Method and Apparatus for Paying Fare

Technical Field

The present specification relates to the field of information technology, and in particular relates to a method and apparatus for paying a fare.

Background

Currently, the method of using the near field communication (NFC) function of a terminal (for example, a mobile phone) to simulate the terminal such as mobile phone into a public transit card so that the user can take a public transit means by "swiping the mobile phone" has come into use, as shown in Fig. 1.

Generally, the terminal which simulates a public transit card must have at least the following three hardware units: NFC front-end chip, NFC antenna and security chip. Among them, the NFC front-end chip and the NFC antenna are used to realize NFC communication, and the account ID and account balance of the public transit card are stored in the security chip in the form of hardware encryption, that is, the function of the security chip is to prevent the account balance from being illegally modified.

When using a terminal to takes a public transit means, a user keeps the terminal close to the fare-collecting device of the public transit means, the fare-collecting device establishes an NFC connection with the terminal, and the fare-collecting device has the permission to rewrite the account balance stored in the security chip in the terminal (for example, rewrite $100 into $98) over the NFC connection to collect the fare.

Based on the existing solution, a low-cost method for paying a fare is required.

Summary

Some embodiments of this specification provide a method and apparatus for paying a fare to solve the high-cost problem with the prior method for paying a fare.

To solve the above-mentioned technical problem, some embodiments of this specification are realized in a following way:

the method for paying a fare in some embodiments of this specification comprises:

establishing, by a user terminal, a near field communication (NFC) connection with a fare-collecting device of a public transit means,

encrypting an account ID of a user according to a pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

transmitting the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server to cause the server to deduct a fare from an account corresponding to the account ID.

The method for paying a fare in some embodiments of this specification comprises:

establishing, by the fare-collecting device of a public transit means, an NFC connection with a user terminal,

receiving over the NFC connection the encrypted data transmitted from the user terminal, wherein the encrypted data is obtained by the user terminal by encrypting the account ID of the user,

decrypting the encrypted data to obtain the account ID of the user, and

sending the account ID to a server so that the server deducts a fare from the account corresponding to the account ID.

The apparatus for paying a fare in some embodiments of this specification comprises:

an establishment module, configured to establish an NFC connection with the fare-collecting device of a public transit means,

an encryption module, configured to encrypt the account ID of a user according to the pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

a transmission module, configured to transmit the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server to cause the server to deduct a fare from the account corresponding to the account ID.

The apparatus for paying a fare in some embodiments of this specification comprises:

an establishment module, configured to establish an NFC connection with a user terminal,

a receiving module, configured to receive over the NFC connection the encrypted data transmitted from the user terminal,

a decryption module, configured to decrypt the encrypted data to obtain the account ID of the user, and

a sending module, configured to send the account ID to a server so that the server deducts a fare from the account corresponding to the account ID.

A device for paying a fare in some embodiments of this specification comprises one or more processors and a memory, a program is stored in the memory and the device is so configured that the one or more processors perform the following steps:

establish an NFC connection with the fare-collecting device of a public transit means,

encrypt the account ID of the user according to the pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

transmit the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server to cause the server to deduct a fare from the account corresponding to the account ID.

A device for collecting a fare in some embodiments of this specification comprises one or more processors and a memory, a program is stored in the memory and the device is so configured that the one or more processors perform the following steps:

establish an NFC connection with a user terminal,

receive over the NFC connection the encrypted data transmitted from the user terminal,

decrypt the encrypted data to obtain the account ID of the user, and

send the account ID to a server so that the server deducts a fare from the account corresponding to the account ID.

From the technical solutions provided in some embodiments of this specification, it can be seen that in some embodiments of this specification, when a user takes a public transit means, the user terminal establishes an NFC connection with the fare-collecting device of the public transit means, the user terminal transmits the encrypted account ID of the user to the fare-collecting device, and the fare-collecting device can request a server to deduct the fare from the account of the user. According to some embodiments of this specification, no security chip is required for the user terminal, the account balance of the user is recorded and modified by the server, and the user can still take a public transit means by "swiping a mobile phone."

Brief Description of the Drawings

To describe some embodiments of this specification or the technical solution in the existing solution more clearly, the following briefly describes the drawings required in the

description of some embodiments or the existing solution. Obviously, the drawings in the following description are only some embodiments of this specification. Without any creative work, those skilled in the art can obtain other drawings on the basis of these drawings.

