comprises the steps of inputting the information related to the transaction of the product including at least the product provider or the product identification information, the payment method, the service points used, and the purchaser's own personal identification number, and transmitting the input payment information to a payment authorization institution and receiving the payment certification key information generated in accordance with the product provider's authentication, the purchaser's own authentication, and the confirmation result of the service points acquired by the purchaser.

[Claim 17]

A commercial transaction device that comprises of a network terminal having an input means for inputting the information about the payment of a transaction target product, a display means for displaying information about the payment, and a transmitting/receiving means for transmitting information and receiving information regarding the payment of the product via a communication network; and performs payment for a transaction target product provided by the product provider, comprising of a means for generating the payment certification key information related to the commercial transaction, and a means for transmitting and displaying the payment certification key information to the network terminal.

10

[Claim 18]

A commercial transaction device that performs payment for a transaction target product provided by a product provider using a network terminal having a display means for displaying the payment information and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; the commercial transaction device comprises of a means for generating the payment certification key information relating to the commercial transaction and a means for receiving and transmitting and displaying the certificate of trust issued from the product purchaser as a certificate of trust with the payment certification key information.

20

[Claim 19]

A commercial transaction device according to any one of the Claims 17 or 18, characterized in that a mobile device is used as the network terminal.

[Claim 20]

A commercial transaction system comprising of a display means for displaying the information regarding payment; a device identification sign; a network terminal having a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payments; a product provider device that settles the price of the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to commercial transactions and transmit it to the network terminal for display, and that receives a part or all of the payment certification key information and the reading result of the device identification sign from the product provider; a means for authenticating whether the information on the device identification sign is genuine and registered in advance with a payment authorization institution, and that transmits the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of the product purchase source in accordance with the authentication result of the information on the device identification sign; and a means for delivering products ordered by a purchaser and making payment for the products.

30

40

[Claim 21]

A commercial transaction system comprising of a display means for displaying the information regarding the payment; a device identification sign; a network terminal having a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that performs payment for the product at the product provider; a means for the payment authorization institution device to generate the payment certification

key information related to the commercial transaction; a means for transmitting and displaying the certificate of trust issued by the product purchasing source and the payment certification key information to the network terminal, and that receives a part or all of the payment certification key information and the reading result of the device identification sign from the product provider; a means for authenticating whether the information on the device identification sign is genuine and registered in advance with the payment authorization institution; and a means for transmitting the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of a product purchase source in accordance with the authentication result of information on the device identification sign.

[Claim 22]

10

A commercial transaction system according to Claims 20 and 21, wherein the network terminal is a mobile device.

[Claim 23]

A commercial transaction system according to any one of Claims 20 to 22, characterized in that the device identification sign is configured with a sign that emits the device serial number information and the telephone number information using the reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength.

[Claim 24]

A commercial transaction system comprising of a mobile terminal having a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product ordering and payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that performs payment for the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to the commercial transaction; a means for transmitting the certificate of trust issued by the product purchasing source and the payment certification key information to the network terminal, and that receives information from the product purchase source regarding the certificate of trust printed in the code character information image by a printing device attached to the network terminal and the reading result of the payment certificate key information; a means for authenticating whether or not the payment certification key information is valid, and that sends the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of the product purchase source in accordance with the authentication result of the payment certification key information; and a means for delivering products ordered by a purchaser and making payment for the products.

20

30

[Claim 25]

A commercial transaction system according to Claim 24, characterized in that the code character information image is configured with an encrypted code character information image.

[Claim 26]

A recording medium characterized in that it consists of a network terminal having a display means for displaying the information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a program for making a payment regarding the product to be traded provided by a product provider; a process for generating the payment certification key information and transmitting and displaying the information to the network terminal, and that transfers the payment certification key information from the network terminal on which the payment certification key information is displayed to a terminal installed at the product purchase source; and a computer-readable program with the commercial transactions recorded thereon, and that includes the processes that cause the payment terminal of the product purchaser to execute payment for a product selected by a purchaser.

40

[Detailed description of invention]

Technical field

50

The present invention relates to a commercial transaction method, a commercial transaction device and

a commercial transaction system that can be used for payment of products purchased at various stores such as supermarkets, electronic stores opened on Internet servers, or vending machines such as for potable drinking water, using terminals that can be connected to a network such as via mobile phones.

Background technology

With the addition of the WWW browsing function (World Wide Web) to the mobile phone, the transaction format of using the mobile phone to access the Internet, browse various types of information, goods, and services, and order the provision of such information, goods, and services as necessary is rapidly expanding. Here, in the present invention, information (content) such as music software that does not have a shape, goods that have a shape, and services such as home delivery service and nursing care service are all defined as products that are subject to commercial transactions. In this case, there are also free nursing services provided by public institutions, but even if they are free, they are included in the products subject to transactions.

10

However, even if a product is ordered using a mobile phone, the settlement method still follow traditional business practices, such as bank transfer, sending of cash, and cash on delivery upon arrival of the product.

In recent times, instead of this conventional method, a method has been implemented in which a credit card number is notified to the product provider (store) at the same time as the product is ordered, and payment is made through the credit card company.

However, this payment method is based on the premise that the number or information that only the credit card company and the person themselves should know will not be leaked to outside parties, and if leaked, there is a risk that it will be misused.

20

Therefore, in the next-generation mobile communication services starting in May 2001, which will equip mobile phones with an IC card called a UIM (User Identity Module), a method is being considered in which confidential data such as credit card numbers are encrypted using a cryptographic program in the IC card allowing payments to be made.

However, even if the data is encrypted and saved using a cryptographic program, if the mobile phone itself is lost, there is a risk that it will be decrypted by an unauthorized third party and misused. In particular, it is believed that there will be many forms of storing not only credit card numbers but also other confidential data such as bank account numbers, insurance card numbers, and electronic money at the same time in IC cards, so the risk of being decrypted by an unauthorized third party is higher than with traditional payment methods.

30

In addition, as with contactless IC cards, networks using wireless networks have a problem in that there is a greater possibility of information leaking to the outside due to hacking, including unauthorized access, than wired networks.

In addition, due to the emergence of unauthorized stores, there is the risk that confidential data may be intercepted and misused during payment at these store.

Furthermore, there is also the problem that the cost of the mobile device itself will increase, the power consumption will also increase, and the battery life will be shortened.

The present invention is made to solve such problems, and the purpose is to provide a commercial transaction method, device, and system that can authenticate the person without disclosing confidential data such as credit numbers to a person authentication institution or credit card company, and can safely settle the purchase of goods.

40

Disclosure of the Invention

In order to achieve the above objectives, the commercial transaction method of the present invention is characterized by being configured as follows.

In other words, it is a method that comprises of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the method is characterized in that it comprises the steps of receiving the payment certification key information related to the commercial transaction from a payment authorization institution, causing the payment certification key information received to be displayed in the display means, forwarding the payment certification key information displayed on the network terminal to a payment terminal installed at the purchaser of goods, and performing payment of the selected goods by the purchaser using the payment terminal of the purchaser of goods. Furthermore, the method comprises of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and

50

the method is characterized in that it comprises the steps of receiving the payment certification key information related to a commercial transaction and a certificate of trust issued by a product purchase source from a payment approval institution, causing the received certificate of trust with the payment certification key information to be displayed on the display means, forwarding the payment certification key information displayed on the network terminal to a payment terminal installed at the purchaser of goods, and performing payment of the selected goods by the purchaser using the payment terminal of the purchaser of goods.

Also, the present invention is characterized in that a mobile device is used as the network terminal.

Moreover, it is characterized in that the network terminal receiving the aforementioned payment certification key information and the network terminal of the ordering party in commercial transactions are different terminals.

10

In addition, it is characterized in that the payment certification key information displayed in the display means is configured with a code character information image.

Further, it is characterized in that the payment certification key information displayed in the aforementioned display means is configured with encrypted code character information images.

It is also characterized in that the network terminal has a sign that records the identification information of each terminal device, and further comprises the steps of causing the payment terminal to read the identification sign, transmitting some or all of the payment certification key information transferred to the payment terminal and the identification sign information to the payment authorization institution, and authenticating whether the identification sign information is legitimately registered in advance with the payment authorization institution, and transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the payment terminal from which the item was purchased.

20

Additionally, it is characterized in that the network terminal has an identification sign that records the identification information of either the IC card or the owner of the network terminal, and further comprises the steps of causing the payment terminal to read the identification sign, transmitting some or all of the payment certification key information transferred to the payment terminal and the identification sign information to the payment authorization institution, and authenticating whether the identification sign information is legitimately registered in advance with the payment authorization institution, and transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the payment terminal from which the item was purchased.

30

Also, it is characterized in that the identification sign is composed of a mark that emits the identification information recorded on the identification sign with reflected light of a predetermined wavelength in response to irradiation light of a predetermined wavelength.

Further, it is characterized in that it further comprises of a step of displaying the information regarding the purchaser included in the payment certification key information on a display unit of the payment terminal from which the product was purchased.

Moreover, it is characterized in that it further comprises of a step of transmitting the content of the transaction that has completed the payment from the payment terminal of the item purchaser to the payment authorization institution and updating the purchase history information of the purchaser.

40

The method is characterized in that it further comprises of a step of transmitting the content of the transaction completed by the payment authorization institution to the network terminal of the purchaser and displaying the content of the transaction.

Notwithstanding, the method comprises of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the method is characterized in that it comprises the steps of receiving the payment certification key information relating to the transaction from the payment authorization institution and a certificate of trust issued by the product purchaser at the network terminal, printing the received certificate of trust with the payment certification key information with the code character information image, reading the signed certificate of trust with the payment certification key information to the payment terminal installed at the product purchaser, and performing payment of the selected goods by the purchaser at the payment terminal of the product purchaser. It is also characterized in that the code character information image is printed with a printing material mixed with crystalline powder that emits the payment certification key information by the reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength. It is further characterized in that the network terminal has an input means

50

for inputting the information on the commercial transaction, which further comprises the steps of inputting the information on a transaction of a product including at least the product provider or the product identification information, the payment method, the purchase amount and the purchaser's own PIN from the input means, and transmitting the input payment information to a payment authorization institution and receiving the payment certification key information generated in response to the authentication of the product provider and the purchaser's own authentication and credit results.

In addition, it is characterized in that the network terminal has an input means for inputting the information on the commercial transaction, which further comprises the steps of inputting the information related to the transaction of the product including at least the product provider or the product identification information, the payment method, the service points used, and the purchaser's own personal identification number, and transmitting the input payment information to a payment authorization institution and receiving the payment certification key information generated in accordance with the product provider's authentication, the purchaser's own authentication, and the confirmation result of the service points acquired by the purchaser.

10

The commercial transaction device of the present invention comprises of a network terminal having an input means for inputting the information about the payment of a transaction target product, a display means for displaying information about the payment, and a transmitting/receiving means for transmitting information and receiving information regarding the payment of the product via a communication network; and the device performs payment for a transaction target product provided by the product provider, comprising of a means for generating the payment certification key information related to the commercial transaction, and a means for transmitting and displaying the payment certification key information to the network terminal.

20

The device performs payment for a transaction target product provided by a product provider using a network terminal having a display means for displaying the payment information and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; the transaction device comprises of a means for generating the payment certification key information relating to the commercial transaction and a means for receiving and transmitting and displaying the certificate of trust issued from the product purchaser as a certificate of trust with the payment certification key information.

Also, the present invention is characterized in that a mobile device is used as the network terminal.

30

Further, the system comprises of a display means for displaying the information regarding payment; a device identification sign; a network terminal having a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payments; a product provider device that settles the price of the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to commercial transactions and transmit it to the network terminal for display, and that receives a part or all of the payment certification key information and the reading result of the device identification sign from the product provider; a means for authenticating whether the information on the device identification sign is genuine and registered in advance with a payment authorization institution, and that transmits the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of the product purchase source in accordance with the authentication result of the information on the device identification sign; and a means for delivering products ordered by a purchaser and making payment for the products.

40

The commercial transaction system of the present invention also includes a display means for displaying the information regarding the payment; a device identification sign; a network terminal having a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that performs payment for the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to the commercial transaction; a means for transmitting and displaying the certificate of trust issued by the product purchasing source and the payment certification key information to the network terminal, and that receives a part or all of the payment certification key information and the reading result of the device identification sign from the product provider; a means for authenticating whether the information on the device identification sign is genuine and registered in advance with the payment authorization institution; and a means for transmitting the payment authorization information corresponding to the payment certification key

50

information from the payment authorization institution to the payment terminal of a product purchase source in accordance with the authentication result of information on the device identification sign.

In addition, the network terminal is characterized in that it is a mobile device.

It is characterized in that the device identification sign is configured with a sign that emits the device serial number information and the telephone number information using the reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength.

The system further comprises of a mobile terminal having a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product ordering and payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that performs payment for the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to the commercial transaction; a means for transmitting the certificate of trust issued by the product purchasing source and the payment certification key information to the network terminal, and that receives information from the product purchase source regarding the certificate of trust printed in the code character information image by a printing device attached to the network terminal and the reading result of the payment certificate key information; a means for authenticating whether or not the payment certification key information is valid, and that sends the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of the product purchase source in accordance with the authentication result of the payment certification key information; and a means for delivering products ordered by a purchaser and making payment for the products.

It is characterized in that the code character information image is configured with an encrypted code character information image.

The transaction method of the present invention can also be realized by a program in a payment authorized institution device. The program can be provided on a recording medium that records the following processes. In other words, it is characterized in that it consists of a network terminal having a display means for displaying the information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a program for making a payment regarding the product to be traded provided by a product provider; a process for generating the payment certification key information and transmitting and displaying the information to the network terminal, and that transfers the payment certification key information from the network terminal on which the payment certification key information is displayed to a terminal installed at the product purchase source; and a computer-readable program with the commercial transactions recorded thereon, and that includes the processes that cause the payment terminal of the product purchaser to execute payment for a product selected by a purchaser.

Detailed Description of the Preferred Embodiments

The embodiments of the present invention will be described in detail below with reference to the accompanying drawings.

FIG. 1 is a system configuration diagram illustrating an embodiment of the overall configuration of the system for implementing the commercial transaction method of the present invention, which includes a mobile phone 1 as a network terminal used by a product purchaser, a store 2 from which the product is provided, a vending machine 3 such as for potable water, and a payment authorization institution 4, which is connected by a communication network 5. The communication network 5 includes a wireless line, a wired line, and an internet network. Here, the network terminal refers to a terminal that can be connected to a network such as the Internet, and in addition to the mobile phone 1 shown in the following example, it includes various other types such as PHS, PDA, personal computer, digital television, etc.

The mobile phone 1 is a commercially available mobile phone with a function that can be connected to an internet network, and as shown in the schematic block diagram of FIG. 2(a), it comprises of a display 11, a wireless transmitter/receiver 12, a control 13, an input 14, a receiver 15, a memory 16, and an external input and output interface 17. In the Internet connection mode, the display 11 displays the Internet connection menus such as news, mobile banking, card/security/insurance, and mobile shopping, as shown in FIG. 2(b).

The external input and output interface 17 includes a wireless communication interface, such as an infrared interface such as Irda and a weak radio wave interface such as Bluetooth, and in this present embodiment, it is used when receiving the store identification number from the transmitter installed in the store. In addition, the external input and output interface 17 includes an interface for a barcode

reader connected to a mobile phone or a built-in on the mobile phone, and the barcode reader may read the identification information, etc., of the store displayed with the barcode information or the identification information, etc. of the product. Furthermore, a camera connected to the mobile phone or a built-in on the mobile phone, and the identification information of each store or the identification information of the product displayed in the code character information image may be captured as image data by the camera. In this case, a program for decoding the code character information images captured as image data is provided in the authentication server of the payment authorization institution 4 above, and by decoding the code character information images sent from the mobile phone in the above program, the identification information of the store or product can be recognized. In addition, the aforementioned program may be provided on a mobile phone machine, and in this case, each of the
10
aforementioned identification information recognized by decoding the code character information image on the mobile phone machine is transmitted to the aforementioned authentication server. By using the external input and output interface 17 as described above, it is possible to input store or product identification information without operating the input unit 14. Here, the identification information of the product includes the product name, product type, and amount, etc.

It should be noted that entering the amount of the product is not a substitute for inputting the amount by a store staff, but it involves a self-scanning action, and is intended for the purchaser to know the payment amount information in advance. As shown in the front and side views of FIGS. 3(a) and (b), the mobile phone 1 of this embodiment is affixed with a first sign 19 that records the equipment serial number with the barcode 31, such as in FIG. 3(c), and a second sign 20 that records the mobile phone
20
number with the barcode 31.

The barcodes of these signs 19 and 20 are printed with a printed material containing crystalline powder that emits the recorded information by the reflected light having a predetermined wavelength λ_a or λ_b in response to an irradiation light having a predetermined wavelength λ_a , as shown in FIG. 4(a). This crystalline powder is provided by SUNSTONE, Inc. in the United States, and is used for authentic identification of pharmaceutical products and banknotes. In this case, the characteristics are adjusted so that the wavelength of the irradiated light and the wavelength of the emitted light differ depending on the application and the system used.

In the present invention, the barcode of the device serial number and mobile phone number is printed on the signs 19 and 20 with a recording ink or toner mixed with the special crystalline powder, which
30
is affixed to the front or side of the mobile phone 1, and the barcode recorded on the signs 19 and 20 is read with the irradiated light at a predetermined wavelength λ_a .

By affixing the device serial number and the mobile phone number signs 19 and 20 recorded with such special recording ink or toner to the mobile phone 1, it is not possible to read the device serial number and mobile phone number other than the irradiated light at a predetermined wavelength. Therefore, by pre-registering the device serial number and the mobile phone number with the payment authorization institution 4, it is possible to identify whether the mobile phone 1 is a legitimate device that can be used for commercial transactions in this system. The side sign 20 also serves to prevent modification of the mobile phone 1.

In this case, it is not necessarily essential to affix the aforementioned sign, and the aforementioned sign
40
may be printed on the casing of the mobile phone itself using the recording ink or the like.

The barcodes of the signs 19 and 20 are inserted into the reader 40 in a cross-sectional configuration as shown in FIG. 4(b) and they are read by irradiating light with a predetermined wavelength. This reader 40 is installed in store 2 and the vending machine 3.

On the other hand, the display unit 11 displays payment certification key information configured with the two-dimensional code 32 as a code character information image as shown in FIG. 3(d). This two-dimensional code 32 is set in the standard code of the Japan Automobile Manufacturers Association and the Japan Stationery Association. This is disclosed in, for example, the Japanese Unexamined Patent Application No. 10-214317, so a detailed explanation will be omitted here.

Using this two-dimensional code (hereinafter referred to as the QR code), approximately 7,000
50
characters (numbers) can be coded and recorded within the area of the display of the mobile phone 1. In the present invention, this QR code is used to represent the information of the payment certification key information. In detail, the information of the payment certification key information composed of a QR code is transferred to the mobile phone 1 to display it in the display 11 as shown in FIG. 3(a), and the mobile phone 1 in this display state is inserted into the reader 21 for reading sharing of the signs 19 and 20, so that the information of the payment certification key is read.

When using a QR code, as shown in FIG. 3(d), the recording contents can be read from any direction within 360° by means of the cutout symbols 33 to 35 located in three locations, so that the positional relationship with the reader is no longer bound, and it is suitable for use by the general user to insert
60
into the reader unit and read. Also, since it is not necessary to strictly define the positional relationship,

the reading time can be shortened accordingly. In addition, even if some part of the code is dirty or damaged, the errors can be corrected, and the number of reading errors can be reduced. In particular, as in the present invention, when reading the data while it is displayed on the display of the mobile phone 1, it is conceivable that reading errors may occur due to dirt on the display unit, etc., but by using a QR code, reading errors caused by dirt on the display unit, etc. can be reduced.

Returning to FIG. 1, the store 2 is equipped with a reader 21 for reading the signs 19, 20 and the QR code, and inputs the read signs 19, 20 and the QR code into the store terminal 22, which is a POS terminal, which allows for payments to be made using the in-store terminals. The vending machine 3 is also equipped with a reader 33 for reading the QR codes and the signs 19, 20.

On the other hand, the payment authorization institution 4 comprises of a authentication server 41, a financial institution (bank or credit company) 42, a store information database (DB) 43, a user information database (DB) 44, and a purchase history database (DB) 45.

The authentication server 41 performs personal authentication and store authentication in response to a personal authentication and store authentication request from the mobile phone 1, and it also makes a credit inquiry to the financial institution 42; and if the person and the store are registered in advance, and there is a response from the financial institution 42 that the credit is OK, processing is performed to permit payment of the product price using the mobile phone 1. The server includes a store registration processing program 410, a user registration processing program 411, a purchase history management program 412, an unauthorized use management program 413, an authentication processing program 414, a QR payment key generation program 415, and a transmission/reception program 416. It should be noted that an encryption/decryption program for encrypting and storing the data from each database 43, 44, and 45 is incorporated as necessary. Additionally, an encryption program for encrypting and transmitting the QR code and a decryption program for decoding the QR code can be incorporated. By encrypting the QR code, unauthorized transactions can be made even more difficult.

The store registration processing program 410 is a program used to register stores (including vending machines and electronic stores on the Internet) that perform payments using this system in the store information DB 43. In addition, the user registration processing program 411 is a program used when registering a user (product purchaser) who makes a payment using this system in the user information DB 44. The purchase history management program 412 is a program used when storing information on the purchase history of products purchased by a user (product purchaser) in the purchase history DB 45.

The unauthorized use management program 413 allows the system to be accessed by a store and a user who are not registered in the store information DB 43 and user information DB 44 in advance, and it is used when registering the store identification number or the device serial number or phone number of mobile phone 1 in the unauthorized use information database (FIG. 9) if the device serial number or phone number of mobile phone 1 is accessed by illegally rewriting it.

The authentication processing program 414 performs personal authentication and store authentication as well as credit inquiries to the financial institution 42 in response to the personal authentication and store authentication requests from the mobile phone 1; and if the person and the store have been registered in advance, and if there is a response from the financial institution 42 that the credit is OK, processing is performed to permit payment of the product using the mobile phone 1.

The QR payment key generation program 415 is a program that generates the payment certification key information composed of the QR code and passes it to the mobile phone 1 in order to authorize the payment of the product. The payment certification key information (hereinafter referred to as "QR authorized certification key information") composed of the QR code is the key information for the store to receive detailed approval information including the results of authentication of the purchaser and the store from the authentication server 41. By reading this QR authorized certification key information read from the store reader 21 and sending the QR authorized certification key information read from the store terminal to the authentication server 41, the store terminal 22 can receive detailed approval information including the results of authentication of the purchaser and the store. In this case, if the QR authorized certification key information read by the reader 21 is different from that generated by the authentication server 41, approval of the authorized information cannot be obtained.

The transmission and reception program 416 is a program for sending and receiving the information necessary for decision making for access from users and stores.

FIG. 6 shows an example of the store information DB registration information, in which the store ID 601, the store name 602, address 603, and the phone number 604 are registered.

FIG. 7 is a diagram showing an example of the registration information for the user information DB, in which the user ID 701, the user name 702, address 703, the mobile phone serial number (device serial number) 704, the mobile phone number 705, PIN number 706, gender 707, date of birth 708, debit card number 709, credit card number 710, web money account number 711, and other personal

characteristics information 712 are registered.

The web money account number 711 is used when making a payment using the web money when purchasing a small-value item such as drinking water from a vending machine. In addition, the personal characteristics information 712 is intended to register the photos, etc. of the individual, and to enable the store staff to verify the identity of the user using features such as a photo when making a payment at a store, and it is registered according to the user's wishes. For example, registering a photo of the user himself/herself has the advantage that store staff can detect misuse by others at the time of payment processing. Further, based on the date of birth 708, it is possible to discover whether the person is a minor or not, and the sale of alcoholic beverages and tobacco can be prohibited. In addition, the driver's license number, etc. may also be registered. By registering a driver's license number, etc., it is also possible to issue a certificate of identity from a third-party authentication server 41 using a mobile phone.

10

FIG. 8 shows an example of the store information in the purchase history DB, in which the date and time of use 801, the name of the store used 802, the approval amount 803, the cumulative amount of the current month's use 804, the cumulative amount of service points 805, and the previous use date 806 are stored. It should be noted that this purchase history information is stored in the order of date and time of use for each user.

FIG. 9 is a diagram showing an example of the information stored in an unauthorized use information database, with the unauthorized user's mobile phone serial number 901, mobile phone number 902, and store ID 903 registered. Here, if only the mobile phone number 902 is registered, this means that the mobile phone serial number is correct, and it also means that the person accessed the site by modifying the mobile phone number sign. In addition, a store that does not have a store ID 903 registered means that the store is not registered in the system, or it is a store that has its store ID illegally rewritten.

20

Here, for unregistered users and stores who are not malicious, a message may be sent to register at the time of access, and registration may be made as unauthorized use only for those who do not perform the registration procedures despite multiple registration instructions.

Below, (1) the method of decision making when purchasing products using a mobile phone 1 at a general store such as a supermarket, (2) the method of decision making when purchasing products at a vending machine, and (3) the method of decision making when purchasing products at an electronic store on the Internet will be explained with reference to the flowchart.

30

FIGS. 10 and 11 are flowcharts illustrating how decisions are made when purchasing products using a mobile phone 1 at general stores such as supermarkets.

First, the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID as the identification information of the store from which he or she intends to purchase the product. The user then inputs his or her personal ID number (the number registered in 706 in FIG. 7), the payment method, and the purchase price of the product (step 1001). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17.

Further, regarding the payment method, there are the options of credit card payments, web money payments, and debit card payments, and if the credit card payment is selected, the number of payments and the credit card number are inputted. In addition, if the web money payment is selected, the web money account number (the number registered in 711 in FIG. 7) is inputted. Similarly, if the debit card payment is selected, the debit card number (the number registered in 709 in FIG. 7) is inputted. In the following flowchart, the operations performed by individuals are shown in a double-bordered format, as in step 1001.

40

When the input is complete, the transmission operation is performed. Then, the information input in step 1001 is sent to the authentication server 41 as the QR authorized certification key issuance request. The authentication server 41 that receives this request for issuing the QR authorized certification key information performs authentication processing for the store and the user (step 1002). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched using the PIN number and the credit card number (or the web money account number, or debit card number), and it is checked whether the user with the PIN number and the credit card number (or the web money account number, or debit card number) is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1003). Even if the personal ID number and the credit card number (or web money account number or debit card number) are not registered, the user is either an unauthorized user or an unregistered user, and a message indicating that the transaction is not

50

possible is sent back to the mobile phone 1 (step 1003). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1001 is automatically deleted.

However, if the store ID, the PIN number, and the credit card number (or web money account number, or debit card number) are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1004) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1005). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1006) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 1007). The store staff enters the price of the desired purchase item using the store terminal (step 1008).

In parallel, the user inserts and attaches the mobile phone 1 with the QR authorized key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 1009). The QR code reader 21 then reads the QR authorized certification key 1201 displayed on the display 11 of the mobile phone 1 (step 1011), and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1010), and forwards the information to the store terminal 22.

The store terminal 22 then sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the QR authorized certification key 1201 was issued by the authentication server itself, only part of the information such as the authorization number and the personal authentication may be sent. FIG. 11 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1012). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1013), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR authorized certification key 1201, and the QR authorized certification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1014). In addition, the user will be notified verbally that a payment cannot be decided by the store staff.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) on the QR authorized certification key 1201 received from the store terminal 22 is recognized as a genuine one issued by the store terminal 22, the authentication server 41 returns the detailed settlement approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed authorization information on the display unit as user information (step 1015). FIG. 12(b) shows an example of this. The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1016).

If there is a response confirming the purchase intention from the person, the transaction is completed by operating the transaction button (step 1017). If the approval button operation is operated, the store

terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1018). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. In addition, the approval completion information is transmitted to the financial institution 42. As a result, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. This approval content 1301 can be stored until it is deleted by the user. However, since the QR authorized certification key 1301 is only valid once, it is automatically deleted after a predetermined period of time. In addition, the financial institution 42 that receives the approval completion information performs procedures to withdraw the amount from the user's designated account.