Fig. 1 shows a method of paying a fare by simulating a mobile phone into a public transit card.

Fig. 2 is a flowchart of a method for paying a fare in some embodiments of this specification.

Fig. 3 is a schematic diagram for an apparatus for paying a fare in some embodiments of this specification.

Fig. 4 is a schematic diagram for another apparatus for paying a fare in some embodiments of this specification.

Fig. 5 is a schematic diagram for a device for paying a fare in some embodiments of this specification.

Fig. 6 is a schematic diagram for another device for paying a fare in some embodiments of this specification.

Detailed Description of the Invention

As described in the background art, a current user terminal must have hardware units such as NFC front-end chip, NFC antenna and security chip so that the user can take a public transit means such as bus or subway by "swiping a mobile phone."

However, on the one hand, requiring a user terminal, for example, a mobile phone, to have a security chip will lead to high hardware cost of the mobile phone; and on the other hand, a large number of mobile phones available on the market still have no security chip, and the users of these mobile phones cannot enjoy the convenience of taking a public transit means by "swiping a mobile phone."

As a result, in some embodiments of this specification, on the one hand, the account balance of a user will not be stored in a user terminal and the account of the user will be maintained by a server; on the other hand, no matter whether the user terminal has a security chip, the NFC front-end chip and NFC antenna of the user terminal can be utilized so that the user terminal establishes an NFC connection with the fare-collecting device of a public transit means, the user terminal transmits the account ID of the user to the fare-collecting device, and then the

fare-collecting device requests a server to deduct a fare from the account corresponding to the account ID.

For the convenience of description, the public transit means in the following description is a subway.

To help those skilled in the art better understand the technical solutions of this specification, the following will clearly and thoroughly describe the technical solutions in some embodiments of this specification in combination with the drawings in one or more embodiments of this specification. Obviously, the embodiments described are only a part, but not all of the embodiments of this specification. All other embodiments obtained by those skilled in the art on the basis of some embodiments of this specification without any creative work should fall within the scope of protection of this specification.

The technical solutions in some embodiments of this specification are described in detail below in combination with the drawings.

Fig. 2 is a flowchart of the method for paying a fare in some embodiments of this specification and the method comprises the following steps:

S200: A user terminal establishes an NFC connection with the fare-collecting device of a public transit means.

In some embodiments of this specification, the user terminal can be a mobile phone, a tablet PC, a notebook PC or a smart device which can be applied in a mobile payment scenario. The fare-collecting device of the public transit means can be a subway gate or a card reader on a bus, and the fare-collecting device is a subway gate in the following description.

In this step, the user can move the user terminal close to the fare-collecting device, and only when the distance between the user terminal and the fare-collecting device is not greater than the NFC induction distance, the user terminal can establish an NFC connection with the fare-collecting device.

It should be noted that the establishment of an NFC connection is independent of the Internet or LAN, and therefore, when both the user terminal and the fare-collecting device are offline, an NFC connection can still be established between them.

S202: The user terminal encrypts the account ID of the user according to the pre-agreed encryption algorithm of the public transit system to obtain encrypted data.

S204: The user terminal transmits the encrypted data to the fare-collecting device over the NFC connection.

In some embodiments of this specification, in order to prevent the account ID of the user from being maliciously intercepted during the transmission, the user terminal can encrypt the account ID of the user and transmit the encrypted data to the fare-collecting device over the NFC connection. In this way, even if the encrypted data is intercepted by a malicious user during the transmission, the lawbreaker cannot decrypt the encrypted data to obtain the account ID of the user.

It should be noted that the encryption algorithm the user terminal uses to encrypt the account ID in step S202 can be an encryption algorithm which is only applicable to data transmission between the user terminal and the public transit means. The encryption algorithm can be executed by a payment application installed on the user terminal, and the encryption algorithm can be agreed on in advance between the payment application and the public transit system (for example, a server of a subway corporation).

S206: The fare-collecting device receives over the NFC connection the encrypted data transmitted from the user terminal.

S208: The fare-collecting device decrypts the encrypted data to obtain the account ID.

S210: The fare-collecting device sends the account ID to a server and the server deducts a fare.

In some embodiments of this specification, the fare-collecting device can acquire the account ID only after decrypting the encrypted data. Later, the fare-collecting can send the account ID obtained by decrypting the encrypted data to the server and the server can deduct the fare from the account corresponding to the account ID.

When a payment application is installed on the user terminal and the account ID is encrypted by the payment application, the server is the server which the payment application corresponds to.

In addition, if the subway the user takes is in segment charging mode, the fare-collecting device needs to acquire over the NFC connection the encrypted data transmitted from the user terminal when the user enters and leaves a station (gets on and off when the user takes a bus). When the user enters a station, the fare-collecting device may make a record according to the account ID obtained by decrypting the encrypted data, and when the user leaves a station, the fare-collecting may calculate the fare according to the account ID obtained by decrypting the encrypted data and send the account ID and the fare to the server, and then the server may deduct the fare from the account corresponding to the account ID.

If the subway the user takes is in uniform charging mode (e.g., the fare is fixed at $2, regardless of the mileage), the fare-collecting device only needs to acquire the account ID and sends the account ID to the server when the user enters a station, and the server deducts the $2 fare from the account corresponding to the account ID.

In the prior method for paying a fare, a user terminal having the three hardware units of an NFC front-end chip, an NFC antenna and a security chip is equivalent to a public transit card, in which an account balance is stored, the user enters or leaves a station by moving the user terminal close to the induction zone of a subway gate, and the fare-collecting device may rewrite the account balance stored in the security chip of the user terminal to complete fare deduction.

In some embodiments of this specification, no account balance may be stored in a user terminal, the fare-collecting device may not directly perform a fare deduction operation, and the fare-collecting device may actually request the server to deduct a fare from the account of a user. The account ID of the user may be obtained by registering an account on the server. Therefore, the fare-collecting device may need to send the account ID sent by the user terminal to the server to request the server to deduct the fare from the account of the user. In this way, the fare-collecting device may complete a fare collection.

In addition, user A can theoretically use the encrypted data obtained by encrypting the account ID of user B to enter a station. That is, when user B enters a station, user A can intercept the encrypted data transmitted from the user terminal of user B to the fare-collecting device, and later use the encrypted data to enter the station, and the server will also deduct a fare from the account of user A.

To prevent this case, the user terminal can acquire the timestamp corresponding to the current time and encrypts the account ID of the user and the timestamp to obtain encrypted data in step S202. In step S208, the fare-collecting device decrypts the encrypted data to obtain the account ID and the timestamp, and in step S210, the fare-collecting device determines whether the time interval from the timestamp obtained by decrypting the encrypted data to the current time satisfies a specified condition. If yes, the fare-collecting device may send the account ID to the server, and if no, the fare-collecting device may refuse to send the account ID to the server. The specified condition may be a specified time length, and can be specified according to the requirement, for example, to be 5 seconds.

In this way, even if user B intercepts the encrypted data and later uses the encrypted data to enter a station, the fare-collecting device will determine that the encrypted data is invalid because of timeout and the fare-collecting device can refuse to send the account ID to the server.

In addition, when the encrypted data is obtained by the user terminal of user A by encrypting the account ID and the timestamp corresponding to the current time, user B can be prevented from later going into the station after intercepting the encrypted data, however, user B can use the intercepted encrypted data to enter the station from another subway gate just at the moment when user A enters the station.

Therefore, in step S202, the user terminal can further acquire the device ID of the fare-collecting device and encrypt the account ID of the user, the timestamp corresponding to the current time and the device ID to obtain encrypted data. The user terminal can acquire the device ID over the established NFC connection. In step S208, the fare-collecting device decrypts the encrypted data to obtain the account ID, timestamp and device ID. In step S210, the fare-collecting device not only needs to determine whether the time interval from the time corresponding to the timestamp obtained by decrypting the encrypted data to the current time satisfies a specified condition, but also needs to determine whether the device ID obtained by decrypting the encrypted data is consistent with its own device ID, if the two determination results are both yes, the fare-collecting device sends the account ID to the server, and if either determination result is no, the fare-collecting device refuses to send the account ID to the server.

In this way, even if user B intercepts the encrypted data of user A and enters the station from another subway gate (or get on another bus) at the moment when user A enters the station, another subway gate will also determine that the device ID obtained by decrypting the encrypted data is not its own device ID and thus will refuse to send the account ID to the server.