10

Based on the above, a decision can be made when purchasing products at general stores using a mobile phone 1. If the user withdraws his or her intent to purchase, the processing of the store terminal is terminated by a cancellation operation at the store terminal. In addition, even if the user himself or herself performs a cancellation operation on the mobile phone 1, the payment processing will be terminated midway and all information such as the QR authorized certification key 1301 will be deleted. As is clear from the explanations above, according to the transaction method, the payment can be approved only by the QR authorized certification key issued by authentication server 41 without conveying confidential information such as the credit number of the user to the store. In addition, since the configuration does not hold any confidential information such as credit card numbers in the mobile phone 1, even if the mobile phone 1 is lost, there is no risk of it being misused for payment settlement. Furthermore, as the validity of the mobile phone serial number and the mobile number is determined by the sign recorded by mixing the special crystalline powder, it is possible to prevent misuse due to modification of the mobile phone itself, and by increasing the security of devices used for the payments, it will have beneficial effects for both the users and stores.

20

Moreover, since the store only needs to add the reader 21, there is an advantage that the cost of joining the system can be reduced. Similarly, the mobile phone 1 can be used as a commercially available mobile phone without adding an IC card or the like. In addition, since the purchase history is managed, it is no longer necessary to issue a point card from the store side. Further, since the user can see the usage status, there is an advantage in that it is useful for making systematic purchase plans.

Also, by using a QR code, the recording contents can be read from any direction in 360 degrees, so there is no restriction on the positional relationship with the reading unit, and it is suitable for use by the general user to insert into the reader unit and read. Also, since it is not necessary to strictly define the positional relationship, the reading time can be shortened accordingly. In addition, even if some part of the code is dirty or damaged, the errors can be corrected, and the number of reading errors can be reduced. In particular, as in the present invention, when reading the data while it is displayed on the display of the mobile phone 1, it is conceivable that reading errors may occur due to dirt on the display unit, etc., but by using a QR code, reading errors caused by dirt on the display unit, etc. can be reduced. The QR authorized certification key is configured to include at least information on the approval number, personal authentication, name, and authorization method, but it may be a one-time password generated based on the approval number, personal authentication, or part or all of the name.

30

40

In this case, for example, the authentication server 41 and the mobile phone 1 are equipped with a password generation program based on the same logic, and when accessing for the second time, the mobile phone 1 automatically sends a password automatically generated based on the PIN number etc. sent on the first time. On the authentication server 41 side, authentication is performed by comparing the mobile phone number, etc., of the mobile phone 1 and the automatically transmitted password with the password automatically generated by the authentication server 41.

From the third time onward, a new password may be automatically generated and automatically sent based on the last automatically generated password.

By using such a so-called one-time password, security can be improved, and the input of a personal identification number can be omitted during the second and subsequent times of access.

50

Next, the method of deciding when purchasing small-value products such as drinking water from the vending machine 3 will be described with reference to the flowchart of FIGS. 14 and 15.

First, the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID of the vending machine 3 from which he or she intends to purchase the product. The user then inputs his or her personal identification number (the number registered in 706 in FIG. 7), the payment method, and the purchase price of the product (step 1401). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17. In addition, there are credit card payment, web money payment, debit card payment, and contactless IC card payment

methods, but since the payment amount is small, the use web money is made, and the web money account number (the number registered in FIG. 7-711) is entered.

When the input is complete, the transmission operation is performed. Then, the information input in step 1401 is sent to the authentication server 41 as the QR authorized certification key issuance request. The authentication server 41 that receives this request for issuing the QR authorized certification key information performs authentication processing for the store (here, the vending machine) and the user (step 1402). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store (vending machine) with the store ID is registered. Similarly, the user information DB 44 is searched by the PIN and the web money account number, and the user of the PIN and web money account number is checked to see if it is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). Furthermore, if the PIN and the web money account number are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1401 is automatically deleted.

However, if the store ID and the web money account number are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1404) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1405). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1406) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

The user inserts into the mobile phone 1 the QR authorized certification key 1201 displayed into the reading unit of the QR code reader 33 attached to the vending machine 3 (step 1407). Then, the selection operation of the vending machine 3 is performed for the desired product to be purchased (step 1408). In the vending machine 3, the price is automatically confirmed by selecting the desired product (step 1409).

The QR code reader 33 reads the QR authorized key 1201 displayed on the display unit 11 of the mobile phone 1 (step 1411) and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1410).

The vending machine 3 sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from mobile phone 1 to the authentication server 41 as a payment approval request. In this case, the communication line can utilize data communication using a PHS telephone. FIG. 15 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1412). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1413), after which an unauthorized use message is sent to the vending machine 3 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR authorized certification key 1201, and the QR authorized certification key 1201 displayed on the display unit 11 is deleted.

In the vending machine 3, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1414). However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all

or part) on the QR authorized certification key 1201 received from the vending machine 3 is recognized as a genuine one issued by the vending machine 3, the authentication server 41 returns the detailed settlement approval to the store terminal 22. This detailed approval information includes the same information as the QR authorized certification key 1201, as well as the purchase history information of the user.

The store terminal 22, which has received the detailed approval, immediately performs the approval process (step 1415). Then, an authorization completion message is sent to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1416). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. In addition, the approval completion information is transmitted to the financial institution 42. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13 (step 1417).

The financial institution 42 that has received the authorization completion message performs procedures to debit the user's web money account or credit account.

Based on the above, it is possible to use the mobile phone 1 to make a decision when purchasing a small-value item from a vending machine.

As is clear from the explanations above, even in the transaction method, the payment can be approved only by the QR authorized certification key issued by the authentication server 41 without conveying confidential information such as the user credit number to the vending machine side.

Next, an explanation will be given of the method of making a payment when purchasing a product at an electronic store on the Internet with reference to the flowcharts of FIGS. 16 and 17.

First, the user (product purchaser) sets his or her mobile phone 1 to the mobile shopping mode, and uses the input means 14 to access a store on the Internet. The user inputs the number of the product to be purchased, the purchase price, and the receiving method, and orders the product (step 1601).

The store that receives the order for the product sends a request for personal authentication to the authentication server 41. The authentication server 41 that receives this personal authentication request sends a request to the mobile phone 1 for inputting its personal identification number (the number registered in 706 in FIG. 7), the payment method, and the store ID.

Then, the user of the mobile phone 1 inputs his or her personal identification number (the number registered in 706 in FIG. 7), the payment method, and the store ID (step 1602). This content is sent to authentication server 41 as a request to issue a QR authorized certification key. Here, the decision-making method is the same as in the previous example.

The authentication server 41 that receives this QR authorized certification key request performs the authentication process of the user (step 1603). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched using the PIN number and the credit card number (or the web money account number, or debit card number), and it is checked whether the user with the PIN number and the credit card number (or the web money account number, or debit card number) is registered in the user DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1604). In addition, if the PIN and credit card number (or web money account number, or debit card number) are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1604). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1602 is automatically deleted.

However, if the store ID, the PIN number, and the credit card number (or web money account number, or debit card number) are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1605) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1606). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1607) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make

payments using this mobile phone; The message, "Please insert it into the reader at the time of payment at the pick-up store specified by the customer", will be displayed.

In addition, the authentication server 41 sends a request to the store to issue a certificate of trust. The store that receives this request for the issuance of a certificate of trust generates the certificate of trust that includes the trust number, user name, product number, amount, settlement method, and receipt method, and sends it back to the authentication server 41. This certificate of trust is equivalent to a product order form from the perspective of the user.

The authentication server 41 that receives the certificate of trust integrates the QR authorized certification key 1201 and the certificate of trust, and sends it to the mobile phone 1 as the certificate of trust with the QR authorized certification key.

10

The user then goes to the pick-up store that he or she has designated, and inserts the certificate of trust with the QR authorized certification key into the reader of the QR code reader 21 attached to the store terminal 22 of the pick-up store, with the certificate of trust displayed on the display unit 11 (step 1608). The QR code reader 21 then reads the QR authorized certification key (step 1609) displayed on the display unit 11 of the mobile phone 1, and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1610), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the certificate of trust with the QR authorized certification key read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the certificate of trust with the QR authorized certification key has been issued by the authentication server itself, only part of the information such as the payment number and the personal authentication may be sent. FIG. 17 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

20

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1611). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1613), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR authorized certification key, and the certificate of trust with the QR authorized certification key displayed on the display unit 11 is deleted.

30

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1613). In addition, the user is notified verbally that the store staff cannot deliver the product or make a payment decision.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and it is found that the information (all or part) on the certificate of trust with the QR authorized certification key received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 will reply to the store terminal 22 with detailed approval. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

40

The store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1614). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1615).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the transaction is completed by operating the transaction button (step 1616). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1617). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. In addition, the authentication server 41 sends the authorization completion information to the financial institution 42. Based on the above, the customer can select a product at a store on the Internet using the mobile phone 1, and receive and approve the product at a pick-up store designated by the user.

50

As is clear from the explanations above, according to the transaction method, the payment can be made only with the QR authorized certification key issued by authentication server 41, without conveying any confidential information such as the user's credit number to the store side on the Internet.

60

Such a method can be used to order tickets for movies, etc., on the Internet, and store the QR authorized certification key on the mobile phone 1, and insert it into the reader at the entrance of the movie theater, for example, to make use of the operational format such as entering the movie theater without a ticket. Here, instead of displaying the certificate of trust with the QR authorized certification key to the display unit 11 and having the reader 21 to read, a method can be adopted in which the certificate of trust with the QR authorized certification key is transferred to a personal computer (PC), printed with an attached printer, and read with a reading device at the receiving store. In this case, the printer's printing toner or ink mixed with the crystal powder similar to the signs 19 and 20 can be used.

FIG. 18 is a flowchart illustrating the procedure. This flowchart corresponds to the continuation of FIG. 16.

First, if the QR authorized certification key is received on the mobile phone 1, the QR authorized certification key is forwarded to a personal computer (PC) (step 1620) and printed with the attached printer (step 1621). A printing example is shown in FIG. 19(a).

Therefore, the user brings the printed certificate of trust with the QR authorized certification key to the receiving store designated by the user, and inserts it into the reading unit of the QR code reader 21 attached to the store terminal 22 at the receiving store. The QR code reader 21 then reads the printed certificate of trust with the QR authorized certification key (step 1622) and forwards the reading to the store terminal 22.

The store terminal 22 then sends the results of the reading of the certificate of trust with the QR authorized certification key to the authentication server 41 as a request for approval, as in the case of FIG. 17.

When the authentication server 41 receives a request for approval, it first examines the validity of whether the QR authorized certification key of the certificate of trust with the QR authorized certification key is genuinely issued by the customer (step 1623). If the result is that it is not legitimate, it is determined that it is fraudulent use, and after registering this with the unauthorized usage information database (FIG. 9) (step 1624), an unauthorized usage message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR authorized certification key, and the certificate of trust with the QR authorized certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1625). In addition, the user is notified verbally that the store staff cannot deliver the product or make a payment decision.

However, if it is found that the QR authorized certification key is genuine, the authentication server 41 will reply to the store terminal 22 with the detailed approval. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1626). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1627).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the transaction is completed by operating the transaction button (step 1628). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1629). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. In addition, the authentication server 41 sends the authorization completion information to the financial institution 42. Based on the above, even if the user does not bring his or her mobile phone 1, the user can receive the product ordered at a store on the Internet at the receiving store designated by the user and make the final payment.

In this case, it is not necessarily essential to transfer the certificate of trust with the QR authorized certification key from the mobile phone 1 to a personal computer (PC), and it may be received directly from the personal computer as a network terminal and printed with a printer.

Using these methods, it is possible to use the printed certificate of trust with the QR authorized certification key in place of, for example, movie tickets ordered over the Internet. FIG. 19(b) shows an example of an admission ticket.

In each of the above examples, it is explained that the same mobile phone 1 is used as a network terminal that transmits information about the payment, etc., of products and as a network terminal that receives code character information images such as a QR payment certification key, but it is not limited to this, and the network terminal for transmitting information and the network terminal for receiving the code character information images may be used as a separate terminal.

By using this, it is also possible to transmit the code character information image to a third party's network terminal. Therefore, instead of gifting products or gift certificates to a third party, it is possible to make a payment using a code character information image transmitted to the third party's network terminal.

A payment processing method in this case will be explained below with reference to FIGS. 20 to 28.

In this case, the payment authorization institution 4 is provided with a gift information database (DB), and the authentication server 41 is provided with a gift information registration processing program 412. As shown in FIG. 20, for example, the gift information DB stores information including the giver ID 2001, the receiver ID 2002, the gift details 2003, the identification ID 2004, and the payment processing date 2005.

In addition, the gift information registration processing program described above is a program used when registering information on specific products or gifts of a certain amount in the gift information DB using the system.

In this payment processing method, the ordering party (the giver of the product) first sets the mobile phone 1 as an information transmitting terminal to the mobile shopping mode, and then uses the input means 14 to enter his or her identification PIN (the number registered in 706 in FIG. 7), payment method, user name of the recipient of the product and the recipient information such as the user ID, and gift details (in this case, the item number of the product to be gifted) (step 2101). Here, the payment method is the same as in the previous example.

When the input is complete, the transmission operation is performed. The information entered in step 2101 is then sent to authentication server 41 as a gift information transmission request.

The authentication server 41 that receives this gift information transmission request performs the authentication process of the user (step 2102). That is, the user information DB 44 is searched by the PIN number, the credit card number (or web money account number, or debit card number) included in the gift information transmission request, and the user of the PIN and the credit card number (or web money account number, or debit card number) is checked to see if the user is registered in the user information DB 44. In addition, the user information DB 44 is searched by the user ID, etc. as the recipient information, and as a result, if the PIN and the credit card number (or web money account number, or debit card number) are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 2103). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and information such as the PIN entered in step 2101 is automatically deleted.

However, if the PIN number, the credit card number (or web money account number, or debit card number), the user ID as the recipient information, and the user name are registered correctly, the user is authenticated as an officially registered user, and the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 2104) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or gift information is sent (step 2105). In other words, of a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message including a message such as insufficient balance to the giver's mobile phone 1. However, if the credit result is OK, the gift information is sent to the recipient's mobile phone 1 input in step 2101. As for this gift information, as shown in FIG. 24(a), the giver's user name and the product name as the gift contents are displayed, and the recipient sends back information to the authentication server 41 regarding refusal or acceptance of the gift contents (step 2106). If the authentication server 41 receives this reply and the information of a rejection is returned, it sends a confirmation message to the recipient's mobile phone 1 to that effect, and after sending a message of the rejection to the giver's mobile phone (see Fig. 24(c)), the information such as the PIN entered in step 2101 is automatically deleted. (step 2107) However, if the information of acceptance is returned, the authentication server 41 sends a request to the recipient's mobile phone 1 to enter the method of receiving the goods (see FIG. 24(b)).

Therefore, the user of the mobile phone 1 enters the store ID and the receiving method (step 2108). The contents are then sent to the authentication server 41 as a QR payment certification key issuance request. The authentication server 41 that receives this QR payment certification key request performs the authentication process of the store (step 2109). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined

whether or not the store with the store ID is registered. As a result, if the store ID is not registered, it is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the recipient's mobile phone 1 (step 2110). In the mobile phone 1, after confirming that the message indicating that the transaction is not possible is displayed on the display unit 11, another store ID or the like can be inputted.

However, if the store ID is registered correctly, the store is authenticated as an officially registered store, and the authentication is accepted.

If the authentication is OK, the authentication server 41 generates a QR payment certification key configured with a two-dimensional code as shown in FIG. 3(d). (Step 2211) The QR payment certification key includes at least the payment number, the personal identification, name, and the payment method information.

10

In addition, the authentication server 41 sends a request to the store to issue a certificate of trust. The store that receives this request for the issuance of a certificate of trust generates the certificate of trust that includes the trust number, user name, product number, amount, payment method, and receipt method, and sends it back to the authentication server 41. This certificate of trust is equivalent to a product order form from the perspective of the user.

The authentication server 41 that has received the certificate of trust combines the QR payment certification key 1201 with the certificate of trust and transmits it to the recipient's mobile phone 1 as a certificate of trust with the QR payment certification key.

In the mobile phone 1, the received QR payment certification key is displayed on the display unit 11 as shown by the reference numeral 1201 in FIG. 12. At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

20

The user then goes to the pick-up store that he or she has designated, and inserts the certificate of trust with the QR payment certification key into the reader of the QR code reader 21 attached to the store terminal 22 of the pick-up store, with the certificate of trust displayed on the display unit 11 (step 2112). The QR code reader 21 then reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 2113), and reads the QR payment certification key with the certificate of trust displayed on the display unit 11 of the mobile phone 1 (step 2114), and forwards the reading to the store terminal 22.

30

The store terminal 22 sends the mobile phone serial number, mobile phone number, and the certificate of trust with the QR payment certification key read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, as for the certificate of trust with the QR payment certification key, it is only necessary to know that it has been issued by the authentication server 41 itself, so only some information such as the payment number and personal authentication may be sent. FIG. 23 shows that only the payment number and the personal authentication information is sent in the payment authorization request.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2115). As a result, if either number is unregistered or different from the registered number, it is determined to be unauthorized use and after registering in the unauthorized use information database (FIG. 9) (step 2116), an unauthorized use message is sent to the store terminal 22 and the mobile phone 1 on the receiving side. In addition, an unauthorized use messages is also sent to the mobile phone 1 on the giver side.

40

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR payment certification key, and the certificate of trust with the QR payment certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2117). In addition, the user is verbally notified that the store staff cannot deliver the product and that payment cannot be made.

50

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and it is found that the information (all or part) on the certificate of trust with the QR payment certification key received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 will reply to the store terminal 22 with detailed payment approval. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed payment approval, displays all or part of the received

detailed payment information as user information in the display unit (step 2118). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 2119).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the payment is completed by operating the payment button (step 2120). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41.

The authentication server 41 that receives this payment completion message updates the purchase history information of the user on the giver side (step 2121). After this, the payment details for confirmation are sent to the terminal for information transmission on the giver's side. As a result, a confirmation message and the payment details 2501 and 2502, as shown in FIG. 25, are displayed on the display unit 11 of the giver's mobile phone 1, for example (step 2122). In addition, the authentication server 41 sends the payment completion information to the financial institution 42.

Based on the above, a specific product can be selected using the giver's terminal, and the product can be received and settled at a store designated by the recipient.

As is clear from the above explanation, according to the transaction method, payment can be made only with the QR payment certification key issued by authentication server 41 without conveying any confidential information such as the credit number of the giver to the store or the recipient of the gift. Furthermore, the recipient of the gift can be authenticated more reliably.

In this transaction method, the gift information is sent to the recipient and the recipient chooses whether or not to accept the gift, although the recipient who will accept or reject the gift is set in advance. The authentication server may decide whether to accept or reject the gift based on this setting. In this case, the above determination processing at the authentication server is performed instead of step 2106 and step 2107.

In addition, the contents of gifts given by this system may be not limited to specific products, but it may be content equivalent to a gift certificate of a certain gift amount.

FIGs. 26 and 27 are flowcharts illustrating the procedure in such a case. The flowchart in FIG. 26 corresponds to the continuation of FIG. 21.

In this case, as a prerequisite, in step 2101 of FIG. 21, a certain amount will be entered in place of the item number as the gift content.

Thereafter, after the processing shown in the flowchart of FIG. 21 is performed, the user on the receiving side inputs the receiving store ID and the purchase price of the product (step 2130). The contents are then sent to the authentication server 41 as a QR payment certification key issuance request. The authentication server 41 that receives this QR payment certification key issuance request performs the authentication process for the store and the purchase amount (step 2131). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. The gift information DB is also searched to check whether the input purchase amount is within the range of the amount stored in the DB. As a result, if the store ID is not registered or the purchase amount exceeds the gift amount, a non-transactionable message is returned to the mobile phone 1 (step 2132). On the receiver's mobile phone 1, after confirming that the message indicating that the transaction is not possible is displayed on the display unit 11, the recipient enters another store ID or purchase amount. However, if the store ID is registered correctly and the purchase amount entered is within the range of the gift amount, the product is certified to be the amount that can be purchased at the store with the official registration, and the certification is accepted.

If the certification is OK, the authentication server 41 generates a QR payment certification key composed of a two-dimensional code as shown in FIG. 3(d) and sends it to the mobile phone 1 (step 2133). The QR payment certification key includes at least the payment number, the personal identification, name, and the payment method information.

In the mobile phone 1, the received QR payment certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 2134). The store staff enters the price of the desired purchase item using the store terminal (step 2135).

In parallel, the user inserts and attaches the mobile phone 1 with the QR payment key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 2136). The QR code reader 21 then reads the QR payment certification key 1201 displayed on the display unit 11 of the mobile phone 1 on the receiving side (step 2137), and reads the mobile phone serial number and the

mobile phone number from the signs 19, 20 (step 2138), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the QR payment certification key 1201 read from the mobile phone 1 on the receiving side to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the QR payment certification key 1201 was issued by the authentication server itself, only part of the information such as the payment number and the personal authentication may be sent. When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2139). As a result, if either number is unregistered or different from the registered number, it is determined to be unauthorized use and after registering in the unauthorized use information database (FIG. 9) (step 2140), an unauthorized use message is sent to the store terminal 22 and the mobile phone 1 on the receiving side. In addition, an unauthorized use messages is also sent to the mobile phone 1 on the giver side.

10

In the receiver's mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR payment certification key 1201, and the QR payment verification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2141). In addition, the user is notified verbally that payment cannot be made by the store staff.

20

However, if both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) of the QR payment certification key 1201 received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 returns the detailed payment approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed payment approval information as user information in the display unit (step 2142). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 2143).

30

If there is a confirmed response of the person's purchase intention, the payment is completed by the payment button operation (step 2144). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41. The authentication server 41 that receives this payment completion message updates the purchase history information of the user on the giver side (step 2145). Thereafter, the payment details for confirmation are transmitted to the mobile phone 1 of the giver. In addition, the payment completion information is sent to financial institution 42. As a result, for example, the payment details 2501 and 2502 for confirmation as shown in FIG. 25 are displayed on the display unit 11 of the giver's mobile phone 1 (Step 2146). The payment details 2501 and 2502 can be stored until deleted by the user. However, since the QR payment certification key 1201 is valid only once, it is automatically deleted after a prescribed time. In addition, the financial institution 42, that receives the payment completion information, takes procedures to debit the payment from the designated account of the user on the giver's side.

40

Based on the above, a certain amount can be specified using the terminal on the giver's side, and the recipient can freely purchase products, etc. at the store within the range of that amount, and settle the payment.

As is clear from the explanation above, according to the transaction method, even if a gift certificate of a certain amount is given, the payment can be made from the account of the giver only by the QR payment certification key issued by authentication server 41, without the store or the receiver receiving the confidential information such as the credit number of the giver. Further, the recipient can be authenticated more reliably.

50

In addition, in each of the above examples, payment by a financial institution is assumed, but the present invention can also be used when making payment by service points for all or part of the payment price. A payment processing method in this case will be explained below with reference to FIGS. 28 to 30.

In this case, the payment authorization institution 4 is provided with a service point database (DB), and the authentication server 41 is provided with a service point registration processing program.

FIG. 28 is a diagram illustrating an example of the storage information for the service point DB, in which the update date 2801, the store name 2802, the number of additional points 2803, the number of

points used 2804, and the service point balance 2805 are stored. This service point information is stored for each user in the order of update the date and time.

In addition, the service point registration processing program performs the payment processing based on service points obtained by purchasing products using this system.

Moreover, there are cases where the use of service points is processed by discounting the amount equivalent to a certain amount at the time of purchase of products based on the number of points, and where the service points are exchanged for products determined in advance based on the number of points, but in this embodiment, it is indicated that the service points are processed as the purchase price of the products.

In this payment processing method, the user (product purchaser) first sets the mobile phone 1 to the mobile shopping mode, and then using the input means 14, the user inputs the store ID of the store from which the product is to be purchased, along with his or her personal identification number (the number registered in 706 in FIG. 7), and the service points corresponding to the purchase price of the product (step 2901). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17.

When the input is complete, the transmission operation is performed. The information entered in step 2901 is then sent to authentication server 41 as a request to issue a QR payment certification key.

The authentication server 41 that receives this QR payment certification key issuance request performs authentication processing for the store and the user (step 2902). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched by PIN to see if the user is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 2903). Furthermore, if the PIN is not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 2901 is automatically deleted.

However, if the store ID and PIN are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the service point DB of the user is searched to inquire about the service point balance (step 2904). In response to this inquiry result, a non-transactionable message or QR payment certification key is generated (step 2905). In other words, if the result of the inquiry is that there is no balance, the authentication server 41 sends a non-transactionable message including a message such as insufficient balance to the mobile phone 1. However, if there is a balance, a QR payment certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 2906) and transmitted to the mobile phone 1. The QR payment certification key includes at least the payment number, the personal authentication, and name information.

In the mobile phone 1, the received QR payment certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 2907). The store staff calculates the number of points corresponding to the purchase price by entering the price of the desired product in the store terminal (step 2908). In parallel, the user inserts and attaches the mobile phone 1 with the QR payment key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 2909). The QR code reader 21 then reads the mobile phone serial number and the mobile phone number from the signs 19, 20 of the mobile phone 1 (step 2910), and reads the QR payment certification key 1201 displayed in the display 11 (step 2911), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the QR payment certification key 1201 read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, it may be understood that the QR payment certification key 1201 was issued by the authentication server itself, so only some information such as the payment number and the personal authentication may be sent. FIG. 30 shows that only the payment number and the personal authentication information is sent in the payment authorization request.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details

of the user information DB 44 (step 2912). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 11) (step 2913), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that receives the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR payment certification key 1201, and the QR payment certification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2914). In addition, the user is notified verbally that payment cannot be made by the store staff.

However, if both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) of the QR payment certification key 1201 received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 returns the detailed payment approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed payment approval information as user information in the display unit (step 2915). The store staff confirms the purchase intent with the user themselves by looking at the display content, and the content of the desired product to be purchased, and the number of points corresponding to the price (Step 2916).

If there is a confirmed response of the person's purchase intention, the payment is completed by the payment button operation (step 2917). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41. The authentication server 41 that receives this payment completion message updates the user's purchase history information and service point information (step 2918). After this, the payment details for confirmation are sent to the mobile phone 1. The payment details can be saved until the user deletes them. However, since the QR payment certification key 1201 is valid only once, it is automatically deleted after a prescribed time.

Based on the above, it is possible to use a mobile phone 1 to make payments using service points when purchasing products at general stores.

As is clear from the explanations above, according to the transaction method, even when making a payment using service points, it is possible to perform the payment using only the QR payment certification key issued by the authentication server 41, making it possible to eliminate the need for a point card or the like. In addition, the authentication of service users can be performed more reliably.

The methods shown in each of the above examples do not require financial settlement, but can be used instead of tickets such as admission tickets or receipts for goods, etc. It should be noted that the procedures described above can be implemented with some changes depending on the financial institution or the like. Furthermore, the procedure performed by the authentication server 41 may be recorded as a program for decision making on a recording medium such as a CD-ROM, and provided to the decision-making system builder.

Although the mobile phone serial number and the mobile phone number signs are recorded using recording materials mixed with a special crystalline powder, other methods of recording in a recording format that can physically determine the authenticity may be used.

In addition, in the next-generation mobile communication services that use mobile phones etc. equipped with an IC card (UIM card), the mobile phone numbers etc. are written on the IC card, and an operation mode is being considered in which the same mobile phone number can be used on different terminals by replacing the IC card.

Thus, in this case, the IC card may be labeled or printed as shown in FIG. 3(c).

In addition, in this case, it is necessary to make the sign readable by an external reader while the IC card is inserted into the slot provided in the mobile phone or the like.

Examples of handsets used in this case will be described with reference to FIGS. 31 and 32.

FIGS. 31 and 32 are partial perspective views of a mobile phone used in the present embodiment, wherein in each figure, the IC card installed in the mobile phone that stores information such as the mobile phone number is represented by the number 300, and a sign 311 as shown in FIG. 3(c) is pasted or printed on the surface of the IC card. It should be noted that, in place of the serial number of the mobile phone, the identification information of each IC card or of the owner is recorded on the sign 311 together with the mobile phone number.

In the present embodiment, a recess 300 is formed that allows the IC card to be mounted such that the sign 311 affixed to the IC card is visible from the reading direction, as shown by the arrow in the figure,

and such as on the back side of the mobile phone 1, for example, as shown in FIG. 31(a). This allows the reader 22 to read the label in the same way as when a label is affixed on the casing of the mobile phone 1.

Also, as shown in FIG. 31(b), an IC card insertion slot 301 found in the mobile phone 1 may be provided, and an opening 302 may be formed in the area where the sign 311 is located so that the sign can be read (visually recognized) by an external reading device when the IC card 310 is inserted into the slot 301. The front surface of the opening 302 may be shielded with a transparent resin material or the like, as long as the sign 311 is visible from the reading direction shown by the arrow in the figure.