Of course, the timestamp and the device ID adopted in the above-mentioned technical means can be used separately. That is, the user terminal can encrypt the account ID and the timestamp corresponding to the current time to obtain encrypted data, or encrypt the account ID and the device ID of the fare-collecting device to obtain encrypted data.

In addition, in some embodiments of this specification, when the fare-collecting device is online, the fare-collecting device can control the opening of the entrance and/or report no error to allow a user to enter a station or get on a bus while sending the account ID to the server. The fare-collecting device can report an error and/or control the closing of the entrance to prevent the user from going into the station or getting on the bus when it refuses to send the account ID to the server.

When the fare-collecting device is offline, if the fare-collecting device refuses to send the account ID to the server, the fare-collecting device can report an error and/or control the closing of the entrance to prevent the user from going into the station or getting on the bus. If the

fare-collecting device needs to send the account ID to the server, the fare-collecting device can first store the account ID to be sent and control the opening of the entrance and/or report no error to allow the user to enter the station or get on the bus. Then, the fare-collecting device can send the stored account ID to the server when connected to a network.

Through the method shown in Fig. 2, no security chip is required for a user terminal, and thus the corresponding hardware cost is saved. In addition, the account balance of a user is recorded and modified by the server, and the user can still take a public transit means by "swiping a mobile phone." Even if the user terminal of the user has no security chip, the user can also move the user terminal close to a subway gate to enter a station and experience the "touch payment."

On the basis of the method for paying a fare in Fig. 2, some embodiments of this specification further provide an apparatus for paying a fare accordingly. As shown in Fig. 3, the apparatus comprises:

an establishment module 301, configured to establish an NFC connection with the fare-collecting device of a public transit means,

an encryption module 302, configured to encrypt the account ID of a user according to the pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

a transmission module 303, configured to transmit the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server and then the server deducts a fare from the account corresponding to the account ID.

The encryption module 302 acquires the timestamp corresponding to the current time and encrypts the account ID of a user and the timestamp to obtain encrypted data.

The encryption module 302 acquires the device ID of the fare-collecting device over the NFC connection and encrypts the account ID of a user and the device ID to obtain encrypted data.

On the basis of the method for paying a fare in Fig. 2, some embodiments of this specification further provide another apparatus for paying a fare accordingly. As shown in Fig. 4, the apparatus comprises:

an establishment module 401, configured to establish an NFC connection with a user terminal,

a receiving module 402, configured to receive over the NFC connection the encrypted data transmitted from the user terminal,

a decryption module 403, configured to decrypt the encrypted data to obtain the account ID of the user, and

a sending module 404, configured to send the account ID to a server so that the server deducts a fare from the account corresponding to the account ID.

The decryption module 403 decrypts the encrypted data to obtain the account ID and the timestamp, and

the sending module 404 determines whether the time interval from the corresponding time of the timestamp to the current time satisfies a specified condition; if yes, the sending module sends the account ID to a server, and if no, the sending module refuses to send the account ID to the server.

The decryption module 403 decrypts the encrypted data to obtain the account ID and the device ID, and

the sending module 404 determines whether the device ID obtained from the decryption is consistent with its own device ID; if yes, the sending module sends the account ID to a server, and if no, the sending module refuses to send the account ID to the server.

The sending module 404 sends the account ID to a server and controls the opening of the entrance and/or reports no error, or refuses to send the account ID to the server and reports an error and/or controls the closing of the entrance.

On the basis of the method for paying a fare in Fig. 2, some embodiments of this specification further provide a device for paying a fare accordingly. As shown in Fig. 5, the device comprises one or more processors and a memory, a program is stored in the memory and the device is so configured that the one or more processors perform the following steps:

establish an NFC connection with the fare-collecting device of a public transit means,

encrypt the account ID of the user according to the pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

transmit the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server and then the server deducts a fare from the account corresponding to the account ID.

On the basis of the method for paying a fare in Fig. 2, some embodiments of this specification further provide another device for paying a fare accordingly. As shown in Fig. 6, the device comprises one or more processors and a memory, a program is stored in the memory and the device is so configured that the one or more processors perform the following steps:

establish an NFC connection with a user terminal,

receive over the NFC connection the encrypted data transmitted from the user terminal,

decrypt the encrypted data to obtain the account ID of the user, and

send the account ID to a server so that the server deducts a fare from the account corresponding to the account ID.