Other configurations may also be used if the sign 311 can be read by an external reader, for example, the entire casing of the mobile phone may be made of a transparent resin material or the like that allows the inside to be seen.

In this way, the invention can be applied to mobile phones, etc. that support the next generation of mobile communication services, and in addition, it is possible to increase security by eliminating the need to store data such as credit card numbers in the IC cards.

It should be noted that the mobile phone 1 may be provided with a reading device for the sign 311, and the reading device may read the sign and transmit the read information to the store terminal.

In this case, for example, as shown in FIG. 32(a), a reading sensor unit 303 connected to the control unit 13 (see FIG. 2(a)) is provided at a location where the mark 311 of the IC card inserted into the slot 301 is located. As a result, the information on the sign 311 read by the reading sensor unit 303 can be transmitted to the authentication server 41 via the transmitting means of the mobile phone 1. It should be noted that the processing of reading information on the sign 311 may be performed while the IC card is inserted into the slot 311, and in this case, a sensor unit may be provided in the portion of the slot corresponding to the portion through which the marker 311 passes.

Moreover, as shown in FIG. 32(b), the IC card 310 is not limited to the one that is inserted into the mobile phone 1, and by inserting a part of the IC card 310 into the slit 304 formed on the side of the mobile phone 1, and sliding it in the sliding direction shown by the arrow in the figure, it is conceivable that the information in the IC card 310 may be read by the sensor unit (not shown). In this case, when sliding a portion of the IC card 310 into the slit 304, a portion of the site corresponding to the site through which the sign 311 passes within the slit 304 may be provided with a reading sensor unit 305.

In addition, when using a wireless or optical non-contact type IC card as the IC card 310, and by inserting the IC card 310 into a reading device installed at each store etc., the sign 311 may be read directly; or as with the above example, the mobile phone 1 may be equipped with a reading device, and the information on the sign 311 may be recognized by radio or light, similar to the information in the IC card 310.

[Brief Description of Drawings]

FIG. 1 is a system configuration diagram showing an embodiment of a system implementing the commercial transaction method of the present invention.

FIG. 2 is a schematic block diagram illustrating a configuration of a mobile phone.

FIG. 3 is a diagram showing an example of a label, a barcode, and a two-dimensional code attached to a mobile phone.

FIG. 4 is a cross-sectional configuration diagram of a reading device that reads the barcode attached to the mobile phone and a two-dimensional code displayed on the display unit.

FIG. 5 is an internal configuration diagram of an authentication server.

FIG. 6 is a diagram illustrating an example of the data stored in the store information database.

FIG. 7 is a diagram illustrating an example of the data stored in the user information database.

FIG. 8 is a diagram illustrating an example of the data stored in the purchase history database.

FIG. 9 is a diagram illustrating an example of the data stored in the unauthorized information database.

FIG. 10 is a flowchart illustrating the procedure for using a mobile phone to settle the price of goods at a general store.

FIG. 11 is a flowchart showing a continuation of FIG. 10.

FIG. 12 is a diagram illustrating an example of a QR payment certification key displayed on the mobile phone and the user information displayed on the store terminal.

FIG. 13 is a diagram illustrating an example of the confirmation information displayed on the mobile phone at the end of payment.

FIG. 14 is a flowchart showing the procedure for the payment of small-value products at a vending machine.

FIG. 15 is a flowchart illustrating the continuation of FIG. 14.

FIG. 16 is a flowchart illustrating the procedure for receiving and clearing items ordered at stores on the Internet at designated receiving stores.

FIG. 17 is a flowchart illustrating the continuation of FIG. 16.

FIG. 18 is a flowchart showing the procedure for bringing a printed copy of the QR payment certification key to the store for payment.

FIG. 19 is a diagram illustrating an example of a printed QR payment certification key.

FIG. 20 is a diagram illustrating an example of the data stored in the gift information database.

FIG. 21 is a flowchart showing the procedure for paying for a gift to another person.

FIG. 22 is a flowchart illustrating the continuation of FIG. 21.

FIG. 23 is a flowchart illustrating the continuation of FIG. 22.

FIG. 24 is a diagram illustrating a display example of the gift information displayed on a mobile phone and a display example after selecting acceptance or rejection of the gift.

FIG. 25 is a diagram illustrating an example of the confirmation information displayed on the giver's mobile phone at the end of payment.

FIG. 26 is a flowchart illustrating the continuation of FIG. 21.

FIG. 27 is a flowchart illustrating the continuation of FIG. 26.

FIG. 28 is a diagram illustrating an example of a service point usage history database.

FIG. 29 is a flowchart illustrating the procedure for making a payment using service points at a general store using a mobile phone.

FIG. 30 is a flowchart illustrating the continuation of FIG. 29.

FIG. 31 is a partial perspective view illustrating an example of a mobile phone used in the present invention.

FIG. 32 is a partial perspective view illustrating an example of a mobile phone used in the present invention.

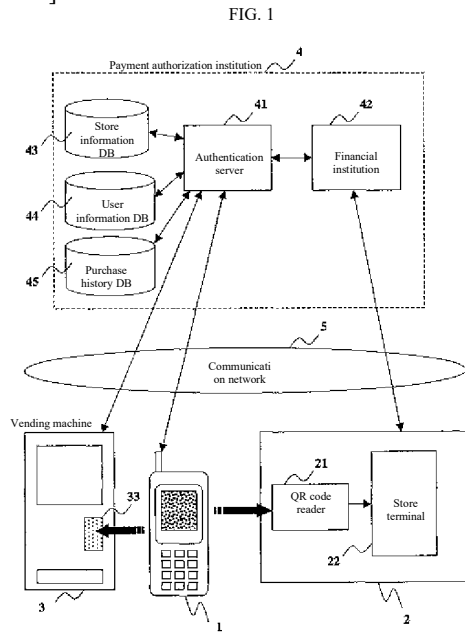
10

20

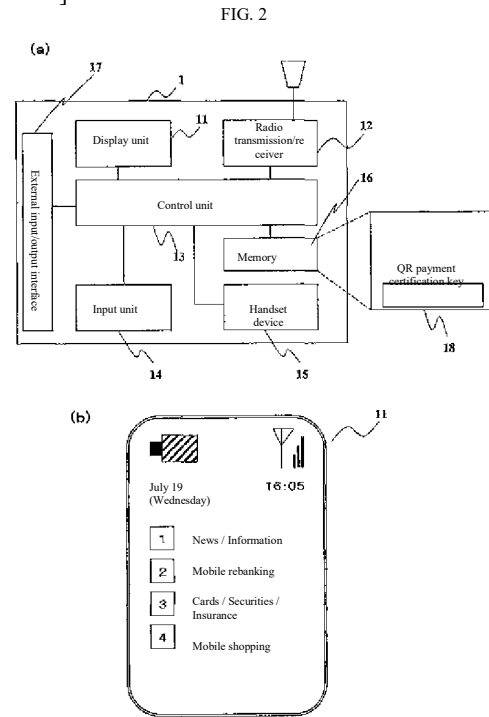
30

40

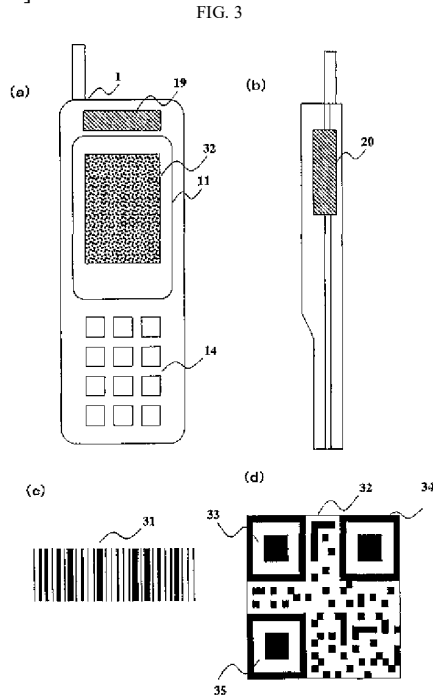
[FIG. 1]



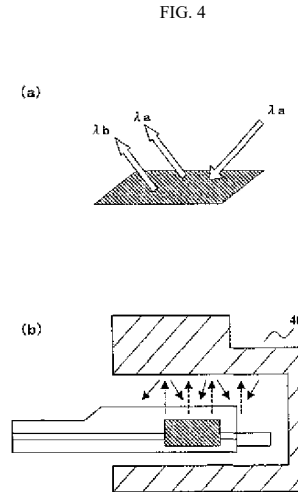
[FIG. 2]



[FIG. 3]

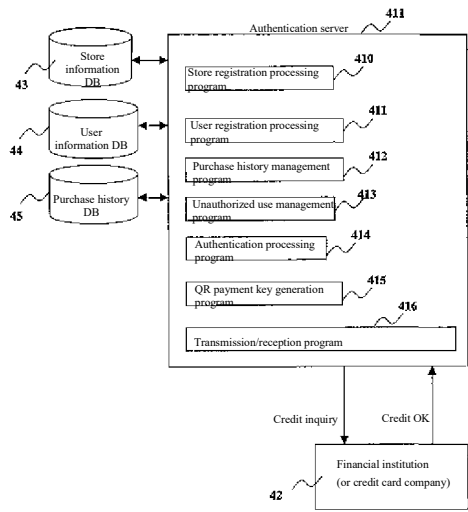


[FIG. 4]



[FIG. 5]

FIG. 5



[FIG. 6]

FIG. 6

Store information database				
Store ID	Store name	Address	Tel. No.	
AA001	AB	1-2-1 XX-cho, Chuo-ku, Tokyo	03-3221-XXXX	
AA002	Supermarket	5-3-4 XX-cho, Meguro-ku, Tokyo	03-3332-XXXX	
AB199	AF Vending machine	3-1-1 YR-cho, Shinagawa-ku, Tokyo	03-4521-XXXX	

[FIG. 7]

FIG. 7

User information database				
User ID	User name	Address	Mobile phone number	Mobile phone number (PIN number)
UR001	Kimura XX	5-2 XX-cho, Chuo-ku, Tokyo	MMAB1234	090-3221-XXXX 4123
UR002	Tanaka XX	3-1 XX-cho, Meguro-ku, Tokyo	MMAB1235	090-3332-XXXX 9198
UR199	Sato XX	1-1 YR-cho, Shinagawa-ku, Tokyo	MMAB9913	090-4521-XXXX 0678

Personal feature information database				
Gender	Date of birth	Debit card number	Credit card number	Web money account number
Male	1960/05/05	ABC Bank 12389	NNM23567	WJNS678

[FIG. 8]

FIG. 8

Purchase history database					
Date and time of purchase	Name of store	Payment amount	Cumulative amount used	Cumulative service points	Date of last use
0007/12	AB Supermarket	¥6500	¥16500	165P	0007/11
0007/13	AB Supermarket	¥2130	¥18630	196P	0007/12
0007/14	AZ Department store	¥4520	¥23150	241P	0007/13

[FIG. 9]

Unauthorized use information database

901	902	903
Mobile phone serial number	Mobile phone number	Store ID
XXXXXXXXXX	093-12345678	001
XXXXXXXXXX	093-12345678	002
XXXXXXXXXX	093-12345678	003
XXXXXXXXXX	093-12345678	004
XXXXXXXXXX	093-12345678	005
XXXXXXXXXX	093-12345678	006
XXXXXXXXXX	093-12345678	007
XXXXXXXXXX	093-12345678	008
XXXXXXXXXX	093-12345678	009

FIG. 9

[FIG. 10]

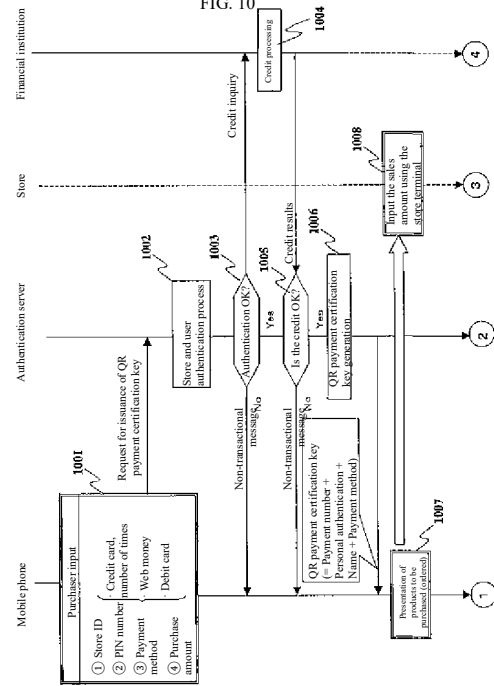


FIG. 10

[FIG. 11]

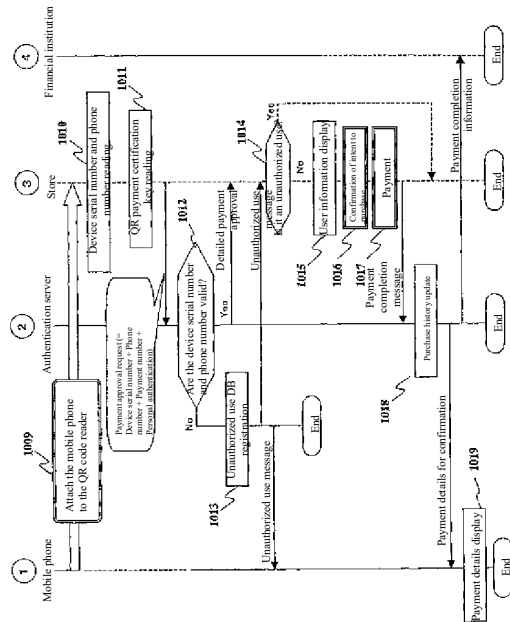


FIG. 11

[FIG. 12]

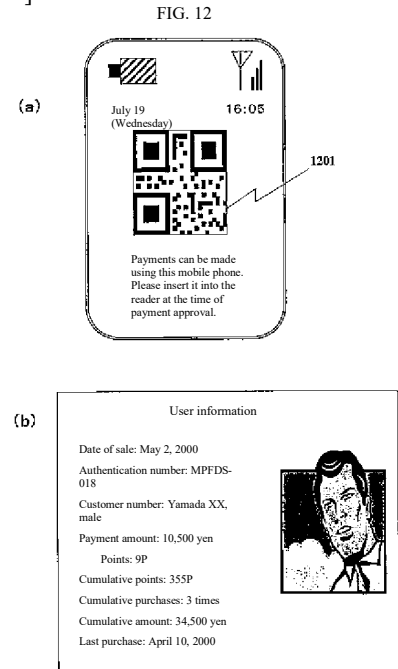


FIG. 12

[FIG. 15]

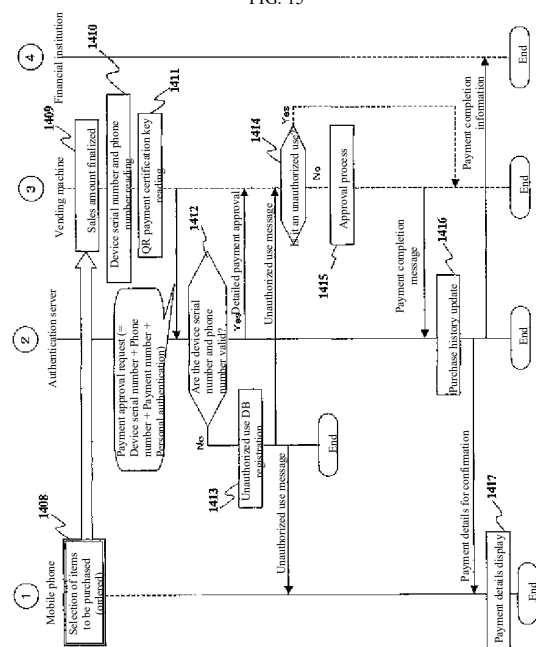


FIG. 15

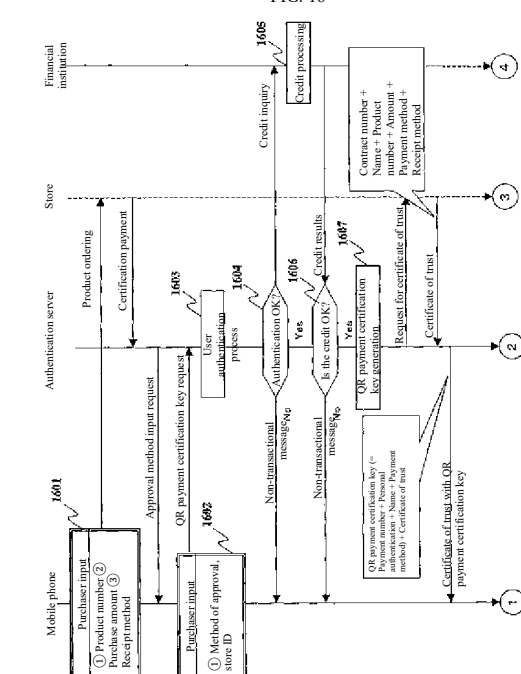
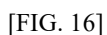
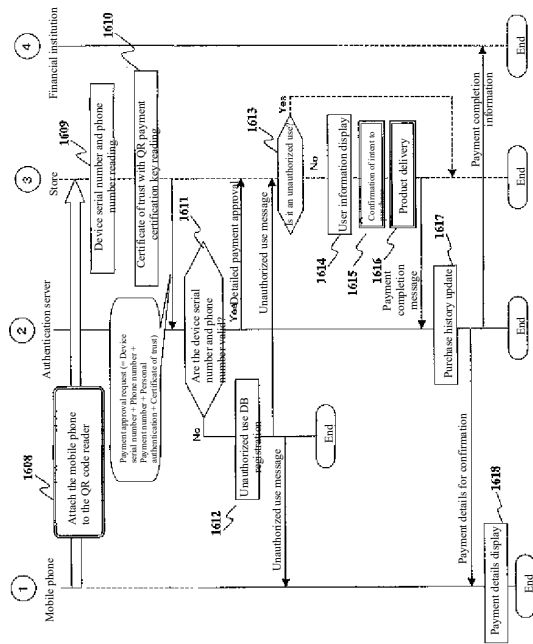
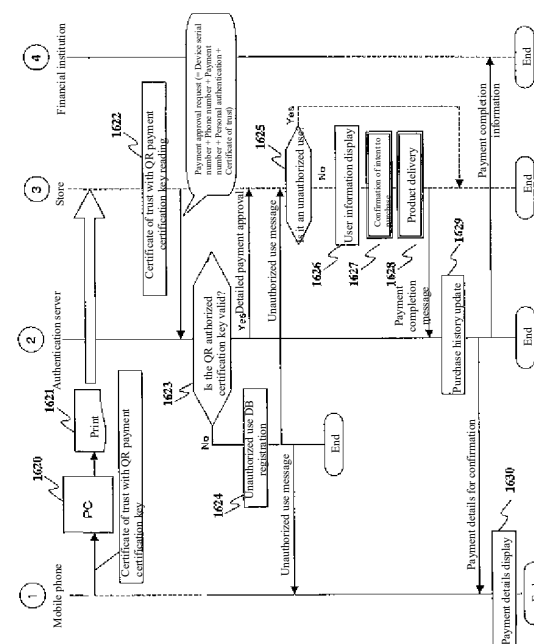


FIG. 16

[FIG. 17]



[FIG. 18]



[FIG. 19]

FIG. 19

(a)

Certificate of trust

1. Item number _____

2. Customer name _____

3. Amount _____

4. Approval method _____

5. Pick-up location _____

(b)

Admission ticket

1. Item number _____

2. Customer name _____

3. Amount _____

4. Approval method _____

5. Pick-up location _____

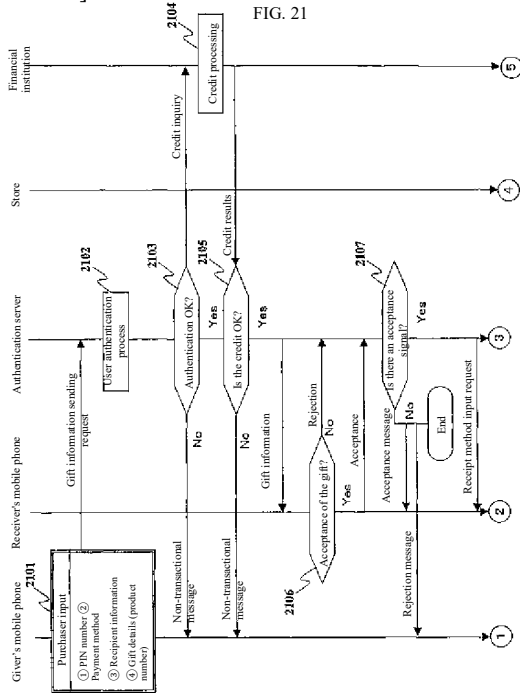
[FIG. 20]

FIG. 20

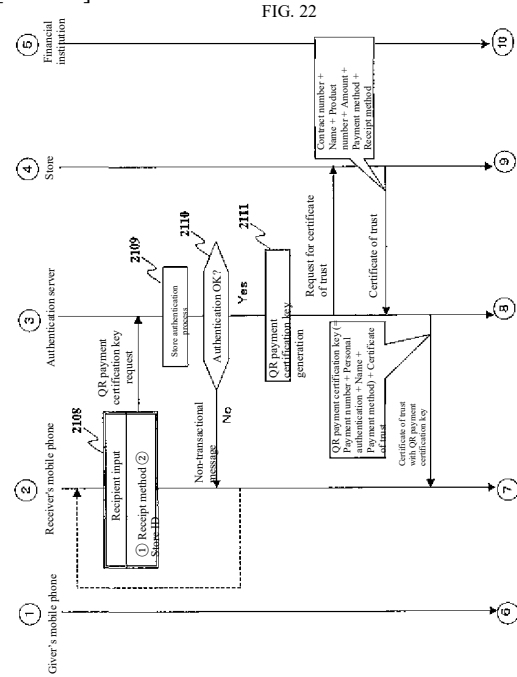
Gift information database

2001	2002	2003	2004	2005
Giver side ID	Receiver ID	Gift details	Identification	Payment processing date
UR001	UR005	00000	P2885	600715
UR045	UR179	¥10,000	P5975	0007120
UR135	UR024	0000	P2498	-

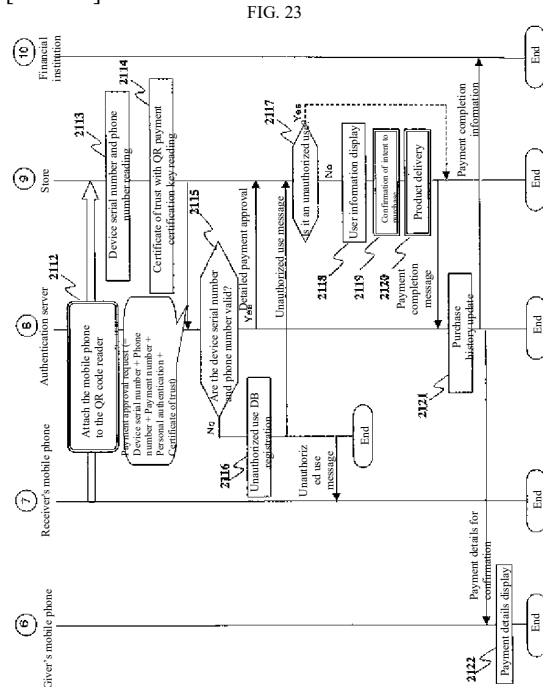
[FIG. 21]



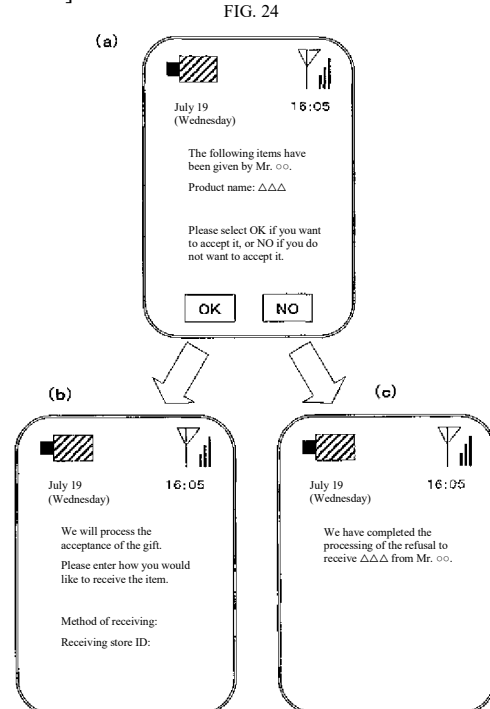
[FIG. 22]



[FIG. 23]

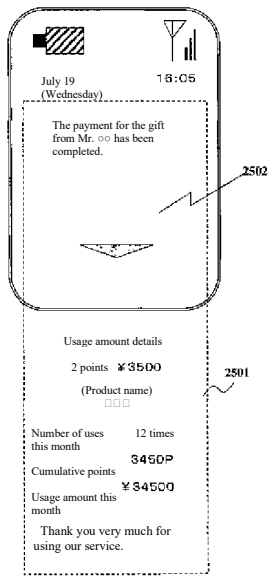


[FIG. 24]



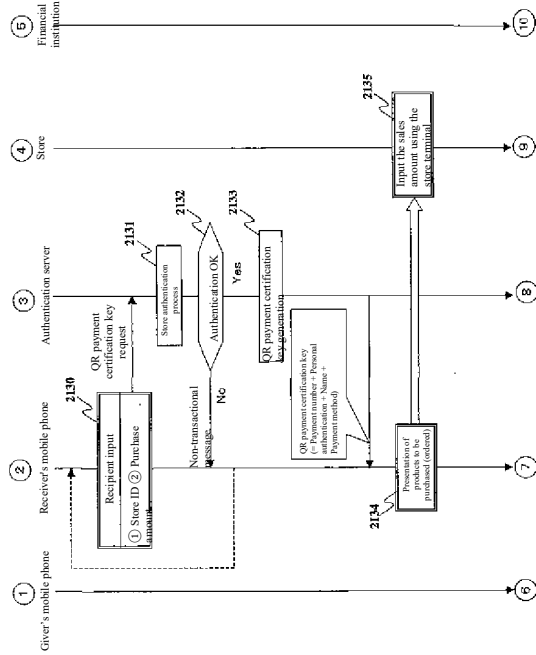
[FIG. 25]

FIG. 25



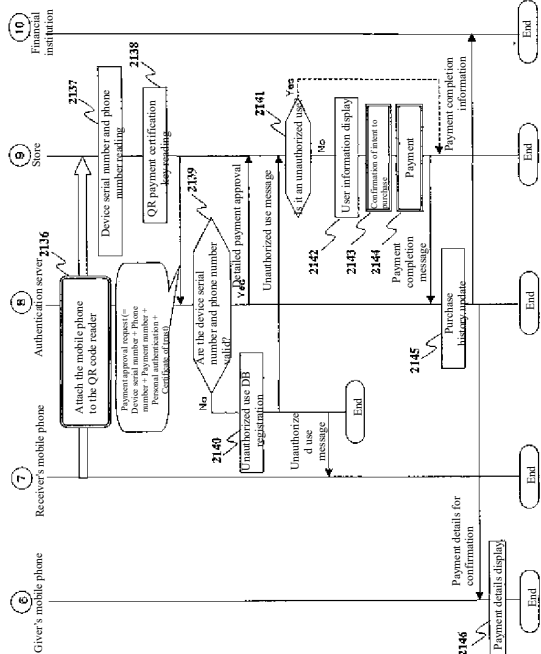
[FIG. 29]

FIG. 26



[FIG. 27]

FIG. 27



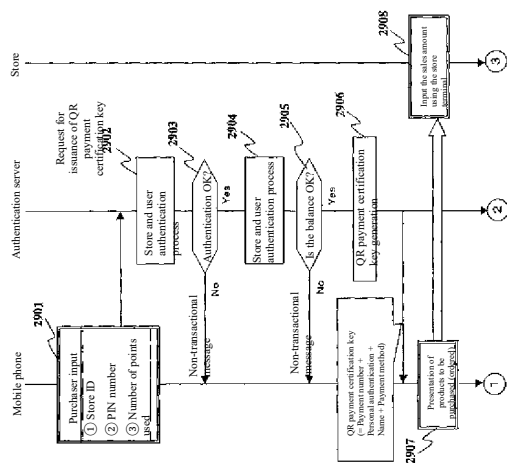
[FIG. 28]

FIG. 28

Service point database					
2801	2802	2803	2804	2805	
Updated date	Name of store used	Number of points added	Number of points used	Service point balance	
0007/12	AB Supermarket	65P	—	165P	
0007/13	AB Supermarket	31P	—	196P	
0007/14	AZ Department store	45P	—	341P	
0007/15	BC Department store	—	200P	141P	

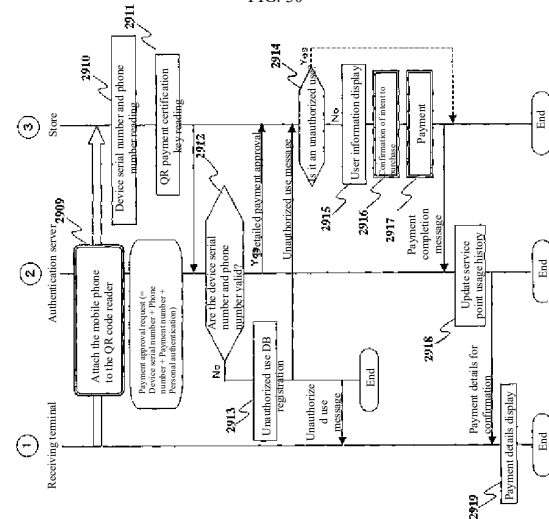
[FIG. 29]

FIG. 29



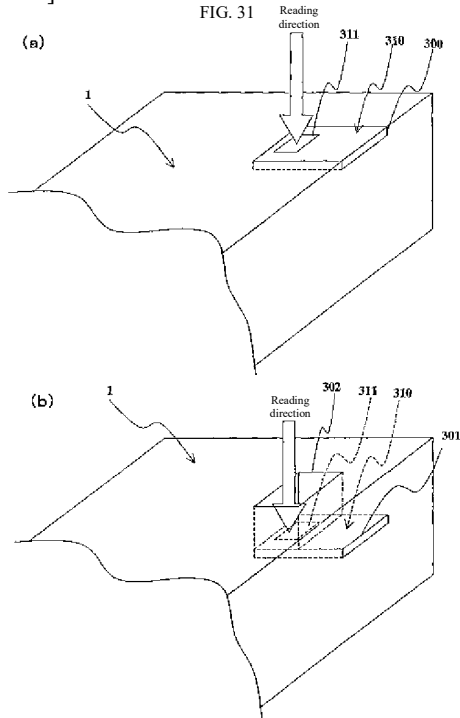
[FIG. 30]

FIG. 30



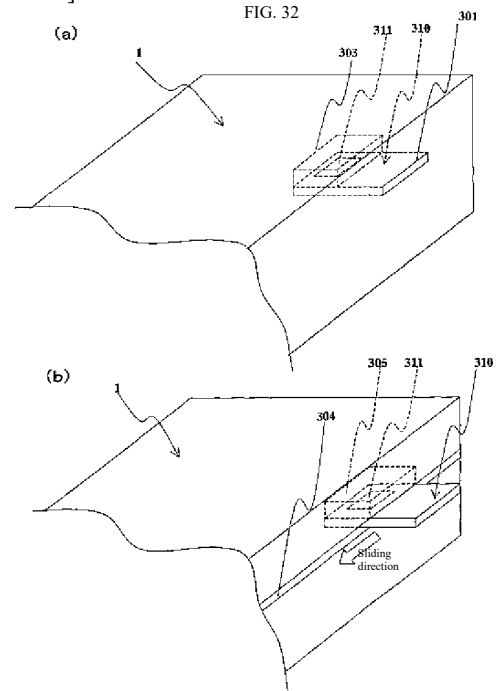
[FIG. 31]

FIG. 31



[FIG. 32]

FIG. 32



[Procedural amendment]

[Submission date] February 14, 2002 (2.14.2002)

[Procedural amendment 1]

[Name of document subject to amendment] Specification

[Name of items subject to amendment] Scope of claims

[Correction method] Changed

[Details of the amendment]

[Scope of Claims]

[Claim 1]

A commercial transaction method comprising of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the commercial transaction method is characterized in that it comprises the steps of receiving the payment certification key information related to the commercial transaction from a payment authorization institution, causing the payment certification key information received to be displayed in the display means, forwarding the payment certification key information displayed on the network terminal to a payment terminal installed at the purchaser of goods, and performing payment of the selected goods by the purchaser using the payment terminal of the purchaser of goods.

[Claim 2]

A commercial transaction method comprising of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the commercial transaction method is characterized in that it comprises the steps of receiving the payment certification key information related to a commercial transaction and a certificate of trust issued by a product purchase source from a payment approval institution, causing the received certificate of trust with the payment certification key information to be displayed on the display means, forwarding the payment certification key information displayed on the network terminal to a payment terminal installed at the purchaser of goods, and performing payment of the selected goods by the purchaser using the payment terminal of the purchaser of goods.

[Claim 3]

A commercial transaction method according to any one of Claims 1 or 2, characterized in that a mobile device is used as the network terminal.

[Claim 4]

A commercial transaction method according to any one of the Claims 1 to 3, characterized in that the network terminal receiving the payment certification key information and the ordering party network terminal in the commercial transaction are different terminals.

[Claim 5]

A commercial transaction method according to any one of the Claims 1 to 4, characterized in that the payment certification key information displayed in the display means is configured with a code character information image.

[Claim 6]

A commercial transaction method according to any one of the Claims 1 to 5, characterized in that the payment certification key information displayed in the display means is configured with an encrypted code character information image.

[Claim 7]

A commercial transaction method according to any one of the Claims 1 to 6, characterized in that the network terminal has a sign that records the identification information of each terminal device, and further comprises the steps of causing the payment terminal to read the identification sign, transmitting

some or all of the payment certification key information transferred to the payment terminal and the identification sign information to the payment authorization institution, and authenticating whether the identification sign information is legitimately registered in advance with the payment authorization institution, and transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the payment terminal from which the item was purchased.

[Claim 8]

A commercial transaction method according to any one of the Claims 1 to 6, characterized in that the network terminal has an identification sign that records the identification information of either the IC card or the owner of the network terminal, and further comprises the steps of causing the payment terminal to read the identification sign, transmitting some or all of the payment certification key information transferred to the payment terminal and the identification sign information to the payment authorization institution, and authenticating whether the identification sign information is legitimately registered in advance with the payment authorization institution, and transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the payment terminal from which the item was purchased.

[Claim 9]

A commercial transaction method according to any one of the Claims 1 to 8, characterized in that the identification sign is composed of a mark that emits the identification information recorded on the identification sign with reflected light of a predetermined wavelength in response to irradiation light of a predetermined wavelength.

[Claim 10]

A commercial transaction method according to any one of the Claims 1 to 9, characterized in that it further comprises of a step of displaying the information regarding the purchaser included in the payment certification key information on a display unit of the payment terminal from which the product was purchased.

[Claim 11]

A commercial transaction method according to any one of the Claims 1 to 10, characterized in that it further comprises of a step of transmitting the content of the transaction that has completed the payment from the payment terminal of the item purchaser to the payment authorization institution and updating the purchase history information of the purchaser.

[Claim 12]

A commercial transaction method according to any one of the Claims 1 to 11, characterized in that it further comprises of a step of transmitting the content of the transaction completed by the payment authorization institution to the network terminal of the purchaser and displaying the content of the transaction.

[Claim 13]

A commercial transaction method comprising of a network terminal having a display means for displaying the information on the payment and a transmitting/receiving means for transmitting and receiving the information regarding the payment of the product via a communication network to make payments regarding the products to be traded provided by the product provider; and the commercial transaction method is characterized in that it comprises the steps of receiving the payment certification key information relating to the transaction from the payment authorization institution and a certificate of trust issued by the product purchaser at the network terminal, printing the received certificate of trust with the payment certification key information with the code character information image, reading the signed certificate of trust with the payment certification key information to the payment terminal installed at the product purchaser, and performing payment of the selected goods by the purchaser at the payment terminal of the product purchaser.

[Claim 14]

A commercial transaction method according to Claim 13, characterized in that the code character information image is printed with a printing material mixed with crystalline powder that emits the payment certification key information by the reflected light of a predetermined wavelength in response

to an irradiation light of a predetermined wavelength.

[Claim 15]

A commercial transaction method according to Claims 1 to 13, characterized in that the network terminal has an input means for inputting the information on the commercial transaction, which further comprises the steps of inputting the information on a transaction of a product including at least the product provider or the product identification information, the payment method, the purchase amount and the purchaser's own PIN from the input means, and transmitting the input payment information to a payment authorization institution and receiving the payment certification key information generated in response to the authentication of the product provider and the purchaser's own authentication and credit results.

[Claim 16]

A commercial transaction method according to Claims 1 to 15, characterized in that the network terminal has an input means for inputting the information on the commercial transaction, which further comprises the steps of inputting the information related to the transaction of the product including at least the product provider or the product identification information, the payment method, the service points used, and the purchaser's own personal identification number, and transmitting the input payment information to a payment authorization institution and receiving the payment certification key information generated in accordance with the product provider's authentication, the purchaser's own authentication, and the confirmation result of the service points acquired by the purchaser.

[Claim 17]

A commercial transaction device that comprises of a network terminal having an input means for inputting the information about the payment of a transaction target product, a display means for displaying information about the payment, and a transmitting/receiving means for transmitting information and receiving information regarding the payment of the product via a communication network; and performs payment for a transaction target product provided by the product provider, comprising of a means for generating the payment certification key information related to the commercial transaction, and a means for transmitting and displaying the payment certification key information to the network terminal.

[Claim 18]

A commercial transaction device that performs payment for a transaction target product provided by a product provider using a network terminal having a display means for displaying the payment information and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; the commercial transaction device comprises of a means for generating the payment certification key information relating to the commercial transaction and a means for receiving and transmitting and displaying the certificate of trust issued from the product purchaser as a certificate of trust with the payment certification key information.

[Claim 19]

A commercial transaction device according to any one of the Claims 17 or 18, characterized in that a mobile device is used as the network terminal.

[Claim 20]

A commercial transaction system comprising of a display means for displaying the information regarding payment; a device identification sign; a network terminal having a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payments; a product provider device that settles the price of the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to commercial transactions and transmit it to the network terminal for display,

and that receives a part or all of the payment certification key information and the reading result of the device identification sign from the product provider; a means for authenticating whether the information on the device identification sign is genuine and registered in advance with a payment authorization institution, and that transmits the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of the product purchase source in accordance with the authentication result of the information on the device identification sign; and a means for delivering products ordered by a purchaser and making payment for the products.

[Claim 21]

A commercial transaction system comprising of a display means for displaying the information regarding the payment; a device identification sign; a network terminal having a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that performs payment for the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to the commercial transaction; a means for transmitting and displaying the certificate of trust issued by the product purchasing source and the payment certification key information to the network terminal, and that receives a part or all of the payment certification key information and the reading result of the device identification sign from the product provider; a means for authenticating whether the information on the device identification sign is genuine and registered in advance with the payment authorization institution; and a means for transmitting the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of a product purchase source in accordance with the authentication result of information on the device identification sign.

[Claim 22]

A commercial transaction system according to Claims 20 and 21, wherein the network terminal is a mobile device.

[Claim 23]

The commercial transaction system according to any one of Claims 20 to 22, characterized in that the device identification sign is configured with a sign that emits the device serial number information and the telephone number information using the reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength.

[Claim 24]

A commercial transaction system comprising of a mobile terminal having a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product ordering and payment via a communication network; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that performs payment for the product at the product provider; a means for the payment authorization institution device to generate the payment certification key information related to the commercial transaction; a means for transmitting the certificate of trust issued by the product purchasing source and the payment certification key information to the network terminal, and that receives information from the product purchase source regarding the certificate of trust printed in the code character information image by a printing device attached to the network terminal and the reading result of the payment certificate key information; a means for authenticating whether or not the payment certification key information is valid, and that sends the payment authorization information corresponding to the payment certification key information from the payment authorization institution to the payment terminal of the product purchase source in accordance with the authentication result of the payment certification key information; and a means for delivering products ordered by a purchaser

and making payment for the products.

[Claim 25]

A commercial transaction system according to Claim 24, characterized in that the code character information image is configured with an encrypted code character information image.

[Claim 26]

A recording medium characterized in that it consists of a network terminal having a display means for displaying the information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a program for making a payment regarding the product to be traded provided by a product provider; a process for generating the payment certification key information and transmitting and displaying the information to the network terminal, and that transfers the payment certification key information from the network terminal on which the payment certification key information is displayed to a terminal installed at the product purchase source; and a computer-readable program with the commercial transactions recorded thereon, and that includes the processes that cause the payment terminal of the product purchaser to execute payment for a product selected by a purchaser.

[Claim 27]

The commercial transaction method according to any one of Claims 5 or 6, characterized in that the code character information image is configured with a barcode or a two-dimensional barcode.

[Claim 28]

The commercial transaction method according to any one of Claims 15 or 16, characterized in that the input means including the imaging means further comprises a step of capturing and inputting the image information in which the identification information of the product provider or the product is encoded by the imaging means; and a step of decoding the input image information and acquiring the identification information of the provider of the product or of the product itself.

[Claim 29]

The commercial transaction device according to any one of Claims 17 to 19, characterized in that the input means includes an imaging means for capturing the image information in which the product provider or the product identification information is encoded as information regarding the transaction of the product, and further includes a means for decoding the image information.

[Claim 30]

The commercial transaction system according to any one of Claims 20 to 23, characterized in that the payment certification key information displayed in the display means is configured with a code character information image.

[Claim 31]

The commercial transaction system according to Claims 24 or 30, characterized in that the code character information image is configured with a barcode or a two-dimensional barcode.

[Claim 32]

A commercial transaction system according to any one of the Claims 20 to 25, 30, and 31, characterized in that the network terminal has an input means for inputting information related to the product transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's own personal identification number.

[Claim 33]

The commercial transaction system according to Claim 32, characterized in that the input means includes an imaging means for capturing the image information encoded with the identification information of the product provider or the product; and the payment authorization institution device characterized in that it further includes a means for decoding the image information captured and transmitted by the imaging means.

[Procedure amendment 2]

[Name of document subject to amendment] Specification

[Name of item subject to amendment] 0009

[Correction method] Changed

[Details of the amendment]

[0009]

It is characterized by being composed of data information images.

The transaction method of the present invention can also be realized by a program in a payment authorized institution device. The program can be provided on a recording medium that records the following processes. In other words, it is characterized in that it consists of a network terminal having a display means for displaying the information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a program for making a payment regarding the product to be traded provided by a product provider; a process for generating the payment certification key information and transmitting and displaying the information to the network terminal, and that transfers the payment certification key information from the network terminal on which the payment certification key information is displayed to a terminal installed at the product purchase source; and a computer-readable program with the commercial transactions recorded thereon, and that includes the processes that cause the payment terminal of the product purchaser to execute payment for a product selected by a purchaser. Furthermore, the method of trading of the present invention is characterized in that the code character information image is composed of a barcode or a two-dimensional barcode.

Moreover, it is characterized in that the input means including the imaging means further comprises a step of capturing and inputting the image information in which the identification information of the product provider or the product is encoded by the imaging means; and a step of decoding the input image information and acquiring the identification information of the provider of the product or of the product itself.

Also, the commercial transaction device of the present invention is characterized in that the input means includes an imaging means for capturing the image information in which the product provider or the product identification information is encoded as information regarding the transaction of the product, and further includes a means for decoding the image information.

Further, the commercial transaction system of the present invention is characterized in that the payment certification key information displayed in the aforementioned display means is composed of a code character information image.

Moreover, it is characterized in that the aforementioned code character information image is composed of a barcode or a two-dimensional barcode.

In addition, it is characterized in that the network terminal has an input means for inputting information related to the product transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's own personal identification number.

It is also characterized in that the input means includes an imaging means for capturing the image information encoded with the identification information of the product provider or the product; and the payment authorization institution device characterized in that it further includes a means for decoding the image information captured and transmitted by the imaging means.

Brief Description of the Drawing

FIG. 1 is a system configuration diagram showing an embodiment of a system implementing the commercial transaction method of the present invention.

FIG. 2 is a schematic block diagram illustrating a configuration of a mobile phone.

FIG. 3 is a diagram showing an example of a label, a barcode, and a two-dimensional code attached to a mobile phone.

FIG. 4 is a cross-sectional configuration diagram of a reading device that reads the barcode attached to the mobile phone and a two-dimensional code displayed on the display unit.

FIG. 5 is an internal configuration diagram of an authentication server.

FIG. 6 is a diagram illustrating an example of the data stored in the store information database.

[International Survey Report]

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP01/04223
A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. ⁷ G06F17/60		
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) Int. Cl. ⁷ G06F17/60		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Tokoku Jitsuyo Shinan Koho 1994-2001 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Tokoku Koho 1996-2001		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5706422 A (AT&T), 13 January, 1998 (23.01.98), column 14 ("A Fifth Illustrative Embodiment") & CA 2176163 A & EP 745961 A2 & JP 8-339407 A	1-26
Y	US 5608778 A (Lucent Technologies Inc.), 04 March, 1997 (04.03.97), column 6, lines 15 to 60 & CA 2156206 A & EP 708547 A2 & JP 8-096043 A	1-26
Y	EP 1017030 A2 (International Business Machines Corporation), 05 July, 2000 (05.07.00), Figs. 2, 3 & JP 2000-194770 A	1-26
Y	JP 9-116960 A (Fujitsu Limited), 02 May, 1997 (02.05.97), Fig. 3 (Family: none)	1-26
☒ 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 "U" earlier document 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 relating 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 "Z" document number of the same patent family		
Date of the actual completion of the international search 14 August, 2001 (14.08.01)		Date of mailing of the international search report 11 September, 2001 (11.09.01)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/04223

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5930767 A (Motorola Inc.), 27 July, 1999 (27.07.99), Figs. 3, 4; column 7, line 66 to column 8, line 13 (Family: none)	1-26
Y	JP 8-016740 A (Toshiba Corporation), 19 January, 1996 (19.01.96), Par. No. [0025] (Family: none)	1-26
Y	US 5789752 A (McMILLON, Steven A.), 04 August, 1998 (04.08.98), Figs. 1, 2 (Family: none)	1-26
Y	WO 85/03787 A1 (WHITE, Peter), 29 August, 1985 (29.08.85), page 14, lines 3 to 10 & CA 1232684 A & EP 172877 A1 & JP 61-501477 A & US 4630201 A	1-26
X, P	WO 01/09807 A1 (E-Mark Systems Inc.), 08 February, 2001 (08.02.01), Figs. 29 to 31 & AU 34559/00 A1 & AU 34560/00 A1 & WO 01/09808 A1	1-26

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

International Survey Report		International application number: PCT/JP01/04223	
A. Classification of the field of invention (International Patent Classification (IPC)) Int.Cl. ⁷ G06F17/60			
B. Areas of Investigation Minimal materials investigated (International Patent Classification (IPC)) Int.Cl. ⁷ G06F17/60			
Items included in the field investigated using materials other than the minimal materials Japanese Utility Model Publication 1922-1996 Japanese Public Utility Model Publication 1971-2001 Japanese Registered Utility Model Publication 1994-2001 Japanese Utility Model Registration Publication 1996-2001			
Electronic databases used in the International Surveys (name of databases, terms used in surveys)			
C. Literature deemed to be relevant			
Category of References*	If the cited document name and sections are related, the relevant sections shall be displayed.	Number of related claims	
Y	US 5708422 A (AT&T) January 13, 1998 (01.13.98) & CA 2176163 A & JP 8-339407 A	1-26	
☒ The literature is also listed in the following column.		See the reference paper on the patent families.	
* Category of References "A" Indicates the general technical level, but not particularly relevant literature. "E" An application or patent filed prior to the date of the international application but published after the date of the international application. "L" Literature that challenge the priority claim or documents cited to establish the date of publication or other special reasons (with reasons). "O" References referring to oral disclosure, use, exhibition, etc. "P" Documents published before the international application and after the month of the application on which priority is claimed. "T" A document published after the international application date or priority date that does not conflict with the application and is cited for the purpose of understanding the principles or theories of the invention. "X" A particularly relevant document that is considered to have no novelty or inventive step in the invention solely in the relevant document. "Y" A particularly relevant document that is considered to have no inventive step by a combination of the relevant document and one or more other documents that are obvious to a person skilled in the art. "&" Patent family literature			
Date of completion of the international survey 14.08.01		International investigation report dispatch date 11.09.01	
Name and address of the International Research Organization Japan Patent Office (ISA/JP) Postal code: 100 - 8915 3-4-3 Kasumigaseki, [Chiyoda]-ku, Tokyo		Patent Office Examiner (Authorized Officer) Susumu Awa [seal:] [illegible]	5L 9168 Phone number: 03-3581-1101, Extension: 3561

Form PCT/ISA/210 (continued from second page) (July 1998)

C (continued) Literature deemed to be relevant		
Category of References*	If the cited document name and sections are related, the relevant sections shall be displayed.	Number of related claims
Y	US 5608778 A (LUCENT TECHNOLOGIES INC) March 4, 1997 (03.04.97) <i>Column 6, lines 15-60</i> & CA 2156206 A & EP 708547 A2 & JP 8-096043 A	1-26
Y	EP 1017030 A2 (INTERNATIONAL BUSINESS MACHINES CORP) July 5, 2000 (07.05.00) <i>FIG. 2, 3</i> & JP 2000-194770 A	1-26
Y	JP 9-116960 A (Fujitsu Limited) May 2, 1997 (05.02.97) <i>FIG. 2</i> (Without family)	1-26
Y	US 5980767 A (MOTOROLA INC) July 27, 1999 (07.27.99) <i>FIG. 3, 4; Columns 7, 66 to Columns 8, 13</i> (Without family)	1-26
Y	JP 8-016740 A (Toshiba Corporation) January 19, 1996 (01.19.96) <i>Paragraph [0025]</i> (Without family)	1-26
Y	US 5789732 A (McMAHON, Steven A) August 4, 1998 (08.04.98) <i>FIG. 1, 2</i> (Without family)	1-26
Y	WO 85/03787 A1 (WHITE, Peter) August 29, 1985 (08.29.85) <i>Page 14, lines 3-10</i> & CA 1232684 A & EP 172877 A1 & JP 61-501477 A & US 4630201 A	1-26

Form PCT/ISA/210 (continued from second page) (July 1998)

International Survey Report

International application
number: PCT/JP01/04223

C (continued) Literature deemed to be relevant		
Category of References*	If the cited document name and sections are related, the relevant sections shall be displayed.	Number of related claims
X,P	WO 01/09807 A1 (Emark Systems Co., Ltd.) February 8, 2001 (02.08.01) <i>FIG. 29-31</i> & AU 34559/00 A1 & AU 34560/00 A1 & WO 01/09808 A1	1-26

Form PCT/ISA/210 (continued from second page) (July 1998)

Continuation from the front page

(51)Int.Cl. ⁷	F I		
	G06K	17/00	L
	G06K	19/00	E
	G06K	19/00	J
	H04B	7/26	109S

(Note) This publication was prepared based on the publication published internationally by the World Intellectual Property Organization (WIPO). The effect of international publication of Japanese patent applications (Japanese utility model registration application) pertaining to this publication is based on Article 184-10, Paragraph 1 of the Patent Act (Article 48-13, Paragraph 2 of the Utility Model Act), and is not related to this publication.

[Publication type] Publication of amendments pursuant to the provisions of Article 17-2 of the Patent Act

[Divisional classification] Division 6, and Division 3

[Issuance date] May 19, 2005 (5.19.2005)

[International publication number] WO2002/008981

[Annual number of issues] Publication/registered publication 2004-001

[Application number] Japanese Patent Application 2002-514614 (P2002-514614)

[International Patent Classification 7th Edition]

G06F 17/60

G06K 17/00

G06K 19/06

G06K 19/07

H04Q 7/38

[FI]

G06F 17/60 414

G06F 17/60 422

G06F 17/60 506

G06F 17/60 512

G06F 17/60 ZEC

G06K 17/00 L

G06K 19/00 E

G06K 19/00 J

H04B 7/26 109S

[Procedural amendment]

[Submission date] December 24, 2002 (12.24.2002)

[Procedural amendment 1]

[Name of document subject to amendment] Specification

[Name of item subject to amendment] Full text

[Correction method] Changed

[Details of the amendment]

[Document name] Specification

[Title of invention] Commercial transaction method and network terminal and commercial transaction system

[Scope of Claims]

[Claim 1] A commercial transaction method comprising of a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a network terminal with a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of

transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment for the product using a payment terminal of a product purchaser.

[Claim 2] A commercial transaction method comprising of a network terminal that includes a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving the information regarding product payment via a communication network; an IC card having a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment of the product price amount using the payment terminal of the product purchaser based on the payment authorization information.

[Claim 3] The commercial transaction method according to any of Claims 1 or 2, characterized in that the network terminal includes an input means for inputting the information related to the commercial transactions; an imaging means for capturing the image information encoded with the identification information of the product provider or the product, and inputs information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number, from the input means, and transmits the entered information regarding the commercial transaction to the payment authorization institution device; and a step of decrypting the image information and receiving the payment certification key information generated according to the product provider's authentication and the purchaser's own authentication and credit results.

[Claim 4] A commercial transaction method comprising of a network terminal that includes a display means for receiving and displaying the payment certification key information regarding the commercial transactions from a payment authorization institution device; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network, which transmits the payment certification key information displayed on the display means to the payment terminal installed at the product purchase source, and whereby payment for the product selected by the purchaser is executed by the product purchase source's payment terminal; and a sign recording the identification information registered in advance with the payment authorization institution, whereby the sign emits the identification information by a reflected light of a predetermined wavelength in response to an irradiated light of a predetermined wavelength.

[Claim 5] The network terminal according to Claim 4, characterized in that the network terminal is equipped with an input means for inputting information regarding the commercial transactions, and whereby the input means includes an imaging means for capturing image information in which the

identification information of a product provider or a product is encoded.

[Claim 6] A commercial transaction system comprising of a display means for displaying information on payment; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a network terminal with a sign recording the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and authorization regarding the payment; a product provider device that performs payment for a product at a product provider, wherein the payment authorization institution device generates the payment certification key information regarding the commercial transaction; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with the payment authorization institution in accordance with the authentication result of the identification information, whereby the payment approval information corresponding to the payment certification key information is transmitted from the payment authorization institution to the payment terminal of the product purchase source; and a means for delivering the product ordered by the purchaser and making payment for the product.

[Claim 7] A commercial transaction system comprising a network terminal that includes a display means for displaying information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; an IC card having a sign that emits the pre-recorded identification information using a reflected light of a predetermined wavelength with respect to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that settles the price of the product at the product provider; a payment authorization institution device that generates the payment certification key information regarding the commercial transactions; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with a payment authorization institution; and a means for transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the product provider device in accordance with the authentication result of the identification information.

[Claim 8] The commercial transaction system according to Claim 6 or Claim 7, characterized in that the network terminal has an input means for inputting information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number; the input means includes an imaging means for capturing image information encoded with the identification information of the product provider or the product; and a payment authorization institution device that further includes a decoding means for decoding the image information captured and transmitted by the imaging means.

[Detailed description of invention]

[0001]

Technical field

The present invention relates to a commercial transaction method, a commercial transaction device and a commercial transaction system that can be used for payment of products purchased at various stores such as supermarkets, electronic stores opened on Internet servers, or vending machines such as for potable drinking water, using terminals that can be connected to a network such as via mobile phones.

[0002]

Background technology

With the addition of the WWW browsing function (World Wide Web) to the mobile phone, the transaction format of using the mobile phone to access the Internet, browse various types of information, goods, and services, and order the provision of such information, goods, and services as necessary is rapidly expanding. Here, in the present invention, information (content) such as music software that does not have a shape, goods that have a shape, and services such as home delivery service and nursing care service are all defined as products that are subject to commercial transactions. In this case, there are also free nursing services provided by public institutions, but even if they are free, they are included in the products subject to transactions.

However, even if a product is ordered using a mobile phone, the settlement method still follows traditional business practices, such as bank transfer, sending of cash, and cash on delivery upon arrival of the product.

In recent times, instead of this conventional method, a method has been implemented in which a credit card number is notified to the product provider (store) at the same time as the product is ordered, and payment is made through the credit card company.

However, this payment method is based on the premise that the number or information that only the credit card company and the person themselves should know will not be leaked to outside parties, and if leaked, there is a risk that it will be misused.

Therefore, in the next-generation mobile communication services starting in May 2001, which will equip mobile phones with an IC card called a UIM (User Identity Module), a method is being considered in which confidential data such as credit card numbers are encrypted using a cryptographic program in the IC card allowing payments to be made.