Some embodiments in the description are described in a progressive way. For the same or similar parts between some embodiments, refer to these embodiments. Each embodiment focuses the differences from the others. Especially, for the devices in Figs. 5 and 6, since they are basically similar to the embodiment of the method, their description is brief. For the relevant description, refer to the description of the embodiment of the method.

In the 1990s, it can obviously be determined whether a technical improvement is a hardware improvement (for example, improvement of the circuit structure of a diode, a transistor or a switch) or software improvement (for example, improvement of the method process). However, with the development of technologies, the improvements of today's many method processes have already been considered as direct improvements of hardware circuit structures. Designers can almost obtain a hardware circuit structure by programming an improved method process into a hardware circuit. Therefore, it cannot say that the improvement of a method process cannot be realized by hardware entity modules. For example, a programmable logic device (PLD), such as a field programmable gate array (FPGA) is such an integrated circuit whose logic function is determined by programming the device. Designers can themselves program a digital system to "integrate" it into a PLD, without asking a chip manufacturer to design and manufacture an application specific integrated circuit (ASIC) chip. Nowadays, programming which replaces manual manufacturing of integrated circuit chips is mostly done by a logic compiler, which is similar to a software compiler used for program development and writing. Original codes before compilation also need to be written by use of a specific programming language, for example, hardware description language (HDL). However, HDL is not the only programming language, and many other programming languages, for example, Advanced Boolean Expression Language (ABEL), Altera Hardware Description Language (AHDL), Confluence, Cornell University Programming Language (CUPL), HDCal, Java Hardware Description Language (JHDL), Lava, Lola, MyHDL, PALASM, and Ruby Hardware Description Language (RHDL) may be used. Currently, Very-High-Speed Integrated Circuit Hardware Description Language (VHDL) and Verilog are the most commonly used. Those skilled in the art should understand that a hardware circuit realizing a logic method process can

easily be obtained by using some of the above-mentioned hardware description languages to perform logic programming for the method process and program it into an integrated circuit.

A controller can be realized in any proper way. For example, a controller can be a microprocessor or processor, a computer-readable medium in which computer-readable program codes (for example, software or firmware) executed by the (micro)processor are stored, a logic gate, a switch, an application specific integrated circuit (ASIC), a programmable logic controller and an embedded micro controller. Examples of a controller include but are not limited to the following microcontrollers: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 and Silicone Labs C8051F320, and a memory controller can be realized as a part of the control logic of the memory. Those skilled in the art also know that besides a controller can be realized in the way of computer-readable program codes, the same function can completely be realized in the form of a logic gate, switch, ASIC, programmable logic controller, embedded microcontroller through logic programming of the procedure of a method. Therefore, such a controller can be considered as a hardware component and the devices configured to realize different functions in the hardware component can also be considered as structures in the hardware component. Or, the devices configured to realize different functions can even be considered as not only software modules realizing a method, but also structures in the hardware component.

The system, apparatus, modules or units described in some embodiments above can be realized by a computer chip or entity, or realized by a product having a function. A typical device is a computer. Specifically, the computer can be a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an e-mail device, a game console, a tablet computer, a wearable device or any combination of these devices.

For the convenience of description, when the apparatus is described, the apparatus is functionally divided into different units and these units are described respectively. Of course, the functions of different units can be realized in one or more pieces of software and/or hardware.

Those skilled in the art should know that some embodiments of this specification can provide a method, a system or a computer program product. Therefore, hardware-only embodiments, software-only embodiments or embodiments combining software with hardware can be adopted for this specification. In addition, the embodiment of a computer program product which can be implemented on one or more computer accessible storage media (including but not limited to disk memory, CD-ROM and optical memory) containing computer program codes can be adopted for this specification.

This specification is described by reference to the flowchart and/or block diagram of the method, device (system) and computer program product of some embodiments of this specification. It should be understood that each process in the flowchart and/or block in the block diagram and the combination of the processes in the flowchart and/or the blocks in the block diagram can be realized by computer program commands. These computer program commands can be provided in a general-purpose computer, a dedicated computer, an embedded processor or the processor of other programmable data processing equipment to produce a machine so that the commands executed by a computer or the processor of other programmable data processing equipment can produce a device configured to realize the designated functions in one process or more processes in the flowchart and/or in one block or more blocks in the block diagram.