However, even if the data is encrypted and saved using a cryptographic program, if the mobile phone itself is lost, there is a risk that it will be decrypted by an unauthorized third party and misused. In particular, it is believed that there will be many forms of storing not only credit card numbers but also other confidential data such as bank account numbers, insurance card numbers, and electronic money at the same time in IC cards, so the risk of being decrypted by an unauthorized third party is higher than with traditional payment methods.

In addition, as with contactless IC cards, networks using wireless networks have a problem in that there is a greater possibility of information leaking to the outside due to hacking, including unauthorized access, than wired networks.

In addition, due to the emergence of unauthorized stores, there is the risk that confidential data may be intercepted and misused during payment at these stores.

Furthermore, there is also the problem that the cost of the mobile device itself will increase, the power consumption will also increase, and the battery life will be shortened.

The present invention is made to solve such problems, and the purpose is to provide a commercial transaction method, device, and system that can authenticate the person without disclosing confidential data such as credit numbers to a person authentication institution or credit card company, and can safely settle the purchase of goods.

[0003]

Disclosure of the Invention

In order to achieve the above objectives, the commercial transaction method of the present invention is characterized by being configured as follows.

In other words, it is a method comprising of a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a network terminal with a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information

displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment for the product using a payment terminal of a product purchaser.

The method also comprises of a network terminal that includes a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving the information regarding product payment via a communication network; an IC card having a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment of the product price amount using the payment terminal of the product purchaser based on the payment authorization information.

Further, the network terminal includes an input means for inputting the information related to the commercial transactions; an imaging means for capturing the image information encoded with the identification information of the product provider or the product, and inputs information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number, from the input means, and transmits the entered information regarding the commercial transaction to the payment authorization institution device; and a step of decrypting the image information and receiving the payment certification key information generated according to the product provider's authentication and the purchaser's own authentication and credit results.

The network terminal of the present invention comprises of a display means for receiving and displaying the payment certification key information regarding the commercial transactions from a payment authorization institution device; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network, which transmits the payment certification key information displayed on the display means to the payment terminal installed at the product purchase source, and whereby payment for the product selected by the purchaser is executed by the product purchase source's payment terminal; and a sign recording the identification information registered in advance with the payment authorization institution, whereby the sign emits the identification information by a reflected light of a predetermined wavelength in response to an irradiated light of a predetermined wavelength.

In addition, the network terminal is equipped with an input means for inputting information regarding the commercial transactions, and whereby the input means includes an imaging means for capturing image information in which the identification information of a product provider or a product is encoded.

The commercial transaction system of the present invention comprises of a display means for displaying information on payment; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a network terminal with a sign

recording the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and authorization regarding the payment; a product provider device that performs payment for a product at a product provider, wherein the payment authorization institution device generates the payment certification key information regarding the commercial transaction; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with the payment authorization institution in accordance with the authentication result of the identification information, whereby the payment approval information corresponding to the payment certification key information is transmitted from the payment authorization institution to the payment terminal of the product purchase source; and a means for delivering the product ordered by the purchaser and making payment for the product.

Also, it is characterized in that the commercial transaction system comprises of a network terminal that includes a display means for displaying information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; an IC card having a sign that emits the pre-recorded identification information using a reflected light of a predetermined wavelength with respect to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that settles the price of the product at the product provider; a payment authorization institution device that generates the payment certification key information regarding the commercial transactions; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with a payment authorization institution; and a means for transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the product provider device in accordance with the authentication result of the identification information.

Moreover, the network terminal has an input means for inputting information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number; the input means includes an imaging means for capturing image information encoded with the identification information of the product provider or the product; and a payment authorization institution device that further includes a decoding means for decoding the image information captured and transmitted by the imaging means.

[0004]

Brief Description of the Drawing

FIG. 1 is a system configuration diagram showing an embodiment of a system implementing the commercial transaction method of the present invention.

FIG. 2 is a schematic block diagram illustrating a configuration of a mobile phone.

FIG. 3 is a diagram showing an example of a label, a barcode, and a two-dimensional code attached to a mobile phone.

FIG. 4 is a cross-sectional configuration diagram of a reading device that reads the barcode attached to the mobile phone and a two-dimensional code displayed on the display unit.

FIG. 5 is an internal configuration diagram of an authentication server.

FIG. 6 is a diagram illustrating an example of the data stored in the store information database.

FIG. 7 is a diagram illustrating an example of the data stored in the user information database.

FIG. 8 is a diagram illustrating an example of the data stored in the purchase history database.

FIG. 9 is a diagram illustrating an example of the data stored in the unauthorized information database.

FIG. 10 is a flowchart illustrating the procedure for using a mobile phone to settle the price of goods at a general store.

FIG. 11 is a flowchart showing a continuation of FIG. 10.

FIG. 12 is a diagram illustrating an example of a QR payment certification key displayed on the mobile phone and the user information displayed on the store terminal.

FIG. 13 is a diagram illustrating an example of the confirmation information displayed on the mobile phone at the end of payment.

FIG. 14 is a flowchart showing the procedure for the payment of small-value products at a vending machine. FIG. 15 is a flowchart illustrating the continuation of FIG. 14.

FIG. 16 is a flowchart illustrating the procedure for receiving and clearing items ordered at stores on the Internet at designated receiving stores.

FIG. 17 is a flowchart illustrating the continuation of FIG. 16.

FIG. 18 is a flowchart showing the procedure for bringing a printed copy of the QR payment certification key to the store for payment.

FIG. 19 is a diagram illustrating an example of a printed QR payment certification key.

FIG. 20 is a diagram illustrating an example of the data stored in the gift information database.

FIG. 21 is a flowchart showing the procedure for paying for a gift to another person.

FIG. 22 is a flowchart illustrating the continuation of FIG. 21.

FIG. 23 is a flowchart illustrating the continuation of FIG. 22.

FIG. 24 is a diagram illustrating a display example of the gift information displayed on a mobile phone and a display example after selecting acceptance or rejection of the gift.

FIG. 25 is a diagram illustrating an example of the confirmation information displayed on the giver's mobile phone at the end of payment.

FIG. 26 is a flowchart illustrating the continuation of FIG. 21.

FIG. 27 is a flowchart illustrating the continuation of FIG. 26.

FIG. 28 is a diagram illustrating an example of a service point usage history database.

FIG. 29 is a flowchart illustrating the procedure for making a payment using service points at a general store using a mobile phone.

FIG. 30 is a flowchart illustrating the continuation of FIG. 29.

FIG. 31 is a partial perspective view illustrating an example of a mobile phone used in the present invention.

FIG. 32 is a partial perspective view illustrating an example of a mobile phone used in the present invention.

[0005]

Detailed Description of the Preferred Embodiments

The embodiments of the present invention will be described in detail below with reference to the accompanying drawings.

FIG. 1 is a system configuration diagram illustrating an embodiment of the overall configuration of the system for implementing the commercial transaction method of the present invention, which includes a mobile phone 1 as a network terminal used by a product purchaser, a store 2 from which the product is provided, a vending machine 3 such as for potable water, and a payment authorization institution 4, which is connected by a communication network 5. The communication network 5 includes a wireless line, a wired line, and an internet network. Here, the network terminal refers to a terminal that can be connected to a network such as the Internet, and in addition to the mobile phone 1 shown in the following example, it includes various other types such as PHS, PDA, personal computer, digital television, etc.

The mobile phone 1 is a commercially available mobile phone with a function that can be connected to an internet network, and as shown in the schematic block diagram of FIG. 2(a), it comprises of a display 11, a wireless transmitter/receiver 12, a control 13, an input 14, a receiver 15, a memory 16, and an external input and output interface 17. In the Internet connection mode, the display 11 displays the Internet connection menus such as news, mobile banking, card/security/insurance, and mobile shopping, as shown in FIG. 2(b).

The external input and output interface 17 includes a wireless communication interface, such as an infrared interface such as Irda and a weak radio wave interface such as Bluetooth, and in this present embodiment, it is used when receiving the store identification number from the transmitter installed in the store. In addition, the external input and output interface 17 includes an interface for a barcode reader connected to a mobile phone or a built-in on the mobile phone, and the barcode reader may read the identification information, etc., of the store displayed with the barcode information or the identification information, etc. of the product. Furthermore, a camera connected to the mobile phone or a built-in on the mobile phone, and the identification information of each store or the identification information of the product displayed in the code character information image may be captured as image

data by the camera. In this case, a program for decoding the code character information images captured as image data is provided in the authentication server of the payment authorization institution 4 above, and by decoding the code character information images sent from the mobile phone in the above program, the identification information of the store or product can be recognized. In addition, the aforementioned program may be provided on a mobile phone machine, and in this case, each of the aforementioned identification information recognized by decoding the code character information image on the mobile phone machine is transmitted to the aforementioned authentication server.

By using the external input and output interface 17 as described above, it is possible to input store or product identification information without operating the input unit 14. Here, the identification information of the product includes the product name, product type, and amount, etc.

It should be noted that entering the amount of the product is not a substitute for inputting the amount by a store staff, but it involves a self-scanning action, and is intended for the purchaser to know the payment amount information in advance.

As shown in the front and side views of FIGS. 3(a) and (b), the mobile phone 1 of this embodiment is affixed with a first sign 19 that records the equipment serial number with the barcode 31, such as in FIG. 3(c), and a second sign 20 that records the mobile phone number with the barcode 31.

The barcodes of these signs 19 and 20 are printed with a printed material containing crystalline powder that emits the recorded information by the reflected light having a predetermined wavelength λ_a or λ_b in response to an irradiation light having a predetermined wavelength λ_a , as shown in FIG. 4(a). This crystalline powder is provided by SUNSTONE, Inc. in the United States, and is used for authentic identification of pharmaceutical products and banknotes. In this case, the characteristics are adjusted so that the wavelength of the irradiated light and the wavelength of the emitted light differ depending on the application and the system used.

In the present invention, the barcode of the device serial number and mobile phone number is printed on the signs 19 and 20 with a recording ink or toner mixed with the special crystalline powder, which is affixed to the front or side of the mobile phone 1, and the barcode recorded on the signs 19 and 20 is read with the irradiated light at a predetermined wavelength λ_a .

By affixing the device serial number and the mobile phone number signs 19 and 20 recorded with such special recording ink or toner to the mobile phone 1, it is not possible to read the device serial number and mobile phone number other than the irradiated light at a predetermined wavelength. Therefore, by pre-registering the device serial number and the mobile phone number with the payment authorization institution 4, it is possible to identify whether the mobile phone 1 is a legitimate device that can be used for commercial transactions in this system. The side sign 20 also serves to prevent modification of the mobile phone 1.

In this case, it is not necessarily essential to affix the aforementioned sign, and the aforementioned sign may be printed on the casing of the mobile phone itself using the recording ink or the like.

The barcodes of the signs 19 and 20 are inserted into the reader 40 in a cross-sectional configuration as shown in FIG. 4(b) and they are read by irradiating light with a predetermined wavelength. This reader 40 is installed in store 2 and the vending machine 3.

On the other hand, the display unit 11 displays payment certification key information configured with the two-dimensional code 32 as a code character information image as shown in FIG. 3(d). This two-dimensional code 32 is set in the standard code of the Japan Automobile Manufacturers Association and the Japan Stationery Association. This is disclosed in, for example, the Japanese Unexamined Patent Application No. 10-214317, so a detailed explanation will be omitted here.

Using this two-dimensional code (hereinafter referred to as the QR code), approximately 7,000 characters (numbers) can be coded and recorded within the area of the display of the mobile phone 1. In the present invention, this QR code is used to represent the information of the payment certification key information. In detail, the information of the payment certification key information composed of a QR code is transferred to the mobile phone 1 to display it in the display 11 as shown in FIG. 3(a), and the mobile phone 1 in this display state is inserted into the reader 21 for reading sharing of the signs 19 and 20, so that the information of the payment certification key is read.

When using a QR code, as shown in FIG. 3(d), the recording contents can be read from any direction within 360° by means of the cutout symbols 33 to 35 located in three locations, so that the positional relationship with the reader is no longer bound, and it is suitable for use by the general user to insert into the reader unit and read. Also, since it is not necessary to strictly define the positional relationship, the reading time can be shortened accordingly. In addition, even if some part of the code is dirty or

damaged, the errors can be corrected, and the number of reading errors can be reduced. In particular, as in the present invention, when reading the data while it is displayed on the display of the mobile phone 1, it is conceivable that reading errors may occur due to dirt on the display unit, etc., but by using a QR code, reading errors caused by dirt on the display unit, etc. can be reduced.

Returning to FIG. 1, the store 2 is equipped with a reader 21 for reading the signs 19, 20 and the QR code, and inputs the read signs 19, 20 and the QR code into the store terminal 22, which is a POS terminal, which allows for payments to be made using the in-store terminals. The vending machine 3 is also equipped with a reader 33 for reading the QR codes and the signs 19, 20.

On the other hand, the payment authorization institution 4 comprises of a authentication server 41, a financial institution (bank or credit company) 42, a store information database (DB) 43, a user information database (DB) 44, and a purchase history database (DB) 45.

The authentication server 41 performs personal authentication and store authentication in response to a personal authentication and store authentication request from the mobile phone 1, and it also makes a credit inquiry to the financial institution 42; and if the person and the store are registered in advance, and there is a response from the financial institution 42 that the credit is OK, processing is performed to permit payment of the product price using the mobile phone 1. The server includes a store registration processing program 410, a user registration processing program 411, a purchase history management program 412, an unauthorized use management program 413, an authentication processing program 414, a QR payment key generation program 415, and a transmission/reception program 416. It should be noted that an encryption/decryption program for encrypting and storing the data from each database 43, 44, and 45 is incorporated as necessary. Additionally, an encryption program for encrypting and transmitting the QR code and a decryption program for decoding the QR code can be incorporated. By encrypting the QR code, unauthorized transactions can be made even more difficult.

The store registration processing program 410 is a program used to register stores (including vending machines and electronic stores on the Internet) that perform payments using this system in the store information DB 43. In addition, the user registration processing program 411 is a program used when registering a user (product purchaser) who makes a payment using this system in the user information DB 44.

The purchase history management program 412 is a program used when storing information on the purchase history of products purchased by a user (product purchaser) in the purchase history DB 45.

The unauthorized use management program 413 allows the system to be accessed by a store and a user who are not registered in the store information DB 43 and user information DB 44 in advance, and it is used when registering the store identification number or the device serial number or phone number of mobile phone 1 in the unauthorized use information database (FIG. 9) if the device serial number or phone number of mobile phone 1 is accessed by illegally rewriting it.

The authentication processing program 414 performs personal authentication and store authentication as well as credit inquiries to the financial institution 42 in response to the personal authentication and store authentication requests from the mobile phone 1; and if the person and the store have been registered in advance, and if there is a response from the financial institution 42 that the credit is OK, processing is performed to permit payment of the product using the mobile phone 1.

The QR payment key generation program 415 is a program that generates the payment certification key information composed of the QR code and passes it to the mobile phone 1 in order to authorize the payment of the product. The payment certification key information (hereinafter referred to as "QR authorized certification key information") composed of the QR code is the key information for the store to receive detailed approval information including the results of authentication of the purchaser and the store from the authentication server 41. By reading this QR authorized certification key information from the store reader 21 and sending the QR authorized certification key information read from the store terminal to the authentication server 41, the store terminal 22 can receive detailed approval information including the results of authentication of the purchaser and the store. In this case, if the QR authorized certification key information read by the reader 21 is different from that generated by the authentication server 41, approval of the authorized information cannot be obtained.

The transmission and reception program 416 is a program for sending and receiving the information necessary for decision making for access from users and stores.

FIG. 6 shows an example of the store information DB registration information, in which the store ID 601, the store name 602, address 603, and the phone number 604 are registered.

FIG. 7 is a diagram showing an example of the registration information for the user information DB, in

which the user ID 701, the user name 702, address 703, the mobile phone serial number (device serial number) 704, the mobile phone number 705, PIN number 706, gender 707, date of birth 708, debit card number 709, credit card number 710, web money account number 711, and other personal characteristics information 712 are registered.

The web money account number 711 is used when making a payment using the web money when purchasing a small-value item such as drinking water from a vending machine. In addition, the personal characteristics information 712 is intended to register the photos, etc. of the individual, and to enable the store staff to verify the identity of the user using features such as a photo when making a payment at a store, and it is registered according to the user's wishes. For example, registering a photo of the user himself/herself has the advantage that store staff can detect misuse by others at the time of payment processing. Further, based on the date of birth 708, it is possible to discover whether the person is a minor or not, and the sale of alcoholic beverages and tobacco can be prohibited. In addition, the driver's license number, etc. may also be registered. By registering a driver's license number, etc., it is also possible to issue a certificate of identity from a third-party authentication server 41 using a mobile phone.

FIG. 8 shows an example of the store information in the purchase history DB, in which the date and time of use 801, the name of the store used 802, the approval amount 803, the cumulative amount of the current month's use 804, the cumulative amount of service points 805, and the previous use date 806 are stored. It should be noted that this purchase history information is stored in the order of date and time of use for each user.

FIG. 9 is a diagram showing an example of the information stored in an unauthorized use information database, with the unauthorized user's mobile phone serial number 901, mobile phone number 902, and store ID 903 registered. Here, if only the mobile phone number 902 is registered, this means that the mobile phone serial number is correct, and it also means that the person accessed the site by modifying the mobile phone number sign. In addition, a store that does not have a store ID 903 registered means that the store is not registered in the system, or it is a store that has its store ID illegally rewritten.

Here, for unregistered users and stores who are not malicious, a message may be sent to register at the time of access, and registration may be made as unauthorized use only for those who do not perform the registration procedures despite multiple registration instructions.

Below, (1) the method of decision making when purchasing products using a mobile phone 1 at a general store such as a supermarket, (2) the method of decision making when purchasing products at a vending machine, and (3) the method of decision making when purchasing products at an electronic store on the Internet will be explained with reference to the flowchart.

FIGS. 10 and 11 are flowcharts illustrating how decisions are made when purchasing products using a mobile phone 1 at general stores such as supermarkets.

First, the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID as the identification information of the store from which he or she intends to purchase the product. The user then inputs his or her personal ID number (the number registered in 706 in FIG. 7), the payment method, and the purchase price of the product (step 1001). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17.

Further, regarding the payment method, there are the options of credit card payments, web money payments, and debit card payments, and if the credit card payment is selected, the number of payments and the credit card number are inputted. In addition, if the web money payment is selected, the web money account number (the number registered in 711 in FIG. 7) is inputted. Similarly, if the debit card payment is selected, the debit card number (the number registered in 709 in FIG. 7) is inputted. In the following flowchart, the operations performed by individuals are shown in a double-bordered format, as in step 1001.

When the input is complete, the transmission operation is performed. Then, the information input in step 1001 is sent to the authentication server 41 as the QR authorized certification key issuance request. The authentication server 41 that receives this request for issuing the QR authorized certification key information performs authentication processing for the store and the user (step 1002). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched using the PIN number and the credit card

number (or the web money account number, or debit card number), and it is checked whether the user with the PIN number and the credit card number (or the web money account number, or debit card number) is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1003). Even if the personal ID number and the credit card number (or web money account number or debit card number) are not registered, the user is either an unauthorized user or an unregistered user, and a message indicating that the transaction is not possible is sent back to the mobile phone 1 (step 1003). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1001 is automatically deleted.

However, if the store ID, the PIN number, and the credit card number (or web money account number, or debit card number) are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1004) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1005). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1006) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 1007). The store staff enters the price of the desired purchase item using the store terminal (step 1008).

In parallel, the user inserts and attaches the mobile phone 1 with the QR authorized key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 1009). The QR code reader 21 then reads the QR authorized certification key 1201 displayed on the display 11 of the mobile phone 1 (step 1011), and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1010), and forwards the information to the store terminal 22.

The store terminal 22 then sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the QR authorized certification key 1201 was issued by the authentication server itself, only part of the information such as the authorization number and the personal authentication may be sent. FIG. 11 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1012). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1013), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR authorized certification key 1201, and the QR authorized certification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1014). In addition, the user will be notified verbally that a payment cannot be decided by the store staff.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) on the QR authorized certification key 1201 received from

the store terminal 22 is recognized as a genuine one issued by the store terminal 22, the authentication server 41 returns the detailed settlement approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed authorization information on the display unit as user information (step 1015). FIG. 12(b) shows an example of this. The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1016).

If there is a response confirming the purchase intention from the person, the transaction is completed by operating the transaction button (step 1017). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1018). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. In addition, the approval completion information is transmitted to the financial institution 42. As a result, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. This approval content 1301 can be stored until it is deleted by the user. However, since the QR authorized certification key 1301 is only valid once, it is automatically deleted after a predetermined period of time. In addition, the financial institution 42 that receives the approval completion information performs procedures to withdraw the amount from the user's designated account.

Based on the above, a decision can be made when purchasing products at general stores using a mobile phone 1. If the user withdraws his or her intent to purchase, the processing of the store terminal is terminated by a cancellation operation at the store terminal. In addition, even if the user himself or herself performs a cancellation operation on the mobile phone 1, the payment processing will be terminated midway and all information such as the QR authorized certification key 1301 will be deleted. As is clear from the explanations above, according to the transaction method, the payment can be approved only by the QR authorized certification key issued by authentication server 41 without conveying confidential information such as the credit number of the user to the store. In addition, since the configuration does not hold any confidential information such as credit card numbers in the mobile phone 1, even if the mobile phone 1 is lost, there is no risk of it being misused for payment settlement. Furthermore, as the validity of the mobile phone serial number and the mobile number is determined by the sign recorded by mixing the special crystalline powder, it is possible to prevent misuse due to modification of the mobile phone itself, and by increasing the security of devices used for the payments, it will have beneficial effects for both the users and stores.

Moreover, since the store only needs to add the reader 21, there is an advantage that the cost of joining the system can be reduced. Similarly, the mobile phone 1 can be used as a commercially available mobile phone without adding an IC card or the like. In addition, since the purchase history is managed, it is no longer necessary to issue a point card from the store side. Further, since the user can see the usage status, there is an advantage in that it is useful for making systematic purchase plans.

Also, by using a QR code, the recording contents can be read from any direction in 360 degrees, so there is no restriction on the positional relationship with the reading unit, and it is suitable for use by the general user to insert into the reader unit and read. Also, since it is not necessary to strictly define the positional relationship, the reading time can be shortened accordingly. In addition, even if some part of the code is dirty or damaged, the errors can be corrected, and the number of reading errors can be reduced. In particular, as in the present invention, when reading the data while it is displayed on the display of the mobile phone 1, it is conceivable that reading errors may occur due to dirt on the display unit, etc., but by using a QR code, reading errors caused by dirt on the display unit, etc. can be reduced. The QR authorized certification key is configured to include at least information on the approval number, personal authentication, name, and authorization method, but it may be a one-time password generated based on the approval number, personal authentication, or part or all of the name.

In this case, for example, the authentication server 41 and the mobile phone 1 are equipped with a password generation program based on the same logic, and when accessing for the second time, the mobile phone 1 automatically sends a password automatically generated based on the PIN number etc. sent on the first time. On the authentication server 41 side, authentication is performed by comparing

the mobile phone number, etc., of the mobile phone 1 and the automatically transmitted password with the password automatically generated by the authentication server 41.

From the third time onward, a new password may be automatically generated and automatically sent based on the last automatically generated password.

By using such a so-called one-time password, security can be improved, and the input of a personal identification number can be omitted during the second and subsequent times of access.

Next, the method of deciding when purchasing small-value products such as drinking water from the vending machine 3 will be described with reference to the flowchart of FIGS. 14 and 15.

First, the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID of the vending machine 3 from which he or she intends to purchase the product. The user then inputs his or her personal identification number (the number registered in 706 in FIG. 7), the payment method, and the purchase price of the product (step 1401). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17. In addition, there are credit card payment, web money payment, debit card payment, and contactless IC card payment methods, but since the payment amount is small, the use web money is made, and the web money account number (the number registered in FIG. 7-711) is entered.

When the input is complete, the transmission operation is performed. Then, the information input in step 1401 is sent to the authentication server 41 as the QR authorized certification key issuance request. The authentication server 41 that receives this request for issuing the QR authorized certification key information performs authentication processing for the store (here, the vending machine) and the user (step 1402). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store (vending machine) with the store ID is registered. Similarly, the user information DB 44 is searched by the PIN and the web money account number, and the user of the PIN and web money account number is checked to see if it is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). Furthermore, if the PIN and the web money account number are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1401 is automatically deleted.

However, if the store ID and the web money account number are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1404) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1405). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1406) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

The user inserts into the mobile phone 1 the QR authorized certification key 1201 displayed into the reading unit of the QR code reader 33 attached to the vending machine 3 (step 1407). Then, the selection operation of the vending machine 3 is performed for the desired product to be purchased (step 1408). In the vending machine 3, the price is automatically confirmed by selecting the desired product (step 1409).

The QR code reader 33 reads the QR authorized key 1201 displayed on the display unit 11 of the mobile phone 1 (step 1411) and reads the mobile phone serial number and the mobile phone number from the

signs 19, 20 (step 1410).

The vending machine 3 sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from mobile phone 1 to the authentication server 41 as a payment approval request. In this case, the communication line can utilize data communication using a PHS telephone. FIG. 15 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1412). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1413), after which an unauthorized use message is sent to the vending machine 3 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR authorized certification key 1201, and the QR authorized certification key 1201 displayed on the display unit 11 is deleted.

In the vending machine 3, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1414). However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) on the QR authorized certification key 1201 received from the vending machine 3 is recognized as a genuine one issued by the vending machine 3, the authentication server 41 returns the detailed settlement approval to the store terminal 22. This detailed approval information includes the same information as the QR authorized certification key 1201, as well as the purchase history information of the user.

The store terminal 22, which has received the detailed approval, immediately performs the approval process (step 1415). Then, an authorization completion message is sent to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1416). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. In addition, the approval completion information is transmitted to the financial institution 42. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13 (step 1417).

The financial institution 42 that has received the authorization completion message performs procedures to debit the user's web money account or credit account.

Based on the above, it is possible to use the mobile phone 1 to make a decision when purchasing a small-value item from a vending machine.

As is clear from the explanations above, even in the transaction method, the payment can be approved only by the QR authorized certification key issued by the authentication server 41 without conveying confidential information such as the user credit number to the vending machine side.

Next, an explanation will be given of the method of making a payment when purchasing a product at an electronic store on the Internet with reference to the flowcharts of FIGS. 16 and 17.

First, the user (product purchaser) sets his or her mobile phone 1 to the mobile shopping mode, and uses the input means 14 to access a store on the Internet. The user inputs the number of the product to be purchased, the purchase price, and the receiving method, and orders the product (step 1601).

The store that receives the order for the product sends a request for personal authentication to the authentication server 41. The authentication server 41 that receives this personal authentication request sends a request to the mobile phone 1 for inputting its personal identification number (the number registered in 706 in FIG. 7), the payment method, and the store ID.

Then, the user of the mobile phone 1 inputs his or her personal identification number (the number registered in 706 in FIG. 7), the payment method, and the store ID (step 1602). This content is sent to authentication server 41 as a request to issue a QR authorized certification key. Here, the decision-making method is the same as in the previous example.

The authentication server 41 that receives this QR authorized certification key request performs the authentication process of the user (step 1603). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched using the PIN number and the credit card number (or the web money account number, or debit card number), and it is checked whether the user with the PIN number and the credit card

number (or the web money account number, or debit card number) is registered in the user DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1604). Even if the personal ID number and the credit card number (or web money account number or debit card number) are not registered, the user is either an unauthorized user or an unregistered user, and a message indicating that the transaction is not possible is sent back to the mobile phone 1 (step 1604). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1602 is automatically deleted.

However, if the store ID, the PIN number, and the credit card number (or web money account number, or debit card number) are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1605) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1606). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1607) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; The message, "Please insert it into the reader at the time of payment at the pick-up store specified by the customer", will be displayed.

In addition, the authentication server 41 sends a request to the store to issue a certificate of trust. The store that receives this request for the issuance of a certificate of trust generates the certificate of trust that includes the trust number, user name, product number, amount, settlement method, and receipt method, and sends it back to the authentication server 41. This certificate of trust is equivalent to a product order form from the perspective of the user.

The authentication server 41 that receives the certificate of trust integrates the QR authorized certification key 1201 and the certificate of trust, and sends it to the mobile phone 1 as the certificate of trust with the QR authorized certification key.

The user then goes to the pick-up store that he or she has designated, and inserts the certificate of trust with the QR authorized certification key into the reader of the QR code reader 21 attached to the store terminal 22 of the pick-up store, with the certificate of trust displayed on the display unit 11 (step 1608). The QR code reader 21 then reads the QR authorized certification key (step 1609) displayed on the display unit 11 of the mobile phone 1, and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1610), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the certificate of trust with the QR authorized certification key read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the certificate of trust with the QR authorized certification key has been issued by the authentication server itself, only part of the information such as the payment number and the personal authentication may be sent. FIG. 17 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1611). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1613), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR authorized certification key, and the certificate of trust with the QR authorized certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1613). In addition, the user is notified verbally that the store staff cannot deliver the product or make a payment decision.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and it is found that the information (all or part) on the certificate of trust with the QR authorized certification key received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 will reply to the store terminal 22 with detailed approval. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1614). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1615).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the transaction is completed by operating the transaction button (step 1616). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1617). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. In addition, the authentication server 41 sends the authorization completion information to the financial institution 42.

Based on the above, the customer can select a product at a store on the Internet using the mobile phone 1, and receive and approve the product at a pick-up store designated by the user.

As is clear from the explanations above, according to the transaction method, the payment can be made only with the QR authorized certification key issued by authentication server 41, without conveying any confidential information such as the user's credit number to the store side on the Internet.

Such a method can be used to order tickets for movies, etc., on the Internet, and store the QR authorized certification key on the mobile phone 1, and insert it into the reader at the entrance of the movie theater, for example, to make use of the operational format such as entering the movie theater without a ticket. Here, instead of displaying the certificate of trust with the QR authorized certification key to the display unit 11 and having the reader 21 to read, a method can be adopted in which the certificate of trust with the QR authorized certification key is transferred to a personal computer (PC), printed with an attached printer, and read with a reading device at the receiving store. In this case, the printer's printing toner or ink mixed with the crystal powder similar to the signs 19 and 20 can be used.

FIG. 18 is a flowchart illustrating the procedure. This flowchart corresponds to the continuation of FIG. 16.

First, if the QR authorized certification key is received on the mobile phone 1, the QR authorized certification key is forwarded to a personal computer (PC) (step 1620) and printed with the attached printer (step 1621). A printing example is shown in FIG. 19(a).

Therefore, the user brings the printed certificate of trust with the QR authorized certification key to the receiving store designated by the user, and inserts it into the reading unit of the QR code reader 21 attached to the store terminal 22 at the receiving store. The QR code reader 21 then reads the printed certificate of trust with the QR authorized certification key (step 1622) and forwards the reading to the store terminal 22.

The store terminal 22 then sends the results of the reading of the certificate of trust with the QR authorized certification key to the authentication server 41 as a request for approval, as in the case of FIG. 17.

When the authentication server 41 receives a request for approval, it first examines the validity of whether the QR authorized certification key of the certificate of trust with the QR authorized certification key is genuinely issued by the customer (step 1623). If the result is that it is not legitimate, it is determined that it is fraudulent use, and after registering this with the unauthorized usage information database (FIG. 9) (step 1624), an unauthorized usage message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR authorized certification

key, and the certificate of trust with the QR authorized certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1625). In addition, the user is notified verbally that the store staff cannot deliver the product or make a payment decision.

However, if it is found that the QR authorized certification key is genuine, the authentication server 41 will reply to the store terminal 22 with the detailed approval. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1626). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1627).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the transaction is completed by operating the transaction button (step 1628). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1629). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. In addition, the authentication server 41 sends the authorization completion information to the financial institution 42. Based on the above, even if the user does not bring his or her mobile phone 1, the user can receive the product ordered at a store on the Internet at the receiving store designated by the user and make the final payment.

In this case, it is not necessarily essential to transfer the certificate of trust with the QR authorized certification key from the mobile phone 1 to a personal computer (PC), and it may be received directly from the personal computer as a network terminal and printed with a printer.

Using these methods, it is possible to use the printed certificate of trust with the QR authorized certification key in place of, for example, movie tickets ordered over the Internet. FIG. 19(b) shows an example of an admission ticket.

In each of the above examples, it is explained that the same mobile phone 1 is used as a network terminal that transmits information about the payment, etc., of products and as a network terminal that receives code character information images such as a QR payment certification key, but it is not limited to this, and the network terminal for transmitting information and the network terminal for receiving the code character information images may be used as a separate terminal.

By using this, it is also possible to transmit the code character information image to a third party's network terminal. Therefore, instead of gifting products or gift certificates to a third party, it is possible to make a payment using a code character information image transmitted to the third party's network terminal.

A payment processing method in this case will be explained below with reference to FIGS. 20 to 28.

In this case, the payment authorization institution 4 is provided with a gift information database (DB), and the authentication server 41 is provided with a gift information registration processing program 412. As shown in FIG. 20, for example, the gift information DB stores information including the giver ID 2001, the receiver ID 2002, the gift details 2003, the identification ID 2004, and the payment processing date 2005.

In addition, the gift information registration processing program described above is a program used when registering information on specific products or gifts of a certain amount in the gift information DB using the system.

In this payment processing method, the ordering party (the giver of the product) first sets the mobile phone 1 as an information transmitting terminal to the mobile shopping mode, and then uses the input means 14 to enter his or her identification PIN (the number registered in 706 in FIG. 7), payment method, user name of the recipient of the product and the recipient information such as the user ID, and gift details (in this case, the item number of the product to be gifted) (step 2101). Here, the payment method is the same as in the previous example.

When the input is complete, the transmission operation is performed. The information entered in step

2101 is then sent to authentication server 41 as a gift information transmission request.

The authentication server 41 that receives this gift information transmission request performs the authentication process of the user (step 2102). That is, the user information DB 44 is searched by the PIN number, the credit card number (or web money account number, or debit card number) included in the gift information transmission request, and the user of the PIN and the credit card number (or web money account number, or debit card number) is checked to see if the user is registered in the user information DB 44. In addition, the user information DB 44 is searched by the user ID, etc. as the recipient information, and as a result, if the PIN and the credit card number (or web money account number, or debit card number) are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 2103). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and information such as the PIN entered in step 2101 is automatically deleted.

However, if the PIN number, the credit card number (or web money account number, or debit card number), the user ID as the recipient information, and the user name are registered correctly, the user is authenticated as an officially registered user, and the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 2104) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or gift information is sent (step 2105). In other words, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message including a message such as insufficient balance to the giver's mobile phone 1. However, if the credit result is OK, the gift information is sent to the recipient's mobile phone 1 input in step 2101. As for this gift information, as shown in FIG. 24(a), the giver's user name and the product name as the gift contents are displayed, and the recipient sends back information to the authentication server 41 regarding refusal or acceptance of the gift contents (step 2106). If the authentication server 41 receives this reply and the information of a rejection is returned, it sends a confirmation message to the recipient's mobile phone 1 to that effect, and after sending a message of the rejection to the giver's mobile phone (see Fig. 24(c)), the information such as the PIN entered in step 2101 is automatically deleted. (step 2107) However, if the information of acceptance is returned, the authentication server 41 sends a request to the recipient's mobile phone 1 to enter the method of receiving the goods (see FIG. 24(b)).

Therefore, the user of the mobile phone 1 enters the store ID and the receiving method (step 2108). The contents are then sent to the authentication server 41 as a QR payment certification key issuance request. The authentication server 41 that receives this QR payment certification key request performs the authentication process of the store (step 2109). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. As a result, if the store ID is not registered, it is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the recipient's mobile phone 1 (step 2110). In the mobile phone 1, after confirming that the message indicating that the transaction is not possible is displayed on the display unit 11, another store ID or the like can be inputted.

However, if the store ID is registered correctly, the store is authenticated as an officially registered store, and the authentication is accepted.

If the authentication is OK, the authentication server 41 generates a QR payment certification key configured with a two-dimensional code as shown in FIG. 3(d). (Step 2211) The QR payment certification key includes at least the payment number, the personal identification, name, and the payment method information.

In addition, the authentication server 41 sends a request to the store to issue a certificate of trust. The store that receives this request for the issuance of a certificate of trust generates the certificate of trust that includes the trust number, user name, product number, amount, payment method, and receipt method, and sends it back to the authentication server 41. This certificate of trust is equivalent to a product order form from the perspective of the user.

The authentication server 41 that has received the certificate of trust combines the QR payment certification key 1201 with the certificate of trust and transmits it to the recipient's mobile phone 1 as a certificate of trust with the QR payment certification key.

In the mobile phone 1, the received QR payment certification key is displayed on the display unit 11 as shown by the reference numeral 1201 in FIG. 12. At the same time, a message such as "You can make

payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

The user then goes to the pick-up store that he or she has designated, and inserts the certificate of trust with the QR payment certification key into the reader of the QR code reader 21 attached to the store terminal 22 of the pick-up store, with the certificate of trust displayed on the display unit 11 (step 2112). The QR code reader 21 then reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 2113), and reads the QR payment certification key with the certificate of trust displayed on the display unit 11 of the mobile phone 1 (step 2114), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, mobile phone number, and the certificate of trust with the QR payment certification key read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, as for the certificate of trust with the QR payment certification key, it is only necessary to know that it has been issued by the authentication server 41 itself, so only some information such as the payment number and personal authentication may be sent. FIG. 23 shows that only the payment number and the personal authentication information is sent in the payment authorization request.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2115). As a result, if either number is unregistered or different from the registered number, it is determined to be unauthorized use and after registering in the unauthorized use information database (FIG. 9) (step 2116), an unauthorized use message is sent to the store terminal 22 and the mobile phone 1 on the receiving side. In addition, an unauthorized use messages is also sent to the mobile phone 1 on the giver side.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR payment certification key, and the certificate of trust with the QR payment certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2117). In addition, the user is verbally notified that the store staff cannot deliver the product and that payment cannot be made.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and it is found that the information (all or part) on the certificate of trust with the QR payment certification key received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 will reply to the store terminal 22 with detailed payment approval. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed payment approval, displays all or part of the received detailed payment information as user information in the display unit (step 2118). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 2119).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the payment is completed by operating the payment button (step 2120). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41.

The authentication server 41 that receives this payment completion message updates the purchase history information of the user on the giver side (step 2121). After this, the payment details for confirmation are sent to the terminal for information transmission on the giver's side. As a result, a confirmation message and the payment details 2501 and 2502, as shown in FIG. 25, are displayed on the display unit 11 of the giver's mobile phone 1, for example (step 2122). In addition, the authentication server 41 sends the payment completion information to the financial institution 42.

Based on the above, a specific product can be selected using the giver's terminal, and the product can be received and settled at a store designated by the recipient.

As is clear from the above explanation, according to the transaction method, payment can be made only with the QR payment certification key issued by authentication server 41 without conveying any confidential information such as the credit number of the giver to the store or the recipient of the gift.

Furthermore, the recipient of the gift can be authenticated more reliably.

In this transaction method, the gift information is sent to the recipient and the recipient chooses whether or not to accept the gift, although the recipient who will accept or reject the gift is set in advance. The authentication server may decide whether to accept or reject the gift based on this setting. In this case, the above determination processing at the authentication server is performed instead of step 2106 and step 2107.

In addition, the contents of gifts given by this system may be not limited to specific products, but it may be content equivalent to a gift certificate of a certain gift amount.

FIGs. 26 and 27 are flowcharts illustrating the procedure in such a case. The flowchart in FIG. 26 corresponds to the continuation of FIG. 21.

In this case, as a prerequisite, in step 2101 of FIG. 21, a certain amount will be entered in place of the item number as the gift content.

Thereafter, after the processing shown in the flowchart of FIG. 21 is performed, the user on the receiving side inputs the receiving store ID and the purchase price of the product (step 2130). The contents are then sent to the authentication server 41 as a QR payment certification key issuance request.

The authentication server 41 that receives this QR payment certification key issuance request performs the authentication process for the store and the purchase amount (step 2131). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. The gift information DB is also searched to check whether the input purchase amount is within the range of the amount stored in the DB. As a result, if the store ID is not registered or the purchase amount exceeds the gift amount, a non-transactionable message is returned to the mobile phone 1 (step 2132). On the receiver's mobile phone 1, after confirming that the message indicating that the transaction is not possible is displayed on the display unit 11, the recipient enters another store ID or purchase amount. However, if the store ID is registered correctly and the purchase amount entered is within the range of the gift amount, the product is certified to be the amount that can be purchased at the store with the official registration, and the certification is accepted.

If the certification is OK, the authentication server 41 generates a QR payment certification key composed of a two-dimensional code as shown in FIG. 3(d) and sends it to the mobile phone 1 (step 2133). The QR payment certification key includes at least the payment number, the personal identification, name, and the payment method information.

In the mobile phone 1, the received QR payment certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 2134). The store staff enters the price of the desired purchase item using the store terminal (step 2135).

In parallel, the user inserts and attaches the mobile phone 1 with the QR payment key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 2136). The QR code reader 21 then reads the QR payment certification key 1201 displayed on the display unit 11 of the mobile phone 1 on the receiving side (step 2137), and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 2138), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the QR payment certification key 1201 read from the mobile phone 1 on the receiving side to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the QR payment certification key 1201 was issued by the authentication server itself, only part of the information such as the payment number and the personal authentication may be sent. When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2139). As a result, if either number is unregistered or different from the registered number, it is determined to be unauthorized use and after registering in the unauthorized use information database (FIG. 9) (step 2140), an unauthorized use message is sent to the store terminal 22.

and the mobile phone 1 on the receiving side. In addition, an unauthorized use message is also sent to the mobile phone 1 on the giver side.

In the receiver's mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR payment certification key 1201, and the QR payment verification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2141). In addition, the user is notified verbally that payment cannot be made by the store staff.

However, if both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) of the QR payment certification key 1201 received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 returns the detailed payment approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed payment approval information as user information in the display unit (step 2142). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 2143).

If there is a confirmed response of the person's purchase intention, the payment is completed by the payment button operation (step 2144). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41. The authentication server 41 that receives this payment completion message updates the purchase history information of the user on the giver side (step 2145). Thereafter, the payment details for confirmation are transmitted to the mobile phone 1 of the giver. In addition, the payment completion information is sent to financial institution 42. As a result, for example, the payment details 2501 and 2502 for confirmation as shown in FIG. 25 are displayed on the display unit 11 of the giver's mobile phone 1 (Step 2146). The payment details 2501 and 2502 can be stored until deleted by the user. However, since the QR payment certification key 1201 is valid only once, it is automatically deleted after a prescribed time. In addition, the financial institution 42, that receives the payment completion information, takes procedures to debit the payment from the designated account of the user on the giver's side.

Based on the above, a certain amount can be specified using the terminal on the giver's side, and the recipient can freely purchase products, etc. at the store within the range of that amount, and settle the payment.

As is clear from the explanation above, according to the transaction method, even if a gift certificate of a certain amount is given, the payment can be made from the account of the giver only by the QR payment certification key issued by authentication server 41, without the store or the receiver receiving the confidential information such as the credit number of the giver. Further, the recipient can be authenticated more reliably.

In addition, in each of the above examples, payment by a financial institution is assumed, but the present invention can also be used when making payment by service points for all or part of the payment price. A payment processing method in this case will be explained below with reference to FIGS. 28 to 30.

In this case, the payment authorization institution 4 is provided with a service point database (DB), and the authentication server 41 is provided with a service point registration processing program.

FIG. 28 is a diagram illustrating an example of the storage information for the service point DB, in which the update date 2801, the store name 2802, the number of additional points 2803, the number of points used 2804, and the service point balance 2805 are stored. This service point information is stored for each user in the order of update the date and time.

In addition, the service point registration processing program performs the payment processing based on service points obtained by purchasing products using this system.

Moreover, there are cases where the use of service points is processed by discounting the amount equivalent to a certain amount at the time of purchase of products based on the number of points, and where the service points are exchanged for products determined in advance based on the number of points, but in this embodiment, it is indicated that the service points are processed as the purchase price of the products.

In this payment processing method, the user (product purchaser) first sets the mobile phone 1 to the mobile shopping mode, and then using the input means 14, the user inputs the store ID of the store from which the product is to be purchased, along with his or her personal identification number (the number registered in 706 in FIG. 7), and the service points corresponding to the purchase price of the product (step 2901). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17.

When the input is complete, the transmission operation is performed. The information entered in step 2901 is then sent to authentication server 41 as a request to issue a QR payment certification key.

The authentication server 41 that receives this QR payment certification key issuance request performs authentication processing for the store and the user (step 2902). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched by PIN to see if the user is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 2903). Furthermore, if the PIN is not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 2901 is automatically deleted.

However, if the store ID and PIN are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the service point DB of the user is searched to inquire about the service point balance (step 2904). In response to this inquiry result, a non-transactionable message or QR payment certification key is generated (step 2905). In other words, if the result of the inquiry is that there is no balance, the authentication server 41 sends a non-transactionable message including a message such as insufficient balance to the mobile phone 1. However, if there is a balance, a QR payment certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 2906) and transmitted to the mobile phone 1. The QR payment certification key includes at least the payment number, the personal authentication, and name information.

In the mobile phone 1, the received QR payment certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 2907). The store staff calculates the number of points corresponding to the purchase price by entering the price of the desired product in the store terminal (step 2908). In parallel, the user inserts and attaches the mobile phone 1 with the QR payment key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 2909). The QR code reader 21 then reads the mobile phone serial number and the mobile phone number from the signs 19, 20 of the mobile phone 1 (step 2910), and reads the QR payment certification key 1201 displayed in the display 11 (step 2911), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the QR payment certification key 1201 read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, it may be understood that the QR payment certification key 1201 was issued by the authentication server itself, so only some information such as the payment number and the personal authentication may be sent. FIG. 30 shows that only the payment number and the personal authentication information is sent in the payment authorization request.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2912). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 11) (step 2913), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that receives the unauthorized use message, the unauthorized use message itself

functions as a deletion command for the QR payment certification key 1201, and the QR payment certification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2914). In addition, the user is notified verbally that payment cannot be made by the store staff.

However, if both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) of the QR payment certification key 1201 received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 returns the detailed payment approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed payment approval information as user information in the display unit (step 2915). The store staff confirms the purchase intent with the user themselves by looking at the display content, and the content of the desired product to be purchased, and the number of points corresponding to the price (Step 2916).

If there is a confirmed response of the person's purchase intention, the payment is completed by the payment button operation (step 2917). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41. The authentication server 41 that receives this payment completion message updates the user's purchase history information and service point information (step 2918). After this, the payment details for confirmation are sent to the mobile phone 1. The payment details can be saved until the user deletes them. However, since the QR payment certification key 1201 is valid only once, it is automatically deleted after a prescribed time.

Based on the above, it is possible to use a mobile phone 1 to make payments using service points when purchasing products at general stores.

As is clear from the explanations above, according to the transaction method, even when making a payment using service points, it is possible to perform the payment using only the QR payment certification key issued by the authentication server 41, making it possible to eliminate the need for a point card or the like. In addition, the authentication of service users can be performed more reliably.

The methods shown in each of the above examples do not require financial settlement, but can be used instead of tickets such as admission tickets or receipts for goods, etc. It should be noted that the procedures described above can be implemented with some changes depending on the financial institution or the like. Furthermore, the procedure performed by the authentication server 41 may be recorded as a program for decision making on a recording medium such as a CD-ROM, and provided to the decision-making system builder.

Although the mobile phone serial number and the mobile phone number signs are recorded using recording materials mixed with a special crystalline powder, other methods of recording in a recording format that can physically determine the authenticity may be used.

In addition, in the next-generation mobile communication services that use mobile phones etc. equipped with an IC card (UIM card), the mobile phone numbers etc. are written on the IC card, and an operation mode is being considered in which the same mobile phone number can be used on different terminals by replacing the IC card.

Thus, in this case, the IC card may be labeled or printed as shown in FIG. 3(c).

In addition, in this case, it is necessary to make the sign readable by an external reader while the IC card is inserted into the slot provided in the mobile phone or the like.

Examples of handsets used in this case will be described with reference to FIGS. 31 and 32.

FIGS. 31 and 32 are partial perspective views of a mobile phone used in the present embodiment, wherein in each figure, the IC card installed in the mobile phone that stores information such as the mobile phone number is represented by the number 300, and a sign 311 as shown in FIG. 3(c) is pasted or printed on the surface of the IC card. It should be noted that, in place of the serial number of the mobile phone, the identification information of each IC card or of the owner is recorded on the sign 311 together with the mobile phone number.

In the present embodiment, a recess 300 is formed that allows the IC card to be mounted such that the sign 311 affixed to the IC card is visible from the reading direction, as shown by the arrow in the figure, and such as on the back side of the mobile phone 1, for example, as shown in FIG. 31(a). This allows the reader 22 to read the label in the same way as when a label is affixed on the casing of the mobile

phone 1.

Also, as shown in FIG. 31(b), an IC card insertion slot 301 found in the mobile phone 1 may be provided, and an opening 302 may be formed in the area where the sign 311 is located so that the sign can be read (visually recognized) by an external reading device when the IC card 310 is inserted into the slot 301. The front surface of the opening 302 may be shielded with a transparent resin material or the like, as long as the sign 311 is visible from the reading direction shown by the arrow in the figure.

Other configurations may also be used if the sign 311 can be read by an external reader, for example, the entire casing of the mobile phone may be made of a transparent resin material or the like that allows the inside to be seen.

In this way, the invention can be applied to mobile phones, etc. that support the next generation of mobile communication services, and in addition, it is possible to increase security by eliminating the need to store data such as credit card numbers in the IC cards.

It should be noted that the mobile phone 1 may be provided with a reading device for the sign 311, and the reading device may read the sign and transmit the read information to the store terminal.

In this case, for example, as shown in FIG. 32(a), a reading sensor unit 303 connected to the control unit 13 (see FIG. 2(a)) is provided at a location where the mark 311 of the IC card inserted into the slot 301 is located. As a result, the information on the sign 311 read by the reading sensor unit 303 can be transmitted to the authentication server 41 via the transmitting means of the mobile phone 1. It should be noted that the processing of reading information on the sign 311 may be performed while the IC card is inserted into the slot 311, and in this case, a sensor unit may be provided in the portion of the slot corresponding to the portion through which the marker 311 passes.

Moreover, as shown in FIG. 32(b), the IC card 310 is not limited to the one that is inserted into the mobile phone 1, and by inserting a part of the IC card 310 into the slit 304 formed on the side of the mobile phone 1, and sliding it in the sliding direction shown by the arrow in the figure, it is conceivable that the information in the IC card 310 may be read by the sensor unit (not shown). In this case, when sliding a portion of the IC card 310 into the slit 304, a portion of the site corresponding to the site through which the sign 311 passes within the slit 304 may be provided with a reading sensor unit 305. In addition, when using a wireless or optical non-contact type IC card as the IC card 310, and by inserting the IC card 310 into a reading device installed at each store etc., the sign 311 may be read directly; or as with the above example, the mobile phone 1 may be equipped with a reading device, and the information on the sign 311 may be recognized by radio or light, similar to the information in the IC card 310.

[Publication type] Publication of amendments pursuant to the provisions of Article 17-2 of the Patent Act

[Divisional classification] Division 6, and Division 3

[Issuance date] May 26, 2005 (5/26/2005)

[International publication number] WO2002/008981

[Annual number of issues] Publication/registered publication 2004-001

[Application number] Japanese Patent Application 2002-514614 (P2002-514614)

[International Patent Classification 7th Edition]

G06F 17/60

G06K 17/00

G06K 19/06

G06K 19/07

H04Q 7/38

[FI]

G06F 17/60 414

G06F 17/60 422

G06F 17/60 506

G06F 17/60 512

G06F 17/60 ZEC

G06K 17/00 L

G06K 19/00 E

G06K 19/00 J

H04B 7/26 109S

[Procedural amendment]

[Submission date] May 29, 2003 (5/29/2003)

[Procedural amendment 1]

[Name of item subject to amendment] Procedural amendment form

[Name of item subject to amendment] Procedural amendment 1

[Correction method] Changed

[Details of the amendment]

[Procedural amendment 1]

[Name of document subject to amendment] Specification

[Name of item subject to amendment] Full text

[Correction method] Changed

[Details of the amendment]

[Document name] Specification

[Title of invention] Commercial transaction method and network terminal and commercial transaction system

[Scope of Claims]

[Claim 1] A commercial transaction method comprising of a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a network terminal with a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the

product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment for the product using a payment terminal of a product purchaser.

[Claim 2] A commercial transaction method comprising of a network terminal that includes a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving the information regarding product payment via a communication network; an IC card having a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment of the product price amount using the payment terminal of the product purchaser based on the payment authorization information.

[Claim 3] The commercial transaction method according to any of Claims 1 or 2, characterized in that the network terminal includes an input means for inputting the information related to the commercial transactions; an imaging means for capturing the image information encoded with the identification information of the product provider or the product, and inputs information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number, from the input means, and transmits the entered information regarding the commercial transaction to the payment authorization institution device; and a step of decrypting the image information and receiving the payment certification key information generated according to the product provider's authentication and the purchaser's own authentication and credit results.

[Claim 4] A commercial transaction method comprising of a network terminal that includes a display means for receiving and displaying the payment certification key information regarding the commercial transactions from a payment authorization institution device; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network, which transmits the payment certification key information displayed on the display means to the payment terminal installed at the product purchase source, and whereby payment for the product selected by the purchaser is executed by the product purchase source's payment terminal; and a sign recording the identification information registered in advance with the payment authorization institution, whereby the sign emits the identification information by a reflected light of a predetermined wavelength

in response to an irradiated light of a predetermined wavelength.

[Claim 5] The network terminal according to Claim 4, characterized in that the network terminal is equipped with an input means for inputting information regarding the commercial transactions, and whereby the input means includes an imaging means for capturing image information in which the identification information of a product provider or a product is encoded.

[Claim 6] A commercial transaction system comprising of a display means for displaying information on payment; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a network terminal with a sign recording the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and authorization regarding the payment; a product provider device that performs payment for a product at a product provider, wherein the payment authorization institution device generates the payment certification key information regarding the commercial transaction; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with the payment authorization institution in accordance with the authentication result of the identification information, whereby the payment approval information corresponding to the payment certification key information is transmitted from the payment authorization institution to the payment terminal of the product purchase source; and a means for delivering the product ordered by the purchaser and making payment for the product.

[Claim 7] A commercial transaction system comprising a network terminal that includes a display means for displaying information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; an IC card having a sign that emits the pre-recorded identification information using a reflected light of a predetermined wavelength with respect to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that settles the price of the product at the product provider; a payment authorization institution device that generates the payment certification key information regarding the commercial transactions; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with a payment authorization institution; and a means for transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the product provider device in accordance with the authentication result of the identification information.

[Claim 8] The commercial transaction system according to Claim 6 or Claim 7, characterized in that the network terminal has an input means for inputting information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number; the input means includes an imaging means for capturing image information encoded with the identification information of the product provider or the product; and a payment authorization institution device that further includes a decoding means for decoding the image information captured and transmitted by the imaging means.

[Detailed description of invention]

[0001]

Technical field

The present invention relates to a commercial transaction method, a commercial transaction device and a commercial transaction system that can be used for payment of products purchased at various stores such as supermarkets, electronic stores opened on Internet servers, or vending machines such as for potable drinking water, using terminals that can be connected to a network such as via mobile phones.
[0002]

Background technology

With the addition of the WWW browsing function (World Wide Web) to the mobile phone, the transaction format of using the mobile phone to access the Internet, browse various types of information, goods, and services, and order the provision of such information, goods, and services as necessary is rapidly expanding. Here, in the present invention, information (content) such as music software that does not have a shape, goods that have a shape, and services such as home delivery service and nursing care service are all defined as products that are subject to commercial transactions. In this case, there are also free nursing services provided by public institutions, but even if they are free, they are included in the products subject to transactions.

However, even if a product is ordered using a mobile phone, the settlement method still follow traditional business practices, such as bank transfer, sending of cash, and cash on delivery upon arrival of the product.

In recent times, instead of this conventional method, a method has been implemented in which a credit card number is notified to the product provider (store) at the same time as the product is ordered, and payment is made through the credit card company.

However, this payment method is based on the premise that the number or information that only the credit card company and the person themselves should know will not be leaked to outside parties, and if leaked, there is a risk that it will be misused.

Therefore, in the next-generation mobile communication services starting in May 2001, which will equip mobile phones with an IC card called a UIM (User Identity Module), a method is being considered in which confidential data such as credit card numbers are encrypted using a cryptographic program in the IC card allowing payments to be made.

However, even if the data is encrypted and saved using a cryptographic program, if the mobile phone itself is lost, there is a risk that it will be decrypted by an unauthorized third party and misused. In particular, it is believed that there will be many forms of storing not only credit card numbers but also other confidential data such as bank account numbers, insurance card numbers, and electronic money at the same time in IC cards, so the risk of being decrypted by an unauthorized third party is higher than with traditional payment methods.