These computer program commands can also be stored in a computer-readable memory which can boot a computer or other programmable data processing equipment to work in a specific mode so that the commands stored in the computer-readable memory can produce manufactures including a command device. The command device realizes the designated functions in one process or more processes in the flowchart and/or in one block or more blocks in the block diagram.

These computer program commands can also be uploaded to a computer or other programmable data processing equipment so that a series of operation steps are performed on the computer or other programmable data processing equipment to produce the processing realized by the computer and the commands executed on the computer or other programmable data processing equipment provide the steps for realizing the designated functions in one process or more processes in the flowchart and/or in one block or more blocks in the block diagram.

In a typical configuration, a computer device comprises one or more processors (CPU), an input/output interface, a network interface and a memory.

The memory may include a volatile memory, a random-access memory (RAM) and/or a nonvolatile memory of computer-readable media, for example, a read-only memory or a flash RAM. The memory is an example of computer-readable media.

Computer-readable media include volatile and nonvolatile media and mobile and immobile media, and they can realize information storage by use of any method or technique. Information can be computer-readable commands, data structures, modules of a program or other data. Examples of storage media of a computer include but are not limited to phase-change RAM (PRAM), static random access memory (SRAM), dynamic random access memory (DRAM), other types of random access memory (RAM), read-only memory (ROM), electrically erasable

programmable read-only memory (EEPROM), flash memory or other memory techniques, compact disk read-only memory (CD-ROM), digital versatile disk (DVD), cassette tape, magnetic tape, magnetic disk or other storage device or any other non-transmission medium, and they can be used to store information which can be accessed by a computer device. According to the definition in this document, computer-readable media excludes transitory media, for example, modulated data signals and carriers.

It should also be noted that the terms "comprise" and "contain" and their variants are intended to cover non-exclusive inclusions so that the process, method, commodity or device comprising a series of elements not only comprises these elements, but also comprises other elements not listed clearly, or comprises the elements intrinsic to the process, method, commodity or device. Without any more restrictions, the element defined by "comprising one…" do not exclude the case that other identical elements exist in the process, method, commodity or device which comprises the element.

Those skilled in the art should know that some embodiments of this specification can provide a method, a system or a computer program product. Therefore, hardware-only embodiments, software-only embodiments or embodiments combining software with hardware can be adopted for this specification. In addition, the embodiment of a computer program product which can be implemented on one or more computer accessible storage media (including but not limited to disk memory, CD-ROM and optical memory) containing computer program codes can be adopted for this specification.

This specification can be described in the general context of a computer executable command executed by a computer, for example, a program module. Generally, a program module comprises a routine, program, object, component and data structure which execute a specific task or realize a specific abstract data type. This specification can also be practiced in distributed computing environments. In the distributed computing environments, tasks are executed by remote processing equipment connected over a communication network. In distributed computing environments, a program module can be located in a local or remote computer storage medium including a storage device.

The above are only embodiments of this specification, but are not used to restrict this specification. Those skilled in the art can make various changes and modifications to this specification. Any modification, equivalent replacement, and improvement within the spirit and principle of this specification should fall within the scope of the claims of this specification.

Claims

1. A method for paying a fare, comprising:

establishing, by a user terminal, a near field communication (NFC) connection with a fare-collecting device of a public transit means,

encrypting an account ID of a user according to a pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

transmitting the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server to cause the server to deduct a fare from an account corresponding to the account ID.

2. The method as claimed in claim 1, wherein encrypting the account ID of the user to obtain the encrypted data specifically comprises:

acquiring a timestamp corresponding to a current time, and

encrypting the account ID of the user and the timestamp to obtain the encrypted data.

3. The method as claimed in claim 1, wherein encrypting the account ID of the user to obtain the encrypted data specifically comprises:

acquiring a device ID of the fare-collecting device over the NFC connection, and

encrypting the account ID of the user and the device ID to obtain the encrypted data.