In addition, as with contactless IC cards, networks using wireless networks have a problem in that there is a greater possibility of information leaking to the outside due to hacking, including unauthorized access, than wired networks.

In addition, due to the emergence of unauthorized stores, there is the risk that confidential data may be intercepted and misused during payment at these store.

Furthermore, there is also the problem that the cost of the mobile device itself will increase, the power consumption will also increase, and the battery life will be shortened.

The present invention is made to solve such problems, and the purpose is to provide a commercial transaction method, device, and system that can authenticate the person without disclosing confidential data such as credit numbers to a person authentication institution or credit card company, and can safely settle the purchase of goods.

[0003]

Disclosure of the Invention

In order to achieve the above objectives, the commercial transaction method of the present invention is characterized by being configured as follows.

In other words, it is a method comprising of a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving information regarding product payment via a communication network; a network terminal with a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an

irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment for the product using a payment terminal of a product purchaser.

The method also comprises of a network terminal that includes a display means for displaying the information regarding the payment; a transmitting/receiving means for transmitting and receiving the information regarding product payment via a communication network; an IC card having a sign that contains the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a prescribed wavelength in response to an irradiation light of a prescribed wavelength in order to make a payment regarding the product to be traded as provided by a product provider; the commercial transaction method further comprises of a step of receiving the payment certification key information regarding a commercial transaction from a payment authorization institution device; a step of displaying the received payment certification key information on the display means; a step of transmitting the payment certification key information displayed on the network terminal to a payment terminal installed at the product purchase source; a step of reading the identification information recorded on the sign and transmitting it to the payment terminal; a step of transmitting part or all of the payment certification key information transferred to the payment terminal and the identification information to the payment authorization institution device; a step of authenticating whether or not the identification information is genuine information registered in advance in a payment authorization institution device; a step of transmitting the payment authorized information corresponding to the payment certification key information from the payment authorization institution device to the payment terminal of the product purchase source according to the authentication result of the identification information; and a step of executing payment of the product price amount using the payment terminal of the product purchaser based on the payment authorization information.

Further, the network terminal includes an input means for inputting the information related to the commercial transactions; an imaging means for capturing the image information encoded with the identification information of the product provider or the product, and inputs information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number, from the input means, and transmits the entered information regarding the commercial transaction to the payment authorization institution device; and a step of decrypting the image information and receiving the payment certification key information generated according to the product provider's authentication and the purchaser's own authentication and credit results.

The network terminal of the present invention comprises of a display means for receiving and displaying the payment certification key information regarding the commercial transactions from a payment authorization institution device; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network, which transmits the payment certification key information displayed on the display means to the payment terminal installed at the product purchase source, and whereby payment for the product selected by the purchaser is executed by the product purchase source's payment terminal; and a sign recording the identification information registered in advance with the payment authorization institution, whereby the sign emits the identification information by a reflected light of a predetermined wavelength in response to an irradiated light of a predetermined wavelength.

The network terminal is equipped with an input means for inputting information regarding the

commercial transactions, and whereby the input means includes an imaging means for capturing image information in which the identification information of a product provider or a product is encoded.

The commercial transaction system of the present invention comprises of a display means for displaying information on payment; a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; a network terminal with a sign recording the identification information registered in advance in the payment authorization institution device, which emits the identification information by a reflected light of a predetermined wavelength in response to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and authorization regarding the payment; a product provider device that performs payment for a product at a product provider, wherein the payment authorization institution device generates the payment certification key information regarding the commercial transaction; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with the payment authorization institution in accordance with the authentication result of the identification information, whereby the payment approval information corresponding to the payment certification key information is transmitted from the payment authorization institution to the payment terminal of the product purchase source; and a means for delivering the product ordered by the purchaser and making payment for the product.

Also, it is characterized in that the commercial transaction system comprises of a network terminal that includes a display means for displaying information regarding the payment and a transmitting/receiving means for transmitting and receiving information regarding the payment of the product via a communication network; an IC card having a sign that emits the pre-recorded identification information using a reflected light of a predetermined wavelength with respect to an irradiation light of a predetermined wavelength; a payment authorization institution device that performs authentication and approval regarding the payment; a product provider device that settles the price of the product at the product provider; a payment authorization institution device that generates the payment certification key information regarding the commercial transactions; a means for transmitting and displaying on the network terminal, which receives part or all of the payment certification key information and identification information as a result of reading the identification sign from the product provider device; a means for authenticating whether the identification information is genuine and whether it is registered in advance with a payment authorization institution; and a means for transmitting the payment approval information corresponding to the payment certification key information from the payment authorization institution to the product provider device in accordance with the authentication result of the identification information.

Moreover, the network terminal has an input means for inputting information regarding the commercial transaction, including at least the product provider or the product identification information, the payment method, the purchase amount, and the purchaser's personal identification number; the input means includes an imaging means for capturing image information encoded with the identification information of the product provider or the product; and a payment authorization institution device that further includes a decoding means for decoding the image information captured and transmitted by the imaging means.

[0004]

Detailed Description of the Preferred Embodiments

The embodiments of the present invention will be described in detail below with reference to the accompanying drawings.

FIG. 1 is a system configuration diagram illustrating an embodiment of the overall configuration of the system for implementing the commercial transaction method of the present invention, which includes a mobile phone 1 as a network terminal used by a product purchaser, a store 2 from which the product is provided, a vending machine 3 such as for potable water, and a payment authorization institution 4, which is connected by a communication network 5. The communication network 5 includes a wireless line, a wired line, and an internet network. Here, the network terminal refers to a terminal that can be connected to a network such as the Internet, and in addition to the mobile phone 1 shown in the following example, it includes various other types such as PHS, PDA, personal computer, digital television, etc.

The mobile phone 1 is a commercially available mobile phone with a function that can be connected to

an internet network, and as shown in the schematic block diagram of FIG. 2(a), it comprises of a display 11, a wireless transmitter/receiver 12, a control 13, an input 14, a receiver 15, a memory 16, and an external input and output interface 17. In the Internet connection mode, the display 11 displays the Internet connection menus such as news, mobile banking, card/security/insurance, and mobile shopping, as shown in FIG. 2(b).

The external input and output interface 17 includes a wireless communication interface, such as an infrared interface such as Irda and a weak radio wave interface such as Bluetooth, and in this present embodiment, it is used when receiving the store identification number from the transmitter installed in the store. In addition, the external input and output interface 17 includes an interface for a barcode reader connected to a mobile phone or a built-in on the mobile phone, and the barcode reader may read the identification information, etc., of the store displayed with the barcode information or the identification information, etc. of the product. Furthermore, a camera connected to the mobile phone or a built-in on the mobile phone, and the identification information of each store or the identification information of the product displayed in the code character information image may be captured as image data by the camera. In this case, a program for decoding the code character information images captured as image data is provided in the authentication server of the payment authorization institution 4 above, and by decoding the code character information images sent from the mobile phone in the above program, the identification information of the store or product can be recognized. In addition, the aforementioned program may be provided on a mobile phone machine, and in this case, each of the aforementioned identification information recognized by decoding the code character information image on the mobile phone machine is transmitted to the aforementioned authentication server.

By using the external input and output interface 17 as described above, it is possible to input store or product identification information without operating the input unit 14. Here, the identification information of the product includes the product name, product type, and amount, etc.

It should be noted that entering the amount of the product is not a substitute for inputting the amount by a store staff, but it involves a self-scanning action, and is intended for the purchaser to know the payment amount information in advance. As shown in the front and side views of FIGS. 3(a) and (b), the mobile phone 1 of this embodiment is affixed with a first sign 19 that records the equipment serial number with the barcode 31, such as in FIG. 3(c), and a second sign 20 that records the mobile phone number with the barcode 31.

The barcodes of these signs 19 and 20 are printed with a printed material containing crystalline powder that emits the recorded information by the reflected light having a predetermined wavelength λ_a or λ_b in response to an irradiation light having a predetermined wavelength λ_a , as shown in FIG. 4(a). This crystalline powder is provided by SUNSTONE, Inc. in the United States, and is used for authentic identification of pharmaceutical products and banknotes. In this case, the characteristics are adjusted so that the wavelength of the irradiated light and the wavelength of the emitted light differ depending on the application and the system used.

In the present invention, the barcode of the device serial number and mobile phone number is printed on the signs 19 and 20 with a recording ink or toner mixed with the special crystalline powder, which is affixed to the front or side of the mobile phone 1, and the barcode recorded on the signs 19 and 20 is read with the irradiated light at a predetermined wavelength λ_a .

By affixing the device serial number and the mobile phone number signs 19 and 20 recorded with such special recording ink or toner to the mobile phone 1, it is not possible to read the device serial number and mobile phone number other than the irradiated light at a predetermined wavelength. Therefore, by pre-registering the device serial number and the mobile phone number with the payment authorization institution 4, it is possible to identify whether the mobile phone 1 is a legitimate device that can be used for commercial transactions in this system. The side sign 20 also serves to prevent modification of the mobile phone 1.

In this case, it is not necessarily essential to affix the aforementioned sign, and the aforementioned sign may be printed on the casing of the mobile phone itself using the recording ink or the like.

The barcodes of the signs 19 and 20 are inserted into the reader 40 in a cross-sectional configuration as shown in FIG. 4(b) and they are read by irradiating light with a predetermined wavelength. This reader 40 is installed in store 2 and the vending machine 3.

On the other hand, the display unit 11 displays payment certification key information configured with the two-dimensional code 32 as a code character information image as shown in FIG. 3(d). This two-dimensional code 32 is set in the standard code of the Japan Automobile Manufacturers Association

and the Japan Stationery Association. This is disclosed in, for example, the Japanese Unexamined Patent Application No. 10-214317, so a detailed explanation will be omitted here.

Using this two-dimensional code (hereinafter referred to as the QR code), approximately 7,000 characters (numbers) can be coded and recorded within the area of the display of the mobile phone 1. In the present invention, this QR code is used to represent the information of the payment certification key information. In detail, the information of the payment certification key information composed of a QR code is transferred to the mobile phone 1 to display it in the display 11 as shown in FIG. 3(a), and the mobile phone 1 in this display state is inserted into the reader 21 for reading sharing of the signs 19 and 20, so that the information of the payment certification key is read.

When using a QR code, as shown in FIG. 3(d), the recording contents can be read from any direction within 360° by means of the cutout symbols 33 to 35 located in three locations, so that the positional relationship with the reader is no longer bound, and it is suitable for use by the general user to insert into the reader unit and read. Also, since it is not necessary to strictly define the positional relationship, the reading time can be shortened accordingly. In addition, even if some part of the code is dirty or damaged, the errors can be corrected, and the number of reading errors can be reduced. In particular, as in the present invention, when reading the data while it is displayed on the display of the mobile phone 1, it is conceivable that reading errors may occur due to dirt on the display unit, etc., but by using a QR code, reading errors caused by dirt on the display unit, etc. can be reduced.

Returning to FIG. 1, the store 2 is equipped with a reader 21 for reading the signs 19, 20 and the QR code, and inputs the read signs 19, 20 and the QR code into the store terminal 22, which is a POS terminal, which allows for payments to be made using the in-store terminals. The vending machine 3 is also equipped with a reader 33 for reading the QR codes and the signs 19, 20.

On the other hand, the payment authorization institution 4 comprises of a authentication server 41, a financial institution (bank or credit company) 42, a store information database (DB) 43, a user information database (DB) 44, and a purchase history database (DB) 45.

The authentication server 41 performs personal authentication and store authentication in response to a personal authentication and store authentication request from the mobile phone 1, and it also makes a credit inquiry to the financial institution 42; and if the person and the store are registered in advance, and there is a response from the financial institution 42 that the credit is OK, processing is performed to permit payment of the product price using the mobile phone 1. The server includes a store registration processing program 410, a user registration processing program 411, a purchase history management program 412, an unauthorized use management program 413, an authentication processing program 414, a QR payment key generation program 415, and a transmission/reception program 416. It should be noted that an encryption/decryption program for encrypting and storing the data from each database 43, 44, and 45 is incorporated as necessary. Additionally, an encryption program for encrypting and transmitting the QR code and a decryption program for decoding the QR code can be incorporated. By encrypting the QR code, unauthorized transactions can be made even more difficult.

The store registration processing program 410 is a program used to register stores (including vending machines and electronic stores on the Internet) that perform payments using this system in the store information DB 43. In addition, the user registration processing program 411 is a program used when registering a user (product purchaser) who makes a payment using this system in the user information DB 44. The purchase history management program 412 is a program used when storing information on the purchase history of products purchased by a user (product purchaser) in the purchase history DB 45.

The unauthorized use management program 413 allows the system to be accessed by a store and a user who are not registered in the store information DB 43 and user information DB 44 in advance, and it is used when registering the store identification number or the device serial number or phone number of mobile phone 1 in the unauthorized use information database (FIG. 9) if the device serial number or phone number of mobile phone 1 is accessed by illegally rewriting it.

The authentication processing program 414 performs personal authentication and store authentication as well as credit inquiries to the financial institution 42 in response to the personal authentication and store authentication requests from the mobile phone 1; and if the person and the store have been registered in advance, and if there is a response from the financial institution 42 that the credit is OK, processing is performed to permit payment of the product using the mobile phone 1.

The QR payment key generation program 415 is a program that generates the payment certification key information composed of the QR code and passes it to the mobile phone 1 in order to authorize the

payment of the product. The payment certification key information (hereinafter referred to as “QR authorized certification key information”) composed of the QR code is the key information for the store to receive detailed approval information including the results of authentication of the purchaser and the store from the authentication server 41. By reading this QR authorized certification key information from the store reader 21 and sending the QR authorized certification key information read from the store terminal to the authentication server 41, the store terminal 22 can receive detailed approval information including the results of authentication of the purchaser and the store. In this case, if the QR authorized certification key information read by the reader 21 is different from that generated by the authentication server 41, approval of the authorized information cannot be obtained.

The transmission and reception program 416 is a program for sending and receiving the information necessary for decision making for access from users and stores.

FIG. 6 shows an example of the store information DB registration information, in which the store ID 601, the store name 602, address 603, and the phone number 604 are registered.

FIG. 7 is a diagram showing an example of the registration information for the user information DB, in which the user ID 701, the user name 702, address 703, the mobile phone serial number (device serial number) 704, the mobile phone number 705, PIN number 706, gender 707, date of birth 708, debit card number 709, credit card number 710, web money account number 711, and other personal characteristics information 712 are registered.

The web money account number 711 is used when making a payment using the web money when purchasing a small-value item such as drinking water from a vending machine. In addition, the personal characteristics information 712 is intended to register the photos, etc. of the individual, and to enable the store staff to verify the identity of the user using features such as a photo when making a payment at a store, and it is registered according to the user's wishes. For example, registering a photo of the user himself/herself has the advantage that store staff can detect misuse by others at the time of payment processing. Further, based on the date of birth 708, it is possible to discover whether the person is a minor or not, and the sale of alcoholic beverages and tobacco can be prohibited. In addition, the driver's license number, etc. may also be registered. By registering a driver's license number, etc., it is also possible to issue a certificate of identity from a third-party authentication server 41 using a mobile phone.

FIG. 8 shows an example of the store information in the purchase history DB, in which the date and time of use 801, the name of the store used 802, the approval amount 803, the cumulative amount of the current month's use 804, the cumulative amount of service points 805, and the previous use date 806 are stored. It should be noted that this purchase history information is stored in the order of date and time of use for each user.

FIG. 9 is a diagram showing an example of the information stored in an unauthorized use information database, with the unauthorized user's mobile phone serial number 901, mobile phone number 902, and store ID 903 registered. Here, if only the mobile phone number 902 is registered, this means that the mobile phone serial number is correct, and it also means that the person accessed the site by modifying the mobile phone number sign. In addition, a store that does not have a store ID 903 registered means that the store is not registered in the system, or it is a store that has its store ID illegally rewritten.

Here, for unregistered users and stores who are not malicious, a message may be sent to register at the time of access, and registration may be made as unauthorized use only for those who do not perform the registration procedures despite multiple registration instructions.

Below, (1) the method of decision making when purchasing products using a mobile phone 1 at a general store such as a supermarket, (2) the method of decision making when purchasing products at a vending machine, and (3) the method of decision making when purchasing products at an electronic store on the Internet will be explained with reference to the flowchart.

FIGS. 10 and 11 are flowcharts illustrating how decisions are made when purchasing products using a mobile phone 1 at general stores such as supermarkets.

First, the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID as the identification information of the store from which he or she intends to purchase the product. The user then inputs his or her personal ID number (the number registered in 706 in FIG. 7), the payment method, and the purchase price of the product (step 1001). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17.

Further, regarding the payment method, there are the options of credit card payments, web money

payments, and debit card payments, and if the credit card payment is selected, the number of payments and the credit card number are inputted. In addition, if the web money payment is selected, the web money account number (the number registered in 711 in FIG. 7) is inputted. Similarly, if the debit card payment is selected, the debit card number (the number registered in 709 in FIG. 7) is inputted. In the following flowchart, the operations performed by individuals are shown in a double-bordered format, as in step 1001.

When the input is complete, the transmission operation is performed. Then, the information input in step 1001 is sent to the authentication server 41 as the QR authorized certification key issuance request. The authentication server 41 that receives this request for issuing the QR authorized certification key information performs authentication processing for the store and the user (step 1002). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched using the PIN number and the credit card number (or the web money account number, or debit card number), and it is checked whether the user with the PIN number and the credit card number (or the web money account number, or debit card number) is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1003). Even if the personal ID number and the credit card number (or web money account number or debit card number) are not registered, the user is either an unauthorized user or an unregistered user, and a message indicating that the transaction is not possible is sent back to the mobile phone 1 (step 1003). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1001 is automatically deleted.

However, if the store ID, the PIN number, and the credit card number (or web money account number, or debit card number) are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1004) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1005). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1006) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 1007). The store staff enters the price of the desired purchase item using the store terminal (step 1008).

In parallel, the user inserts and attaches the mobile phone 1 with the QR authorized key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 1009). The QR code reader 21 then reads the QR authorized certification key 1201 displayed on the display 11 of the mobile phone 1 (step 1011), and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1010), and forwards the information to the store terminal 22.

The store terminal 22 then sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the QR authorized certification key 1201 was issued by the authentication server itself, only part of the information such as the authorization number and the personal authentication may be sent. FIG. 11 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile

phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1012). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1013), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR authorized certification key 1201, and the QR authorized certification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1014). In addition, the user will be notified verbally that a payment cannot be decided by the store staff.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) on the QR authorized certification key 1201 received from the store terminal 22 is recognized as a genuine one issued by the store terminal 22, the authentication server 41 returns the detailed settlement approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed authorization information on the display unit as user information (step 1015). FIG. 12(b) shows an example of this. The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1016).

If there is a response confirming the purchase intention from the person, the transaction is completed by operating the transaction button (step 1017). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1018). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. In addition, the approval completion information is transmitted to the financial institution 42. As a result, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. This approval content 1301 can be stored until it is deleted by the user. However, since the QR authorized certification key 1301 is only valid once, it is automatically deleted after a predetermined period of time. In addition, the financial institution 42 that receives the approval completion information performs procedures to withdraw the amount from the user's designated account.

Based on the above, a decision can be made when purchasing products at general stores using a mobile phone 1. If the user withdraws his or her intent to purchase, the processing of the store terminal is terminated by a cancellation operation at the store terminal. In addition, even if the user himself or herself performs a cancellation operation on the mobile phone 1, the payment processing will be terminated midway and all information such as the QR authorized certification key 1301 will be deleted. As is clear from the explanations above, according to the transaction method, the payment can be approved only by the QR authorized certification key issued by authentication server 41 without conveying confidential information such as the credit number of the user to the store. In addition, since the configuration does not hold any confidential information such as credit card numbers in the mobile phone 1, even if the mobile phone 1 is lost, there is no risk of it being misused for payment settlement. Furthermore, as the validity of the mobile phone serial number and the mobile number is determined by the sign recorded by mixing the special crystalline powder, it is possible to prevent misuse due to modification of the mobile phone itself, and by increasing the security of devices used for the payments, it will have beneficial effects for both the users and stores.

Moreover, since the store only needs to add the reader 21, there is an advantage that the cost of joining the system can be reduced. Similarly, the mobile phone 1 can be used as a commercially available mobile phone without adding an IC card or the like. In addition, since the purchase history is managed, it is no longer necessary to issue a point card from the store side. Further, since the user can see the usage status, there is an advantage in that it is useful for making systematic purchase plans.

Also, by using a QR code, the recording contents can be read from any direction in 360 degrees, so there is no restriction on the positional relationship with the reading unit, and it is suitable for use by

the general user to insert into the reader unit and read. Also, since it is not necessary to strictly define the positional relationship, the reading time can be shortened accordingly. In addition, even if some part of the code is dirty or damaged, the errors can be corrected, and the number of reading errors can be reduced. In particular, as in the present invention, when reading the data while it is displayed on the display of the mobile phone 1, it is conceivable that reading errors may occur due to dirt on the display unit, etc., but by using a QR code, reading errors caused by dirt on the display unit, etc. can be reduced. The QR authorized certification key is configured to include at least information on the approval number, personal authentication, name, and authorization method, but it may be a one-time password generated based on the approval number, personal authentication, or part or all of the name.

In this case, for example, the authentication server 41 and the mobile phone 1 are equipped with a password generation program based on the same logic, and when accessing for the second time, the mobile phone 1 automatically sends a password automatically generated based on the PIN number etc. sent on the first time. On the authentication server 41 side, authentication is performed by comparing the mobile phone number, etc., of the mobile phone 1 and the automatically transmitted password with the password automatically generated by the authentication server 41.

From the third time onward, a new password may be automatically generated and automatically sent based on the last automatically generated password.

By using such a so-called one-time password, security can be improved, and the input of a personal identification number can be omitted during the second and subsequent times of access.

Next, the method of deciding when purchasing small-value products such as drinking water from the vending machine 3 will be described with reference to the flowchart of FIGS. 14 and 15.

First, the user (product purchaser) sets the mobile phone 1 that he or she owns to the mobile shopping mode, and then uses the input means 14 to enter the store ID of the vending machine 3 from which he or she intends to purchase the product. The user then inputs his or her personal identification number (the number registered in 706 in FIG. 7), the payment method, and the purchase price of the product (step 1401). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17. In addition, there are credit card payment, web money payment, debit card payment, and contactless IC card payment methods, but since the payment amount is small, the use web money is made, and the web money account number (the number registered in FIG. 7-711) is entered.

When the input is complete, the transmission operation is performed. Then, the information input in step 1401 is sent to the authentication server 41 as the QR authorized certification key issuance request. The authentication server 41 that receives this request for issuing the QR authorized certification key information performs authentication processing for the store (here, the vending machine) and the user (step 1402). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store (vending machine) with the store ID is registered. Similarly, the user information DB 44 is searched by the PIN and the web money account number, and the user of the PIN and web money account number is checked to see if it is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). Furthermore, if the PIN and the web money account number are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1401 is automatically deleted.

However, if the store ID and the web money account number are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1404) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1405). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1406).

and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

The user inserts into the mobile phone 1 the QR authorized certification key 1201 displayed into the reading unit of the QR code reader 33 attached to the vending machine 3 (step 1407). Then, the selection operation of the vending machine 3 is performed for the desired product to be purchased (step 1408). In the vending machine 3, the price is automatically confirmed by selecting the desired product (step 1409).

The QR code reader 33 reads the QR authorized key 1201 displayed on the display unit 11 of the mobile phone 1 (step 1411) and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1410).

The vending machine 3 sends the mobile phone serial number, the mobile phone number, and the QR authorized certification key 1201 read from mobile phone 1 to the authentication server 41 as a payment approval request. In this case, the communication line can utilize data communication using a PHS telephone. FIG. 15 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1412). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1413), after which an unauthorized use message is sent to the vending machine 3 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR authorized certification key 1201, and the QR authorized certification key 1201 displayed on the display unit 11 is deleted.

In the vending machine 3, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1414). However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) on the QR authorized certification key 1201 received from the vending machine 3 is recognized as a genuine one issued by the vending machine 3, the authentication server 41 returns the detailed settlement approval to the store terminal 22. This detailed approval information includes the same information as the QR authorized certification key 1201, as well as the purchase history information of the user.

The store terminal 22, which has received the detailed approval, immediately performs the approval process (step 1415). Then, an authorization completion message is sent to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1416). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. In addition, the approval completion information is transmitted to the financial institution 42. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13 (step 1417).

The financial institution 42 that has received the authorization completion message performs procedures to debit the user's web money account or credit account.

Based on the above, it is possible to use the mobile phone 1 to make a decision when purchasing a small-value item from a vending machine.

As is clear from the explanations above, even in the transaction method, the payment can be approved only by the QR authorized certification key issued by the authentication server 41 without conveying confidential information such as the user credit number to the vending machine side.

Next, an explanation will be given of the method of making a payment when purchasing a product at an electronic store on the Internet with reference to the flowcharts of FIGS. 16 and 17.

First, the user (product purchaser) sets his or her mobile phone 1 to the mobile shopping mode, and uses the input means 14 to access a store on the Internet. The user inputs the number of the product to be purchased, the purchase price, and the receiving method, and orders the product (step 1601).

The store that receives the order for the product sends a request for personal authentication to the

authentication server 41. The authentication server 41 that receives this personal authentication request sends a request to the mobile phone 1 for inputting its personal identification number (the number registered in 706 in FIG. 7), the payment method, and the store ID.

Then, the user of the mobile phone 1 inputs his or her personal identification number (the number registered in 706 in FIG. 7), the payment method, and the store ID (step 1602). This content is sent to authentication server 41 as a request to issue a QR authorized certification key. Here, the decision-making method is the same as in the previous example.

The authentication server 41 that receives this QR authorized certification key request performs the authentication process of the user (step 1603). In other words, the store information DB 43 is searched based on the store ID included in the QR authorized certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched using the PIN number and the credit card number (or the web money account number, or debit card number), and it is checked whether the user with the PIN number and the credit card number (or the web money account number, or debit card number) is registered in the user DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1604). Even if the personal ID number and the credit card number (or web money account number or debit card number) are not registered, the user is either an unauthorized user or an unregistered user, and a message indicating that the transaction is not possible is sent back to the mobile phone 1 (step 1604). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 1602 is automatically deleted.

However, if the store ID, the PIN number, and the credit card number (or web money account number, or debit card number) are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 1605) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or QR authorized certification key is generated (step 1606). That is, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message to the mobile phone 1, which includes a message such as insufficient balance. However, if the credit is OK, a QR authorized certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 1607) and transmitted to the mobile phone 1. This QR authorized certification key consists of at least information on the approval number, personal identification, name, and the method of authorization.

In the mobile phone 1, the received QR authorized certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; The message, "Please insert it into the reader at the time of payment at the pick-up store specified by the customer", will be displayed.

In addition, the authentication server 41 sends a request to the store to issue a certificate of trust. The store that receives this request for the issuance of a certificate of trust generates the certificate of trust that includes the trust number, user name, product number, amount, settlement method, and receipt method, and sends it back to the authentication server 41. This certificate of trust is equivalent to a product order form from the perspective of the user.

The authentication server 41 that receives the certificate of trust integrates the QR authorized certification key 1201 and the certificate of trust, and sends it to the mobile phone 1 as the certificate of trust with the QR authorized certification key.

The user then goes to the pick-up store that he or she has designated, and inserts the certificate of trust with the QR authorized certification key into the reader of the QR code reader 21 attached to the store terminal 22 of the pick-up store, with the certificate of trust displayed on the display unit 11 (step 1608). The QR code reader 21 then reads the QR authorized certification key (step 1609) displayed on the display unit 11 of the mobile phone 1, and reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 1610), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the certificate of trust with the QR authorized certification key read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the certificate of trust with the QR authorized certification key has been issued by the authentication

server itself, only part of the information such as the payment number and the personal authentication may be sent. FIG. 17 shows that only the authorization number and the personal authentication information are included in the decision authorization request and sent.

When the authentication server 41 receives a request for approval, it first confirms whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 1611). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 9) (step 1613), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR authorized certification key, and the certificate of trust with the QR authorized certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1613). In addition, the user is notified verbally that the store staff cannot deliver the product or make a payment decision.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and it is found that the information (all or part) on the certificate of trust with the QR authorized certification key received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 will reply to the store terminal 22 with detailed approval. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1614). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1615).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the transaction is completed by operating the transaction button (step 1616). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1617). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. In addition, the authentication server 41 sends the authorization completion information to the financial institution 42. Based on the above, the customer can select a product at a store on the Internet using the mobile phone 1, and receive and approve the product at a pick-up store designated by the user.

As is clear from the explanations above, according to the transaction method, the payment can be made only with the QR authorized certification key issued by authentication server 41, without conveying any confidential information such as the user's credit number to the store side on the Internet.

Such a method can be used to order tickets for movies, etc., on the Internet, and store the QR authorized certification key on the mobile phone 1, and insert it into the reader at the entrance of the movie theater, for example, to make use of the operational format such as entering the movie theater without a ticket. Here, instead of displaying the certificate of trust with the QR authorized certification key to the display unit 11 and having the reader 21 to read, a method can be adopted in which the certificate of trust with the QR authorized certification key is transferred to a personal computer (PC), printed with an attached printer, and read with a reading device at the receiving store. In this case, the printer's printing toner or ink mixed with the crystal powder similar to the signs 19 and 20 can be used.

FIG. 18 is a flowchart illustrating the procedure. This flowchart corresponds to the continuation of FIG. 16.

First, if the QR authorized certification key is received on the mobile phone 1, the QR authorized certification key is forwarded to a personal computer (PC) (step 1620) and printed with the attached printer (step 1621). A printing example is shown in FIG. 19(a).

Therefore, the user brings the printed certificate of trust with the QR authorized certification key to the receiving store designated by the user, and inserts it into the reading unit of the QR code reader 21 attached to the store terminal 22 at the receiving store. The QR code reader 21 then reads the printed

certificate of trust with the QR authorized certification key (step 1622) and forwards the reading to the store terminal 22.

The store terminal 22 then sends the results of the reading of the certificate of trust with the QR authorized certification key to the authentication server 41 as a request for approval, as in the case of FIG. 17.

When the authentication server 41 receives a request for approval, it first examines the validity of whether the QR authorized certification key of the certificate of trust with the QR authorized certification key is genuinely issued by the customer (step 1623). If the result is that it is not legitimate, it is determined that it is fraudulent use, and after registering this with the unauthorized usage information database (FIG. 9) (step 1624), an unauthorized usage message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR authorized certification key, and the certificate of trust with the QR authorized certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 1625). In addition, the user is notified verbally that the store staff cannot deliver the product or make a payment decision.

However, if it is found that the QR authorized certification key is genuine, the authentication server 41 will reply to the store terminal 22 with the detailed approval. This detailed payment authorization information includes information similar to the QR authorized certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed approval, displays all or part of the received detailed approval information as user information in the display unit (step 1626). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 1627).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the transaction is completed by operating the transaction button (step 1628). If the approval button operation is operated, the store terminal 22 sends an authorization completion message to the authentication server 41. The authentication server 41, which receives this authorization completion message, updates the user's purchase history information (step 1629). Thereafter, the details of the decision are sent to the mobile phone 1 for confirmation. Accordingly, the display unit 11 of the mobile phone 1 displays the decision details 1301 for confirmation as shown in FIG. 13. In addition, the authentication server 41 sends the authorization completion information to the financial institution 42. Based on the above, even if the user does not bring his or her mobile phone 1, the user can receive the product ordered at a store on the Internet at the receiving store designated by the user and make the final payment.

In this case, it is not necessarily essential to transfer the certificate of trust with the QR authorized certification key from the mobile phone 1 to a personal computer (PC), and it may be received directly from the personal computer as a network terminal and printed with a printer.

Using these methods, it is possible to use the printed certificate of trust with the QR authorized certification key in place of, for example, movie tickets ordered over the Internet. FIG. 19(b) shows an example of an admission ticket.

In each of the above examples, it is explained that the same mobile phone 1 is used as a network terminal that transmits information about the payment, etc., of products and as a network terminal that receives code character information images such as a QR payment certification key, but it is not limited to this, and the network terminal for transmitting information and the network terminal for receiving the code character information images may be used as a separate terminal.

By using this, it is also possible to transmit the code character information image to a third party's network terminal. Therefore, instead of gifting products or gift certificates to a third party, it is possible to make a payment using a code character information image transmitted to the third party's network terminal.

A payment processing method in this case will be explained below with reference to FIGS. 20 to 28.

In this case, the payment authorization institution 4 is provided with a gift information database (DB), and the authentication server 41 is provided with a gift information registration processing program

412. As shown in FIG. 20, for example, the gift information DB stores information including the giver ID 2001, the receiver ID 2002, the gift details 2003, the identification ID 2004, and the payment processing date 2005.

In addition, the gift information registration processing program described above is a program used when registering information on specific products or gifts of a certain amount in the gift information DB using the system.

In this payment processing method, the ordering party (the giver of the product) first sets the mobile phone 1 as an information transmitting terminal to the mobile shopping mode, and then uses the input means 14 to enter his or her identification PIN (the number registered in 706 in FIG. 7), payment method, user name of the recipient of the product and the recipient information such as the user ID, and gift details (in this case, the item number of the product to be gifted) (step 2101). Here, the payment method is the same as in the previous example.

When the input is complete, the transmission operation is performed. The information entered in step 2101 is then sent to authentication server 41 as a gift information transmission request.

The authentication server 41 that receives this gift information transmission request performs the authentication process of the user (step 2102). That is, the user information DB 44 is searched by the PIN number, the credit card number (or web money account number, or debit card number) included in the gift information transmission request, and the user of the PIN and the credit card number (or web money account number, or debit card number) is checked to see if the user is registered in the user information DB 44. In addition, the user information DB 44 is searched by the user ID, etc. as the recipient information, and as a result, if the PIN and the credit card number (or web money account number, or debit card number) are not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 2103). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and information such as the PIN entered in step 2101 is automatically deleted.

However, if the PIN number, the credit card number (or web money account number, or debit card number), the user ID as the recipient information, and the user name are registered correctly, the user is authenticated as an officially registered user, and the authentication is accepted.

If the authentication is OK, the authentication server 41 sends a credit inquiry regarding the usage limit or the balance to the financial institution 42. Then, if the credit processing at the financial institution 42 (step 2104) returns a credit result of OK or NG, depending on the credit result, a transaction prohibition message or gift information is sent (step 2105). In other words, if a credit result of NG is returned, the authentication server 41 sends a transaction prohibition message including a message such as insufficient balance to the giver's mobile phone 1. However, if the credit result is OK, the gift information is sent to the recipient's mobile phone 1 input in step 2101. As for this gift information, as shown in FIG. 24(a), the giver's user name and the product name as the gift contents are displayed, and the recipient sends back information to the authentication server 41 regarding refusal or acceptance of the gift contents (step 2106). If the authentication server 41 receives this reply and the information of a rejection is returned, it sends a confirmation message to the recipient's mobile phone 1 to that effect, and after sending a message of the rejection to the giver's mobile phone (see Fig. 24(c)), the information such as the PIN entered in step 2101 is automatically deleted. (step 2107) However, if the information of acceptance is returned, the authentication server 41 sends a request to the recipient's mobile phone 1 to enter the method of receiving the goods (see FIG. 24(b)).

Therefore, the user of the mobile phone 1 enters the store ID and the receiving method (step 2108). The contents are then sent to the authentication server 41 as a QR payment certification key issuance request. The authentication server 41 that receives this QR payment certification key request performs the authentication process of the store (step 2109). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. As a result, if the store ID is not registered, it is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the recipient's mobile phone 1 (step 2110). In the mobile phone 1, after confirming that the message indicating that the transaction is not possible is displayed on the display unit 11, another store ID or the like can be inputted.

However, if the store ID is registered correctly, the store is authenticated as an officially registered store, and the authentication is accepted.

If the authentication is OK, the authentication server 41 generates a QR payment certification key

configured with a two-dimensional code as shown in FIG. 3(d). (Step 2211) The QR payment certification key includes at least the payment number, the personal identification, name, and the payment method information.

In addition, the authentication server 41 sends a request to the store to issue a certificate of trust. The store that receives this request for the issuance of a certificate of trust generates the certificate of trust that includes the trust number, user name, product number, amount, payment method, and receipt method, and sends it back to the authentication server 41. This certificate of trust is equivalent to a product order form from the perspective of the user.

The authentication server 41 that has received the certificate of trust combines the QR payment certification key 1201 with the certificate of trust and transmits it to the recipient's mobile phone 1 as a certificate of trust with the QR payment certification key.

In the mobile phone 1, the received QR payment certification key is displayed on the display unit 11 as shown by the reference numeral 1201 in FIG. 12. At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

The user then goes to the pick-up store that he or she has designated, and inserts the certificate of trust with the QR payment certification key into the reader of the QR code reader 21 attached to the store terminal 22 of the pick-up store, with the certificate of trust displayed on the display unit 11 (step 2112). The QR code reader 21 then reads the mobile phone serial number and the mobile phone number from the signs 19, 20 (step 2113), and reads the QR payment certification key with the certificate of trust displayed on the display unit 11 of the mobile phone 1 (step 2114), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, mobile phone number, and the certificate of trust with the QR payment certification key read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, as for the certificate of trust with the QR payment certification key, it is only necessary to know that it has been issued by the authentication server 41 itself, so only some information such as the payment number and personal authentication may be sent. FIG. 23 shows that only the payment number and the personal authentication information is sent in the payment authorization request.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2115). As a result, if either number is unregistered or different from the registered number, it is determined to be unauthorized use and after registering in the unauthorized use information database (FIG. 9) (step 2116), an unauthorized use message is sent to the store terminal 22 and the mobile phone 1 on the receiving side. In addition, an unauthorized use messages is also sent to the mobile phone 1 on the giver side.

In the mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the certificate of trust with the QR payment certification key, and the certificate of trust with the QR payment certification key displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2117). In addition, the user is verbally notified that the store staff cannot deliver the product and that payment cannot be made.

However, in the event that both the mobile phone serial number and the mobile phone number are legitimate, and it is found that the information (all or part) on the certificate of trust with the QR payment certification key received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 will reply to the store terminal 22 with detailed payment approval. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22, which receives the detailed payment approval, displays all or part of the received detailed payment information as user information in the display unit (step 2118). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 2119).

If there is a confirmed response of the person's intent to purchase, the product is handed over, and the

payment is completed by operating the payment button (step 2120). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41.

The authentication server 41 that receives this payment completion message updates the purchase history information of the user on the giver side (step 2121). After this, the payment details for confirmation are sent to the terminal for information transmission on the giver's side. As a result, a confirmation message and the payment details 2501 and 2502, as shown in FIG. 25, are displayed on the display unit 11 of the giver's mobile phone 1, for example (step 2122). In addition, the authentication server 41 sends the payment completion information to the financial institution 42.

Based on the above, a specific product can be selected using the giver's terminal, and the product can be received and settled at a store designated by the recipient.

As is clear from the above explanation, according to the transaction method, payment can be made only with the QR payment certification key issued by authentication server 41 without conveying any confidential information such as the credit number of the giver to the store or the recipient of the gift. Furthermore, the recipient of the gift can be authenticated more reliably.

In this transaction method, the gift information is sent to the recipient and the recipient chooses whether or not to accept the gift, although the recipient who will accept or reject the gift is set in advance. The authentication server may decide whether to accept or reject the gift based on this setting. In this case, the above determination processing at the authentication server is performed instead of step 2106 and step 2107.

In addition, the contents of gifts given by this system may be not limited to specific products, but it may be content equivalent to a gift certificate of a certain gift amount.

FIGs. 26 and 27 are flowcharts illustrating the procedure in such a case. The flowchart in FIG. 26 corresponds to the continuation of FIG. 21.

In this case, as a prerequisite, in step 2101 of FIG. 21, a certain amount will be entered in place of the item number as the gift content.

Thereafter, after the processing shown in the flowchart of FIG. 21 is performed, the user on the receiving side inputs the receiving store ID and the purchase price of the product (step 2130). The contents are then sent to the authentication server 41 as a QR payment certification key issuance request. The authentication server 41 that receives this QR payment certification key issuance request performs the authentication process for the store and the purchase amount (step 2131). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. The gift information DB is also searched to check whether the input purchase amount is within the range of the amount stored in the DB. As a result, if the store ID is not registered or the purchase amount exceeds the gift amount, a non-transactionable message is returned to the mobile phone 1 (step 2132). On the receiver's mobile phone 1, after confirming that the message indicating that the transaction is not possible is displayed on the display unit 11, the recipient enters another store ID or purchase amount. However, if the store ID is registered correctly and the purchase amount entered is within the range of the gift amount, the product is certified to be the amount that can be purchased at the store with the official registration, and the certification is accepted.

If the certification is OK, the authentication server 41 generates a QR payment certification key composed of a two-dimensional code as shown in FIG. 3(d) and sends it to the mobile phone 1 (step 2133). The QR payment certification key includes at least the payment number, the personal identification, name, and the payment method information.

In the mobile phone 1, the received QR payment certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 2134). The store staff enters the price of the desired purchase item using the store terminal (step 2135).

In parallel, the user inserts and attaches the mobile phone 1 with the QR payment key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 2136). The QR code reader 21 then reads the QR payment certification key 1201 displayed on the display unit 11 of the mobile phone 1 on the receiving side (step 2137), and reads the mobile phone serial number and the

mobile phone number from the signs 19, 20 (step 2138), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the QR payment certification key 1201 read from the mobile phone 1 on the receiving side to the authentication server 41 as a payment approval request. In this case, since it is only necessary to know that the QR payment certification key 1201 was issued by the authentication server itself, only part of the information such as the payment number and the personal authentication may be sent.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2139). As a result, if either number is unregistered or different from the registered number, it is determined to be unauthorized use and after registering in the unauthorized use information database (FIG. 9) (step 2140), an unauthorized use message is sent to the store terminal 22 and the mobile phone 1 on the receiving side. In addition, an unauthorized use messages is also sent to the mobile phone 1 on the giver side.

In the receiver's mobile phone 1 that has received the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR payment certification key 1201, and the QR payment verification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2141). In addition, the user is notified verbally that payment cannot be made by the store staff.

However, if both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) of the QR payment certification key 1201 received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 returns the detailed payment approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed payment approval information as user information in the display unit (step 2142). The store staff confirms the purchase intention with the user themselves by looking at the contents of the display and the contents and price of the products they wish to purchase (step 2143).

If there is a confirmed response of the person's purchase intention, the payment is completed by the payment button operation (step 2144). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41. The authentication server 41 that receives this payment completion message updates the purchase history information of the user on the giver side (step 2145). Thereafter, the payment details for confirmation are transmitted to the mobile phone 1 of the giver. In addition, the payment completion information is sent to financial institution 42. As a result, for example, the payment details 2501 and 2502 for confirmation as shown in FIG. 25 are displayed on the display unit 11 of the giver's mobile phone 1 (Step 2146). The payment details 2501 and 2502 can be stored until deleted by the user. However, since the QR payment certification key 1201 is valid only once, it is automatically deleted after a prescribed time. In addition, the financial institution 42, that receives the payment completion information, takes procedures to debit the payment from the designated account of the user on the giver's side.

Based on the above, a certain amount can be specified using the terminal on the giver's side, and the recipient can freely purchase products, etc. at the store within the range of that amount, and settle the payment.

As is clear from the explanation above, according to the transaction method, even if a gift certificate of a certain amount is given, the payment can be made from the account of the giver only by the QR payment certification key issued by authentication server 41, without the store or the receiver receiving the confidential information such as the credit number of the giver. Further, the recipient can be authenticated more reliably.

In addition, in each of the above examples, payment by a financial institution is assumed, but the present invention can also be used when making payment by service points for all or part of the payment price. A payment processing method in this case will be explained below with reference to FIGS. 28 to 30.

In this case, the payment authorization institution 4 is provided with a service point database (DB), and

the authentication server 41 is provided with a service point registration processing program.

FIG. 28 is a diagram illustrating an example of the storage information for the service point DB, in which the update date 2801, the store name 2802, the number of additional points 2803, the number of points used 2804, and the service point balance 2805 are stored. This service point information is stored for each user in the order of update the date and time.

In addition, the service point registration processing program performs the payment processing based on service points obtained by purchasing products using this system.

Moreover, there are cases where the use of service points is processed by discounting the amount equivalent to a certain amount at the time of purchase of products based on the number of points, and where the service points are exchanged for products determined in advance based on the number of points, but in this embodiment, it is indicated that the service points are processed as the purchase price of the products.

In this payment processing method, the user (product purchaser) first sets the mobile phone 1 to the mobile shopping mode, and then using the input means 14, the user inputs the store ID of the store from which the product is to be purchased, along with his or her personal identification number (the number registered in 706 in FIG. 7), and the service points corresponding to the purchase price of the product (step 2901). Here, the identification information of the store or product may be obtained from the transmitter, etc. installed in the store via the external input and output interface 17.

When the input is complete, the transmission operation is performed. The information entered in step 2901 is then sent to authentication server 41 as a request to issue a QR payment certification key.

The authentication server 41 that receives this QR payment certification key issuance request performs authentication processing for the store and the user (step 2902). In other words, the store information DB 43 is searched based on the store ID included in the QR payment certification key issuance request, and it is determined whether or not the store with the store ID is registered. Similarly, the user information DB 44 is searched by PIN to see if the user is registered in the user information DB 44. As a result, if the store ID is not registered, the store is either an unauthorized store or an unregistered store, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 2903). Furthermore, if the PIN is not registered, the user is an unauthorized user or an unregistered user, and a message indicating that transactions are not possible is sent back to the mobile phone 1 (step 1403). In the mobile phone 1, a message indicating that the transaction is not possible is displayed on the display unit 11, and the information such as the store ID that was inputted in step 2901 is automatically deleted.

However, if the store ID and PIN are correctly registered, and the store is authenticated as an officially registered store and the user is officially registered, the authentication is accepted.

If the authentication is OK, the service point DB of the user is searched to inquire about the service point balance (step 2904). In response to this inquiry result, a non-transactionable message or QR payment certification key is generated (step 2905). In other words, if the result of the inquiry is that there is no balance, the authentication server 41 sends a non-transactionable message including a message such as insufficient balance to the mobile phone 1. However, if there is a balance, a QR payment certification key consisting of a two-dimensional code as shown in FIG. 3(d) is generated (step 2906) and transmitted to the mobile phone 1. The QR payment certification key includes at least the payment number, the personal authentication, and name information.

In the mobile phone 1, the received QR payment certification key is shown in the display 11 as shown by the reference numeral 1201 in FIG. 12(a). At the same time, a message such as "You can make payments using this mobile phone; please insert it into the device reader when making the payments" is displayed.

Therefore, the user presents the pre-selected desired product to the store staff at the store terminal 22 and places an order for the desired product (step 2907). The store staff calculates the number of points corresponding to the purchase price by entering the price of the desired product in the store terminal (step 2908).

In parallel, the user inserts and attaches the mobile phone 1 with the QR payment key 1201 displayed to the reader portion of the QR code reader 21 attached to the store terminal 22 (step 2909). The QR code reader 21 then reads the mobile phone serial number and the mobile phone number from the signs 19, 20 of the mobile phone 1 (step 2910), and reads the QR payment certification key 1201 displayed in the display 11 (step 2911), and forwards the reading to the store terminal 22.

The store terminal 22 sends the mobile phone serial number, the mobile phone number, and the QR

payment certification key 1201 read from the mobile phone 1 to the authentication server 41 as a payment approval request. In this case, it may be understood that the QR payment certification key 1201 was issued by the authentication server itself, so only some information such as the payment number and the personal authentication may be sent. FIG. 30 shows that only the payment number and the personal authentication information is sent in the payment authorization request.

When the authentication server 41 receives a payment authorization request, it first checks whether the mobile phone serial number and the mobile phone number are legitimate against the registration details of the user information DB 44 (step 2912). As a result, if either number is unregistered or different from the registered number, it is determined that the device has been used fraudulently and is registered in the unauthorized use information database (FIG. 11) (step 2913), after which an unauthorized use message is sent to the store terminal 22 and the mobile phone 1.

In the mobile phone 1 that receives the unauthorized use message, the unauthorized use message itself functions as a deletion command for the QR payment certification key 1201, and the QR payment certification key 1201 displayed on the display unit 11 is deleted.

In the store terminal 22, upon receiving the unauthorized use message, the display unit displays the user as an unauthorized user, and the process is terminated (step 2914). In addition, the user is notified verbally that payment cannot be made by the store staff.

However, if both the mobile phone serial number and the mobile phone number are legitimate, and the information (all or part) of the QR payment certification key 1201 received from the store terminal 22 is recognized to be genuine information issued by the customer himself or herself, the authentication server 41 returns the detailed payment approval to the store terminal 22. This detailed payment authorization information includes information similar to the QR payment certification key 1201, as well as personal characteristic information such as information on the user's purchase history and a photo of the user.

The store terminal 22 displays all or part of the received detailed payment approval information as user information in the display unit (step 2915). The store staff confirms the purchase intent with the user themselves by looking at the display content, and the content of the desired product to be purchased, and the number of points corresponding to the price (Step 2916).

If there is a confirmed response of the person's purchase intention, the payment is completed by the payment button operation (step 2917). If the payment button operation is operated, the store terminal 22 sends a payment completion message to the authentication server 41. The authentication server 41 that receives this payment completion message updates the user's purchase history information and service point information (step 2918). After this, the payment details for confirmation are sent to the mobile phone 1. The payment details can be saved until the user deletes them. However, since the QR payment certification key 1201 is valid only once, it is automatically deleted after a prescribed time.

Based on the above, it is possible to use a mobile phone 1 to make payments using service points when purchasing products at general stores.

As is clear from the explanations above, according to the transaction method, even when making a payment using service points, it is possible to perform the payment using only the QR payment certification key issued by the authentication server 41, making it possible to eliminate the need for a point card or the like. In addition, the authentication of service users can be performed more reliably.

The methods shown in each of the above examples do not require financial settlement, but can be used instead of tickets such as admission tickets or receipts for goods, etc. It should be noted that the procedures described above can be implemented with some changes depending on the financial institution or the like. Furthermore, the procedure performed by the authentication server 41 may be recorded as a program for decision making on a recording medium such as a CD-ROM, and provided to the decision-making system builder.

Although the mobile phone serial number and the mobile phone number signs are recorded using recording materials mixed with a special crystalline powder, other methods of recording in a recording format that can physically determine the authenticity may be used.

In addition, in the next-generation mobile communication services that use mobile phones etc. equipped with an IC card (UIM card), the mobile phone numbers etc. are written on the IC card, and an operation mode is being considered in which the same mobile phone number can be used on different terminals by replacing the IC card.

Thus, in this case, the IC card may be labeled or printed as shown in FIG. 3(c).

In addition, in this case, it is necessary to make the sign readable by an external reader while the IC card is inserted into the slot provided in the mobile phone or the like.

Examples of handsets used in this case will be described with reference to FIGS. 31 and 32.

FIGS. 31 and 32 are partial perspective views of a mobile phone used in the present embodiment, wherein in each figure, the IC card installed in the mobile phone that stores information such as the mobile phone number is represented by the number 300, and a sign 311 as shown in FIG. 3(c) is pasted or printed on the surface of the IC card. It should be noted that, in place of the serial number of the mobile phone, the identification information of each IC card or of the owner is recorded on the sign 311 together with the mobile phone number.

In the present embodiment, a recess 300 is formed that allows the IC card to be mounted such that the sign 311 affixed to the IC card is visible from the reading direction, as shown by the arrow in the figure, and such as on the back side of the mobile phone 1, for example, as shown in FIG. 31(a). This allows the reader 22 to read the label in the same way as when a label is affixed on the casing of the mobile phone 1.

Also, as shown in FIG. 31(b), an IC card insertion slot 301 found in the mobile phone 1 may be provided, and an opening 302 may be formed in the area where the sign 311 is located so that the sign can be read (visually recognized) by an external reading device when the IC card 310 is inserted into the slot 301. The front surface of the opening 302 may be shielded with a transparent resin material or the like, as long as the sign 311 is visible from the reading direction shown by the arrow in the figure.

Other configurations may also be used if the sign 311 can be read by an external reader, for example, the entire casing of the mobile phone may be made of a transparent resin material or the like that allows the inside to be seen.

In this way, the invention can be applied to mobile phones, etc. that support the next generation of mobile communication services, and in addition, it is possible to increase security by eliminating the need to store data such as credit card numbers in the IC cards.

It should be noted that the mobile phone 1 may be provided with a reading device for the sign 311, and the reading device may read the sign and transmit the read information to the store terminal.

In this case, for example, as shown in FIG. 32(a), a reading sensor unit 303 connected to the control unit 13 (see FIG. 2(a)) is provided at a location where the mark 311 of the IC card inserted into the slot 301 is located. As a result, the information on the sign 311 read by the reading sensor unit 303 can be transmitted to the authentication server 41 via the transmitting means of the mobile phone 1. It should be noted that the processing of reading information on the sign 311 may be performed while the IC card is inserted into the slot 311, and in this case, a sensor unit may be provided in the portion of the slot corresponding to the portion through which the marker 311 passes.

Moreover, as shown in FIG. 32(b), the IC card 310 is not limited to the one that is inserted into the mobile phone 1, and by inserting a part of the IC card 310 into the slit 304 formed on the side of the mobile phone 1, and sliding it in the sliding direction shown by the arrow in the figure, it is conceivable that the information in the IC card 310 may be read by the sensor unit (not shown). In this case, when sliding a portion of the IC card 310 into the slit 304, a portion of the site corresponding to the site through which the sign 311 passes within the slit 304 may be provided with a reading sensor unit 305. In addition, when using a wireless or optical non-contact type IC card as the IC card 310, and by inserting the IC card 310 into a reading device installed at each store etc., the sign 311 may be read directly; or as with the above example, the mobile phone 1 may be equipped with a reading device, and the information on the sign 311 may be recognized by radio or light, similar to the information in the IC card 310.

[Brief Description of Drawings]

[FIG. 1] A system configuration diagram showing an embodiment of a system implementing the commercial transaction method of the present invention.

[FIG. 2] A schematic block diagram illustrating a configuration of a mobile phone.

[FIG. 3] A diagram showing an example of a label, a barcode, and a two-dimensional code attached to a mobile phone.

[Fig. 4] Across-sectional configuration diagram of a reading device that reads the barcode attached to the mobile phone and a two-dimensional code displayed on the display unit.

[FIG. 5] An internal configuration diagram of the authentication server.

[FIG. 6] A diagram illustrating an example of the data stored in the store information database.

[FIG. 7] A diagram showing an example of data stored in a user information database.

[FIG. 8] A diagram showing an example of the data stored in the purchase history database.

[FIG. 9] A diagram showing an example of the data stored in the unauthorized use information database.

[FIG. 10] A flowchart illustrating the procedure for using a mobile phone to settle the price of goods at a general store.

[FIG. 11] A flowchart showing a continuation of FIG. 10.

[FIG. 12] A diagram illustrating an example of a QR payment certification key displayed on the mobile phone and the user information displayed on the store terminal.

[FIG. 13] A diagram illustrating an example of the confirmation information displayed on the mobile phone at the end of payment.

[FIG. 14] A flowchart showing the procedure for the payment of small-value products at a vending machine.

[FIG. 15] A flowchart showing a continuation of FIG. 14.

[FIG. 16] A flowchart illustrating the procedure for receiving and clearing items ordered at stores on the Internet at designated receiving stores.

[FIG. 17] A flowchart showing a continuation of FIG. 16.

[FIG. 18] A flowchart showing the procedure for bringing a printed copy of the QR payment certification key to the store for payment.

[FIG. 19] A diagram illustrating an example of a printed QR payment certification key.

[FIG. 20] A diagram showing an example of the data stored in the gift information database.

[FIG. 21] A flowchart showing the procedure for settlement of gifts to others.

[FIG. 22] A flowchart showing a continuation of FIG. 21.

[FIG. 23] A flowchart showing a continuation of FIG. 22.

[FIG. 24] A diagram illustrating a display example of the gift information displayed on a mobile phone and a display example after selecting acceptance or rejection of the gift.

[FIG. 25] A diagram showing an example of information for confirmation displayed on the mobile phone on the giver's side at the end of payment.

[FIG. 26] A flowchart showing a continuation of FIG. 21.

[FIG. 27] A flowchart showing a continuation of FIG. 26.

[FIG. 28] A diagram illustrating an example of a service point usage history database.

[FIG. 29] A flowchart illustrating the procedure for making a payment using service points at a general store using a mobile phone.

[FIG. 30] A flowchart showing a continuation of FIG. 29.

[FIG. 31] A partial perspective view illustrating an example of a mobile phone used in the present invention.

[FIG. 32] A partial perspective view illustrating an example of a mobile phone used in the present invention.