4. A method for paying a fare, comprising:

establishing, by a fare-collecting device of a public transit means, an NFC connection with a user terminal,

receiving over the NFC connection encrypted data transmitted from the user terminal,

decrypting the encrypted data to obtain the account ID of the user, and

sending the account ID to a server to cause the server to deduct a fare from an account corresponding to the account ID.

5. The method as claimed in claim 4, wherein the decrypting the encrypted data to obtain the account ID specifically comprises:

decrypting the encrypted data to obtain the account ID and a timestamp, and

the sending the account ID to a server specifically comprises:

determining whether a time interval between a time corresponding to the timestamp and a current time satisfies a specified condition,

if yes, sending the account ID to the server, and

if no, refusing to send the account ID to the server.

6. The method as claimed in claim 4, wherein the decrypting the encrypted data to obtain the account ID specifically comprises:

decrypting the encrypted data to obtain the account ID and a device ID, and

the sending the account ID to a server specifically comprises:

determining whether the device ID obtained from the decryption is consistent with a device ID of the fare-collecting device,

if yes, sending the account ID to the server, and

if no, refusing to send the account ID to the server.

7. The method as claimed in claim 5 or 6, wherein the sending the account ID to a server specifically comprises:

sending the account ID to a server and controlling an opening of an entrance and/or reporting no error, and

the refusing to send the account ID to the server specifically comprises:

refusing to send the account ID to the server and reporting an error and/or controlling a closing of the entrance.

8. An apparatus for paying a fare, comprising:

an establishment module, configured to establish an NFC connection with the fare-collecting device of a public transit means,

an encryption module, configured to encrypt an account ID of a user according to a pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

a transmission module, configured to transmit the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server to cause the server to deduct a fare from an account corresponding to the account ID.

9. The apparatus as claimed in claim 8, wherein the encryption module acquires a timestamp corresponding to a current time and encrypts the account ID of the user and the timestamp to obtain the encrypted data.

10. The apparatus as claimed in claim 8, wherein the encryption module acquires a device ID of the fare-collecting device over the NFC connection and encrypts the account ID of the user and the device ID to obtain the encrypted data.

11. An apparatus for paying a fare, comprising:

an establishment module, configured to establish an NFC connection with a user terminal,

a receiving module, configured to receive over the NFC connection the encrypted data transmitted from the user terminal,

a decryption module, configured to decrypt the encrypted data to obtain the account ID of the user, and

a sending module, configured to send the account ID to a server so that the server deducts a fare from an account corresponding to the account ID.

12. The apparatus as claimed in claim 11, wherein the decryption module decrypts the encrypted data to obtain the account ID and a timestamp, and

the sending module determines whether a time interval from a time corresponding to the timestamp to the current time satisfies a specified condition; if yes, the sending module sends the account ID to the server, and if no, the sending module refuses to send the account ID to the server.

13. The apparatus as claimed in claim 11, wherein the decryption module decrypts the encrypted data to obtain the account ID and a device ID, and

the sending module determines whether the device ID obtained from the decryption is consistent with a device ID associated with the apparatus; if yes, the sending module sends the account ID to the server, and if no, the sending module refuses to send the account ID to the server.

14. The apparatus as claimed in claim 12 or 13, wherein the sending module sends the account ID to a server and controls an opening of an entrance and/or reports no error, or refuses to send the account ID to the server and reports an error and/or controls a closing of the entrance.

15. A device for paying a fare, comprising one or more processors and a memory, a program being stored in the memory and the device being so configured that the one or more processors perform the following steps:

establish an NFC connection with the fare-collecting device of a public transit means,

encrypt an account ID of a user according to a pre-agreed encryption algorithm of a public transit system to obtain encrypted data, and

transmit the encrypted data to the fare-collecting device over the NFC connection so that the fare-collecting device decrypts the encrypted data to obtain the account ID and sends the account ID to a server to cause the server to deduct a fare from an account corresponding to the account ID.

16. A device for collecting a fare, comprising one or more processors and a memory, a program being stored in the memory and the device being so configured that the one or more processors perform the following steps:

establish an NFC connection with a user terminal,

receive over the NFC connection encrypted data transmitted from the user terminal,

decrypt the encrypted data to obtain an account ID of a user, and

send the account ID to a server to cause the server to deduct a fare from an account corresponding to the account ID.